JYVÄSKYLÄ STUDIES IN COMPUTING
256

Jaana Kuula

The Hyperspectral and Smartphone Technology in CBRNE Countermeasures and Defence

JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 256

Jaana Kuula

The Hyperspectral and Smartphone Technology in CBRNE Countermeasures and Defence

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 2
joulukuun 17. päivänä 2016 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 2, on December 17, 2016 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2016

The Hyperspectral and Smartphone Technology in CBRNE Countermeasures and Defence

JYVÄSKYLÄ STUDIES IN COMPUTING 256

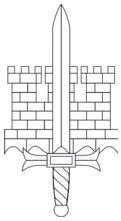
Jaana Kuula

The Hyperspectral and Smartphone Technology in CBRNE Countermeasures and Defence

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2016

Editors
Timo Männikkö
Department of Mathematical Information Technology, University of Jyväskylä
Pekka Olsbo, Ville Korkiakangas
Publishing Unit, University Library of Jyväskylä



Produced in association with the National Defence University
Department of Warfare

URN:ISBN:978-951-39-6889-2
ISBN 978-951-39-6889-2 (PDF)

ISBN 978-951-39-6888-5 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2016

To my Mother
Kirsti Kuula, born Huurtola (Haltt)
* 23.1.1925 † 1.5.2013

ABSTRACT

Kuula, Jaana
The Hyperspectral and Smartphone Technology in CBRNE Countermeasures and Defence
Jyväskylä: University of Jyväskylä, 2016, 214 p. (+ included articles)
(Jyväskylä Studies in Computing
ISSN 1456-5390; 256)
ISBN 978-951-39-6888-5 (nid.)
ISBN 978-951-39-6889-2 (PDF)
Finnish summary
Diss.

Caused by industrial and military use as well as other sources of chemical, biological, radiological, nuclear and high-yield explosive (CBRNE) materials, the global threat of weapons of mass destruction (WMDs) remains in spite of such weapons being internationally prohibited. With these materials, industrial and transportation accidents are likely in all countries and can also be triggered by natural disasters, such as in Fukushima in 2011. In addition, governments cannot fully control the manufacturing and usage of WMDs, as extreme terrorists have access to as well as the knowledge and motivation to use such materials. Due to multiple large-scale risks, the countering of CBRNE threats requires well-practiced joint operations by different authorities and new technical countermeasure methods. This dissertation studies how two novel technologies, hyperspectral technology and smartphone technology, can be used in CBRNE countermeasures and defence, especially by the police, defence forces and rescue services. The research is carried out adaptively via the concept development and experimentation (CD&E) method by forming the research framework with the generic military and civilian capability requirements of the European and North Atlantic operating concepts of CBRNE countermeasures and defence and by testing the capability requirements with related empirical experiments carried out as a part of the study. The experiments with hyperspectral technology focus on the detection of explosives, chemical warfare agents (CWAs), biofluids and other forensic samples, whereas the tests with smartphone technology deal with mobile emergency alerting, command and control, public warning and the information management of CBRNE incidents. The experiments are carried out with the Central Finland Police Department, the National Bureau of Investigation (NBI) and other units of the Police of Finland, the Finnish Defence Forces, the Rescue Department of Central Finland, the Finnish Institute for Verification of the Chemical Weapons Convention (Verifin) and the leading Finnish explosives manufacturer, Forcit.

Keywords: CBRNE countermeasures, CBRNE defence, CBRNE detection, joint operation, crisis management, emergency alerting, public warning, hyperspectral technology, smartphone technology

Author

Jaana Kuula
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Supervisors

Pekka Neittaanmäki
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Mika Hyytiäinen
Department of Warfare
National Defence University
Finland

Reviewers

Hugo Lavoie
Defence Research and Development Canada, Valcartier
The Department of National Defence
Canada

Kirsi Helkala
Norwegian Defence Cyber Academy
The Norwegian Cyber Defence Competency and
Transformation Centre
Norway

Opponent

Sasu Tarkoma
Department of Computer Science
University of Helsinki
Finland

ACKNOWLEDGEMENTS

I thank Professor and dean of the Faculty of Information Technology Pekka Neittaanmäki for inviting me to the university after my previous career and supervising my dissertation process. I also thank my supervisor in the National Defence University, Military Professor Mika Hyytiäinen, for helping me to embed my information technology research in the security sciences field. Thank you also to director of research, Professor Hannu H. Kari, for the additional support from NDU for my research. I am also grateful to the reviewers of my thesis, Professor Kirsi Helkala from the Norwegian Defence Cyber Academy and Hugo Lavoie from the Defence Research and Development Canada, and to my opponent, Professor Sasu Tarkoma from the University of Helsinki.

I also thank former Chief Police Officer, PhD Markku Luoma from the Central Finland Police Department for kindly giving the initial permission to conduct the necessary experiments with the police, which then developed into wide multi-authority research and this thesis. Thank you also to the head of laboratory research and development PhD Tapani Reinikainen for the National Bureau of Investigation's support for our hyperspectral research on crime scene investigation. For their help in carrying out the experiments, special thanks to police officers Tuomo Korhonen, Tuomas Teräväinen, Jukka Saarelainen and Pekka Poutiainen from the Central Finland Police Department, chief of communications Marko Luotonen from the National Police Board, captain, pioneer Marko Haukkamäki from the Air Force Command Finland, rescue chief Simo Tarvainen and risk manager Jarkko Jäntti from the Rescue Department of Central Finland, director, Professor Paula Vanninen and CBRNE specialists Martin Söderström and Matti Kuula from Verifin, and explosives manufacturer Forcit. Thank you to preparedness manager Janne Koivukoski and Taito Vainio from the Ministry of Interior and to the main funders of SpeCSI, SpeCSI Solutions and Sapporo projects, the Finnish funding agency for research and innovation Tekes and the University of Jyväskylä. Thanks also to my co-workers in these projects, especially Ilkka Pölönen, Hannu-Heikki Puupponen and Heikki Rinta. Warm thanks to the director of the Department of Mathematical Information Technology Professor Tuomo Rossi and to my project and travel secretaries Lea Hakala and Tiina Lampinen from the Faculty of Information Technology.

My dearest thanks to my sweet daughter Iina Kuula for bearing all the struggle with me, producing videos and other materials for my projects, pushing through her own degree in this same year and for starting her own career abroad in UK. My deep gratitude also to my mother Kirsti Kuula, who regretfully passed away during my thesis process and never saw my work finished. Further thanks to my father Pentti Kuula and to my sister Thina Kauppinen and brother Ilkka Kuula with their families. Finally, warm thanks to Raimo Lehtomäki and Marko Lehtomäki with his family for supporting Iina and me.

Jyväskylä, November 30, 2016
Jaana Kuula

LIST OF FIGURES

LIST OF TABLES

CONTENTS

LIST OF INCLUDED ARTICLES

PI **Jaana Kuula**, Heikki Rinta, Ilkka Pölönen, Hannu-Heikki Puupponen, Marko Haukkamäki and Tuomas Teräväinen. Detecting Explosive Substances by the IR Spectrography. *Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XV, edited by Augustus W. Fountain III, Proc. of SPIE Vol. 9073, 90730Q · © 2014 SPIE CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050157*, 2014.

PII **Jaana Kuula**. Drone Based Hyperspectral Detection of CBRNE Threats. *Jussi Paatero & Nils Meinander (Eds.). Proceedings of the NBC-2015 Symposium – How does the landscape evolve? - Helsinki, Finland, May, 2015. ISBN 978-952-93-5586-0*, 2015.

PIII **Jaana Kuula**, Ilkka Pölönen, Hannu-Heikki Puupponen, Tuomas Selander, Tapani Reinikainen and Tapani Kalenius. Using VIS/NIR and IR Spectral Cameras for Detecting and Separating Crime Scene Details. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI, edited by Edward M. Carapezza, Proc. of SPIE Vol. 8359, 83590P © 2012 SPIE · CCC code: 0277-786X/12/$18 · doi: 10.1117/12.918555*, 2012.

PIV **Jaana Kuula**, Heikki Rinta, Ilkka Pölönen and Hannu-Heikki Puupponen. The Challenges of Analysing Blood Stains with Hyperspectral Imaging. *Sensing Technologies for Global Health, Military Medicine, and Environmental Monitoring IV, edited by Šárka O. Southern, Mark A. Mentzer, Isaac Rodriguez-Chavez, Virginia E. Wotring, Proc. of SPIE Vol. 9112, 91120W · © 2014 SPIE · CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050180*, 2014.

PV **Jaana Kuula**, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen and Tuomo Korhonen. Smartphones as an Alerting, Command and Control System for the Preparedness Groups and Civilians: Results of Preliminary Tests with the Finnish Police. *Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013, T. Comes, F. Fiedrich, S. Fortier, J. Geldermann and T. Müller, eds.*, 2013.

PVI **Jaana Kuula**, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen and Tuomo Korhonen. Alerting Security Authorities and Civilians with Smartphones in Acute Situations. *Proceedings of the 12th European Conference on Information Warfare and Security ECIW-2013, Jyväskylä, Finland, 11-12. July*, 2013.

Articles **PI–PIV** deal with the usability and capability of hyperspectral technology and articles **PV–PVI** with smartphone technology in the security field, particularly in forensic and crime scene investigation and CBRNE detec-

tion, as well as in emergency management, alerting, warning, command and control, the situational awareness of authorities and the public warning of private civilians. The articles on hyperspectral technology were produced in two separate research and development projects, of which the *SpeCSI* project was carried out in 2012 and the *SpeCSI Solutions* project in 2013–2014. Of the publications on hyperspectral technology, article **PIII** was written first, and it was produced during the *SpeCSI* project in 2012. The author participated in the research and was in charge of the business development in the project. Article **PIII** focuses on the hyperspectral detection of forensic samples, of which particularly blood, gunshot and primer residues and fingerprints are relevant for CBRNE countermeasures and defence. The article is based on laboratory experiments organized with the police. The author contributed to the article by participating in the selection of the tested samples and the planning of research designs and by constructing and producing the written content as the lead author of the research paper.

Articles **PI, PII** and **PIV** are based on the research conducted during the *SpeCSI Solutions* project in 2013–2014. The author worked in the project as the project manager and as the designer and organizer of empirical research experiments. Article **PI** deals with the hyperspectral detection of pure explosives and explosion residue. Explosion residue was produced through field experiments and measured with pure explosives in the laboratory. The experiments were carried out with the defence forces and police. The author contributed to the article by leading the planning and by organizing the empirical experiments as well as by constructing and producing the written content as the lead author. The detection of explosives and explosion residue is essential for CBRNE countermeasures and defence.

Article **PII** discusses the airborne hyperspectral detection of explosives, blood and CWAs from a mid-lightweight drone. The measuring tests of explosives and blood were carried out as authentic airborne field experiments with a hyperspectral camera mounted on a drone, whereas the detection tests of CWAs were carried out in a specialized laboratory. The experiments were carried out with the police, explosives manufacturer Forcit Ltd. and Verifin. The author led the planning and organizing of the empirical experiments and collated and produced the written article. The airborne detection of explosives, CWAs and blood is extremely important for CBRNE countermeasures and defence.

Article **PIV** discusses the deeper hyperspectral analysis and constitution of blood. The discussed experiments and measurements were carried out in the laboratory. The author led the planning and organizing of the experiments and collated and produced the article as the lead author. The detection and analysis of blood is relevant for CBRNE countermeasures and defence.

Articles **PV** and **PVI** were produced during the *Sapporo* project, which specialized in the research and development of smartphone technology and software in emergency management and warning carried out in 2011–2013. The author worked as the project manager of the project and also designed and or-

ganized the practical experiments within the project. Article **PV** presents the results of the experiments with the developed smartphone-based emergency management, alerting, warning, command and control and situational awareness system for the police force's internal use. The author led the design of the experiments with the police and constructed and wrote the article as the lead author of the paper. The police-tested emergency management activities carried out with the produced smartphone system are necessary for the responsible authorities during the management of actualized emergencies, such as in the management of CBRNE incidents and carrying out CBRNE countermeasures and defence.

Article **PVI** deals with the emergency alerting and warning experiments carried out with the developed smartphone system with civilian organizations and with the private citizens by the police. The author led the design of the experiments and constructed and wrote the article as the lead author of the paper. The tested emergency management and warning activities are necessary for the authorities and civilian organizations during emergencies, including the management of CBRNE incidents and carrying out CBRNE countermeasures and defence.

OTHER PUBLICATIONS AND PUBLIC PRESENTATIONS

During and after the *SpeCSI*, *SpeCSI Solutions* and *Sapporo* projects, also several other scientific articles and international conference presentations were produced. These are listed below together for the hyperspectral and smartphone technology according to their time of publication, newest on top:

1. **Jaana Kuula**. The Changing Nature and Influence of CBRNE Threats. *ISMS International Society of Military Sciences Annual Conference 2016, Warsaw, Poland, 12-14. October,* 2016.
2. **Jaana Kuula**. Smartphone Based Multi-Channel Emergency Alerting. *Latvian Presidency of the Council of the European Union, Workshop on Civil Protection: Workshop on needs of persons with disability throughout disaster management cycle, Riga, Latvia, 12-13. January,* 2015.
3. **Jaana Kuula**. The Hyperspectral Investigation of Fires and Explosions. *The 22nd International Symposium on the Forensic Sciences, Adelaide, Australia, conference presentation, 31. August - 4. September,* 2014
4. **Jaana Kuula**. Enriched Crisis Communication with Smartphones in Escalated Emergencies. *The 5th International Disaster and Risk Conference IDRC, Davos, Switzerland, conference presentation, 24-28. August,* 2014.
5. **Jaana Kuula**. Emergency Alerting with Smartphones. *Critical Communications Europe, Amsterdam, The Netherlands, conference presentation, 11-12. March,* 2014
6. **Jaana Kuula** and Olli Kauppinen. SAPPORO Älypuhelinviestintä Vaaratilanteessa – Tapauskertomus Kemikaalionnettomuuden Pelastusharjoituk-

sesta. *ISSN 2323-4997, ISBN 978-951-39-5573-1, Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisuja 6/2014, 78 s., January*, 2014

7. **Jaana Kuula**, Ilkka Pölönen, Hannu-Heikki Puupponen and Tapani Reinikainen. The Challenge of Using Hyperspectral Imaging in Crime Scene Investigation. *The European Academy of Forensic Science EAFS2012 - Towards Forensic Science 2.0 Conference, The Hague, The Netherlands, conference presentation, 20-24. August,* 2012
8. **Jaana Kuula**, Jonne Räsänen, Pauli Kettunen, Olli Kauppinen and Slava Panasenko. Mobile Emergency Messaging and the Vulnerability of Crisis Communication. *Proceedings of the 8th Symposium of CBRNE Threats, Turku, Finland, 11-14. June,* 2012
9. **Jaana Kuula**, Ilkka Pölönen and Hannu-Heikki Puupponen. Using Hyperspectral Imaging for Detecting Destructive Subjects and Materials. *Proceedings of the 8th Symposium of CBRNE Threats, Turku, Finland, 11-14. June,* 2012
10. **Jaana Kuula**, Markku Häkkinen and Jukka Jalasvuori. The Need for International Harmonization of Emergency Notification Systems: The Case of Finland. *Proceedings of the Global Risk Forum GRF, One Health Summit, Davos, Switzerland, 19-22. February*, 2012

1 INTRODUCTION

1.1 The research environment and background of the study

CBRNE materials, referring to chemical, biological, radioactive, nuclear and explosive substances, form a very serious security and health risk when they are handled in the wrong way. Potential risks may actualize due to various accidents, such as human errors, technical failures or natural disasters, or as a consequence of terroristic and other criminal acts. The worst CBRNE incidents cause large numbers of casualties. Especially nuclear, biological and chemical materials (NBCs) have the capacity to inflict death and destruction on a very large scale, up to thousands and hundreds of thousands people, for which reason they are called weapons of mass destruction, or WMDs (Encyclopedia Britannica, 2014).

CBRNE materials exist and will always remain within society all over the world, making the CBRNE threat permanent. Also, their volume seems to be increasing rather than decreasing. The existence, volume, transportation and increased number of potential users alone maintain the risk, and additional CBRNE disasters have also been caused by nature. In recent years, CBRNE risks have also moved to a new level, where the WMD threat is no longer ruled by governmental actors only but also by organized terrorists. This shift emphasizes the fact that even though particularly CWAs were originally developed to be used in the battlefields only, due to the ruthless behavior and internationally networked organization of terrorists, they are nowadays also a direct risk for civilians.

Because of this permanent, changed and increased nature of CBRNE risk, CBRNE countermeasures also need to be renovated. First, the responsibility, knowledge and facilities of CBRNE countermeasures and defence can not be addressed through military actors' responsibility only, as amongst civilian society the countering of actualized CBRNE threats requires involvement by many different authorities and civilian organizations at all levels. Second, changed and shared responsibilities also require modified operating concepts, which

need to be practiced in the same way as the rescue and defence organizations rehearse their capability of responding immediately to other kinds of emerging threats. Third, CBRNE countermeasures require new technologies and methods. It is not enough that the threat be recognized when it has already been released or when it is too late to prevent the exposure. It is also not satisfactory that the threat agent be identified only after casualties are caused. People also need to be warned and advised efficiently about the threat, independently of whether they are responsible authorities or civilians. Unlike with traditional warning sirens, the usage of today's warning systems should not be limited to merely the point when the threat emerges. Instead, the warning, informing, commanding and counseling of authorities and civilians need to be carried on as long as the immediate threat exists and the direct countermeasures are carried out. These also include the after-care of casualties and other involved people, which may take up to several years after the incident. In addition, when a CBRNE emergency takes place, the situation needs to be assessed frequently, especially concerning the moving and changing of the threat; the operation and condition of the rescuers' operative staff; the condition, number and location of casualties; and the damage to critical infrastructure and other property as well as the resilience of and risk to other people.

This study deals with countermeasures and technical methods in responding to CBRNE threats. This response is called CBRN(E) countermeasures (EDA, 2014) or CBRN(E) defence (ACO, 2015). Within this context, the discussion is limited to key actors, protection methods and technologies without a deeper discourse on the reasons for a possible accident or intentional act. Also, active measures against a possible intruder are not discussed. The research proposes hyperspectral technology and smartphone technology as potential CBRNE protection technologies and aims at finding out whether they can be used for responding to CBRNE threats. The scientific and practical motivation behind studying these two technologies is that they are fast, commercially available "off-the-shelf" and, for the most part, feasible in regard to size and price. They also take in, process and produce digital data and are integrable and compatible with other systems. In addition, both are novel emerging technologies at the growth stage of their lifecycle, with the greatest benefits of their utilization still ahead. In this context, hyperspectral technology can be classified as a detection technology and smartphone technology as an information management and communication technology, especially focusing on alerting, warning and command and control tasks.

1.1.1 CBRNE accidents

The manufacturing, storage and usage of the WMDs are prohibited worldwide by international agreements. This does not, however, guarantee that CBRNE risks or materials capable for mass destruction do not exist. There are plenty of industrial chemicals and explosives and also biological, radioactive and nuclear materials that are being used under strict control for acceptable civilian purposes, which, at the same time, are, however, a potential risk if they are released in

uncontrolled circumstances. For example, road accidents and other transportation risks in the railway, maritime and air cargo industries, human errors, leaks and other technical failures, fires and natural disasters in production premises and warehouses cause a large number of CBRNE accidents all over the world. Very often, economic and material costs in addition to the number of human casualties are high. For example, in one of the recent large-scale CBRNE disasters caused by an accident in a warehouse explosion in Tianjin, China, in August 2015 (Guardian, 2015), warehouses containing 700 tons of highly toxic sodium cyanide, which is a much more hazardous material than had been authorized, were located closer to homes than permitted. In the explosion, 173 people were killed, more than 100 of them being firefighters and police officers. Authorities (Guardian, 2015) sealed all waterways leading out of the blast zone to curb cyanide contamination after noticing that three waste water discharge monitoring stations within the evacuated area showed excessive levels of cyanide, with one station recording a level 27.4 times the normal limit (BBC, 2015c). According to the BBC (2015c), more than 720 people were taken to the hospital, and several thousand people living near the port had to leave their homes. The 700 tons of sodium cyanide at the site is soluble in water, and, when dissolved or burned, it releases the highly poisonous gas hydrogen cyanide. The accident required (BBC, 2015c) more than 1,000 firefighters and more than 200 chemical and biological experts from the military to the scene to contain the fires and to neutralize and dispose of the toxic chemicals.

The worst industrial CBRNE disaster in history took place in a pesticide plant in Bhopal, India in 1984 (Bhopal, 2008). In the accident, an estimated 10,000 or more people died, and about 500,000 more people suffered agonizing injuries with disastrous effects from the massive poisoning caused by 40 tons of the toxic gas Methy-Iso-Cyanate (MIC), which was accidentally released from Union Carbide's Bhopal plant and spread throughout the city (Bhopal, 2008). The technical reason for the tragedy was water within a tank, which led to huge catastrophic consequences. Whether the water got there due to corporate negligence or by sabotage, however, varies depending on the source.

The worst CBRNE accident caused by a natural disaster took place in Japan in 2011 (World Nuclear Association, 2015), when an underwater earthquake near Sendai created a 15-meter tsunami, which then disabled the power supply and cooling mechanism of three Fukushima Daiichi reactors, causing a nuclear accident on March 11, 2011. All three cores largely melted in the first three days, followed by high radioactive releases. Over 100,000 people were evacuated from their homes because of radiation, but no deaths or cases of radiation sickness from the nuclear accident were reported (World Nuclear Association, 2015).

1.1.2 CBRNE attacks

The most serious deliberate CBRNE incidents related to CWAs have recently been the usage of chlorine, sarin and mustard gas in Syria in 2013 and 2015. First, chlorine was claimed to have been used in 2013 and 2015 (Schleifer, 2015),

and the UN has confirmed the usage of sarin in 2013 (Charbonneau and Nichols, 2013). Also, mustard gas is said to have been used in 2015 (Naylor, 2015). The Syrian government, the rebels and ISIS have all been accused of carrying out the attacks, and, irrespective of the offender, all these incidents are extremely serious and most exceptional crimes, especially after the usage of poison gas in World War I (ending in 1918) and World War II (ending in 1945).

The usage of chemical weapons (OPCW, 2015) was prohibited originally by the 1899 Hague Peace Conference and again by global commitment in the 1925 Geneva Protocol, which forbids the use of chemical and biological weapons in war. The Protocol was signed after chemical weapons were used on a massive scale in the battlefield during World War I, resulting in more than 100,000 fatalities and a million casualties. Despite the global agreement, poison gas was used again in World War II in carrying out the Holocaust in the form of Zyclon-B and other gases. After that, sarin was used in 1995 in Japan (Pletcher, 2014; Osaki, 2015), when members of the Japan-based religious movement AUM Shinrikyo released it in Tokyo's subway system, resulting in 13 dead and some 5,000–6,000 injured, of which many are still ill or injured after 20 years. Also, a very rare incident related to toxic chemicals was revealed to police in Finland in January 2014 (Hänninen and Passi, 2014), when a two-person plan to kill around 50 persons with firearms and self-prepared toxic gas at the university premises in Helsinki was exposed. According to the Court of Appeal (Kerkelä, 2014), the two persons arrested had an executable plan ready for the killings and the arms and chemical materials for fulfilling the plan.

Also, biological and radioactive warfare agents have been used against international agreements. The worst biological attacks in U.S. history (FBI, 2015) took place soon after the 9/11 attack on the World Trade Center and Pentagon in September 2001, as anthrax letters were found in government buildings in Washington leading to five persons dying and 17 becoming sick from the toxic bacteria. Accordingly, the most well-known case of using a radioactive agent to kill is the former KGB agent Litvinenko's death from radioactive poisoning in 2006 (Smith-Spark and Black, 2015), which is claimed to have been a murder with polonium-210.

Compared with chemical and biological agents, mass destruction has more often been caused via explosives. Some of these contain military explosives, whereas others are improvised constructions entailing various chemical and other compounds. Explosives are also often used in armed attacks and in spreading other destructive materials. Some of the most serious bombings in recent years on (or under) the ground took place in Brussels, Istanbul and Baghdad in 2016, Ankara and Paris in 2015, Nairobi in 2013, and 10 years earlier in Madrid in 2004 and in London in 2005. In the Westgate shopping mall (Guardian, 2013) in Nairobi, the shooting and bombing with grenades lasted more than three days in September 2013, leaving around 70 people dead. Two years later, in October 2015, two suicide-bombs were exploded in Ankara (Guardian, 2015) in the middle of crowds, killing nearly 100 and injuring almost 200 people. Just one month later, a serious shooting and suicide bombing in

Paris killed 130 and wounded hundreds of people in November 2015 (BBC, 2015f). Five months after that, in April 2016, two bombings in the Brussels airport and metro killed 32 (BBC, 2016), and barely two months thereafter 44 people were killed and more than 230 wounded in a bombing at the Istanbul airport at the end of June (Karimi and Almasy, 2016). In just a couple of days, this was followed by a bomb attack in Baghdad in the beginning of July, quickly killing more than 200 and injuring around 150 people (Tawfeek and Capelouto, 2016). Some weeks later (Choi, 2016), the attack was confirmed as ISIS' deadliest, by killing 292 people. It was also found to have been executed through a new method, a vehicle-borne improvised explosive device (VBIED), where the explosives also differed from those used previously. The new explosive was said to have been a binary bomb compiled of two different chemicals in a vehicle on site. Different from other explosives, it created extreme heat in a precise location, with massive burning effects yet without a significant shock wave or the collapse of buildings. The two earlier bombings in Europe 10 years previous were just as disastrous. The bombing in the commuter train system in Madrid in 2004 (BBC, 2015a) killed nearly 200 and injured more than 1,800 people, while in the London underground in 2005 (HC, 2006) 56 people died and more than 700 were injured.

In regard to air traffic, explosives have been claimed to have caused, for example, the Russian airplane crash in Egypt in 2015 (Topham et al., 2015), the Malaysian airplane crash in Ukraine in 2014 (BBC, 2015b) and the American airplane explosion in Lockerbie, Scotland, in 1988 (History, 2015a). These each caused the deaths of 200–300 people. Also, the 9/11 attacks (History, 2015b) through terrorists hijacking four airplanes and flying two of them into the two towers of the World Trade Center in New York and one into the Pentagon near Washington in 2001 can be seen as attacks with explosive materials, even if there were no particular bombs on the planes. When vehicles with full gasoline tanks are targeted to hit a building they explode and cause similar demolition and burning effects as conventional explosives. The 9/11 attacks (History, 2015b) with airplanes in 2001 caused the deaths of more than 3,000 people.

There are also other examples of strikes with improvised explosive devices (IEDs) or homemade explosives (HMEs) by individuals or groups. Some of the most disastrous bombings of this kind in recent years took place in Boston and Oslo. In the Boston bombing (Boston Marathon, 2015) in April 2013, two brothers exploded two self-made pressure-cooker bombs packed with shrapnel and other materials during the Boston Marathon, killing three and wounding more than 260 people. Accordingly, in Oslo in July 2011, a lone-wolf terrorist referred to the Boston bombing and exploded a homemade fertilizer bomb (Fischer, 2011) near a government building, killing 8 and wounding 89, after which he killed 69 and wounded 62 via shooting (Victim list, 2015).

Figure 1 depicts an overview of global CBRN threats and activity in the summer of 2016 (CBRNeWorld, 2016) and in Figure 2 from a year earlier in the summer of 2015 (CBRNeWorld, 2015). The figures demonstrate that severe

threats and incidents take place all over the world all the time and that there is no indication of their decrease or cessation.

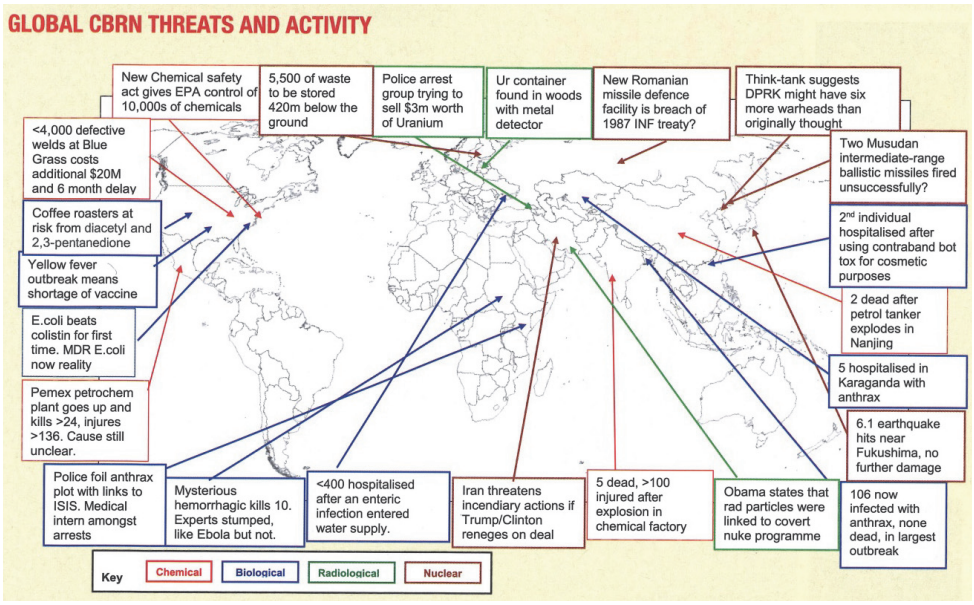


FIGURE 1 Overview of global CBRN threats and activity in the summer of 2016.

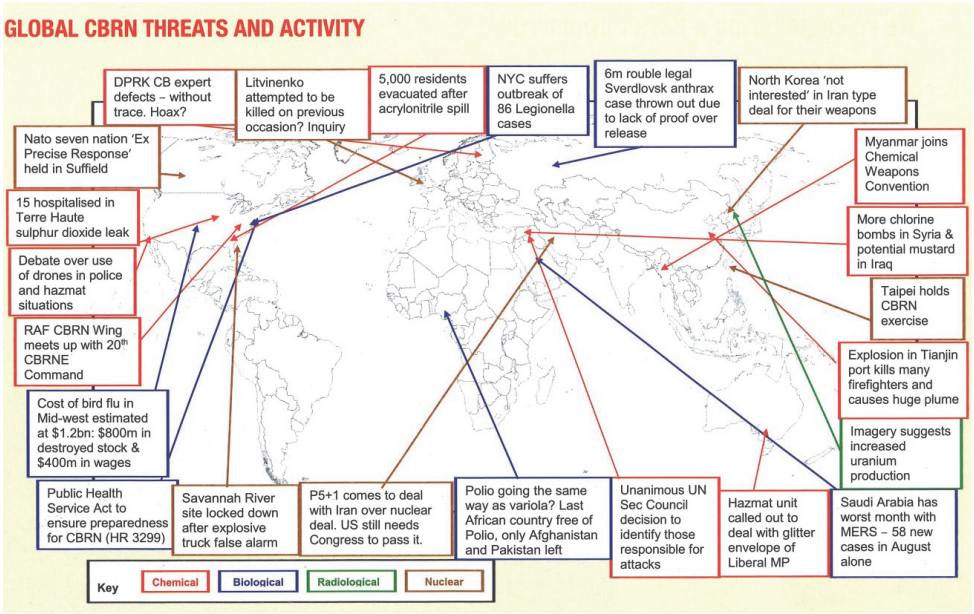


FIGURE 2 Overview of global CBRN threats and activity in the summer of 2015.

1.1.3 The likelihood and costs of CBRNE incidents

The likelihood of both accidental and deliberate CBRNE incidents is related to the availability and volume of source materials, with the level of caution in handling them and with the overall situation and stability of the world and nature. Sometimes the extent of the threat itself may also prevent escalation, such as in the case of nuclear weapons during the Cold War (Salminen, 2015). In war zones, escalating incidents with CBRNE may follow when the ammunitions or fire reach critical industrial sites and warehouses.

The deliberate injurious usage of CBRNE materials has, after the World Wars I and II, focused mainly on terrorism with explosives. Recent examples, political rhetoric and open manifests by various extremists, however, indicate that the likelihood of using chemical, biological and radioactive agents as well as nuclear weapons may have also been increasing. Although some of the past events seem to be individual incidents without clear connections to other events, others are related to wider political, religious or other radical movements, which cause violent occurrences frequently on a national or international basis. Regardless of whether CBRNE materials have been used once for a single purpose or more frequently for a wider cause, all incidents substantiate the fact that CBRNE materials can and are being used practically each year in some part of the world, either by governments, organized radical groups, smaller terrorist bodies, or individual persons. Even if these materials are not directly available, there is often on-hand knowledge of how such materials can be produced. Many source materials can also be obtained quite easily and freely. Fatal plans and the preparation of hazardous materials can therefore not be prevented, and openly reported cases of the use of deliberate CBRNE strikes may encourage and increase interest in them even more.

In all, further CBRNE incidents, even with WMDs, are possible, and the costs of each potential attack will be high. For example, the total cost associated with the decontamination following the 2001 anthrax letters in Washington was, according to Schmitt and Zacchia's analysis (2012), about 320 million USD. Also, higher figures of more than one billion USD have been presented, as the cleaning work in the buildings took more than two years. In a wider study, the researchers of the European Commission funded Network for the Economic Analysis of Terrorism (Ramseger et al., 2009) concluded that the costs of CBRNE disasters are much higher than the costs of prevention and that the costs of biological incidents are much higher than the costs of chemical and radiological events. The researchers report that the assumed possible direct damage from a biological disaster with CHF 2,010 million/year is 10 to 20 times greater than the expected amount of loss for both chemical and radiological incidents. According to the report (Ramseger et al., 2009), the evaluated indirect costs for biological threats range from several billion to tens of billions USD, whereas countermeasure costs are smaller, ranging from the hundreds of millions to about 10 billion USD. The report also gives even higher figures for the

indirect costs of pandemic incidents, for example, the estimated 4.4 trillion USD (11% of the global GDP) for a pandemic influenza.

The expenditure in countermeasures differs greatly by country. For example, the expenditure on bio defence programs alone (Ramseger et al., 2009) in European countries is from a few hundred thousand to tens of millions euros for a reference year and in the USA about 200 million euros. The same researchers also point out that in this area there is often overlap with goals not related to the prevention of or protection against CBRN terror, in particular regarding efforts of increasing general security in the chemical industry. They also note that for some CBRNE protection activities, CBRN terror is only a minor aspect, as the major objective in the destruction of chemical weapons is disarmament, and investments in this, at the same time, prevent the access of chemical weapons by terrorists.

1.1.4 The authorities' role

In the most serious scenarios, CBRNE incidents cause very large numbers of casualties and huge material destruction. Frequent incidents also have the risk of escalation and the spreading of contamination to new areas and people. The management of these kinds of large-scale devastations require pre-planned and rehearsed operating concepts, for which best knowledge, experience and practice is provided by large security and military organizations such as the North Atlantic Treaty Organization (NATO) and the European Defence Agency (EDA). Both of these multinational security agencies have created their own CBRNE countermeasures operating concepts, which individual member states can apply according their own country's policies and rules. For example, Canada (DND/CF, 2012) has produced its own national CBRNE defence model related to NATO's operating concept, whereas the non-NATO member state Finland regards in its own CBRNE strategy the guidelines of the EDA.

The CBRNE countermeasures and defence operating concepts define the capability requirements that security authorities need to produce during a massive CBRNE incident. Referring to the Canadian CBRNE defense operating concept (DND/CF, 2012) and the outline of the EDA's CBRNE countermeasures concept (EDA, 2014), some of the required capabilities are related to physical activities, such as protection and hazard management, limiting CBRN contamination, decontamination and providing medical countermeasures and support to exposed persons. Another part of the capabilities are functions that operate with non-material assets by assessing, transferring and processing information and data in various forms. These functions also include technical devices for carrying out the needed tasks, but the critical substances delivered and exchanged are immaterial. Capability requirements related to these immaterial functions include particularly detection, identification and monitoring activities; CBRNE assessment and intelligence; information management and CBRNE warning and reachback. Both physical and immaterial capabilities are critical for accomplishing the CBRNE countermeasure operations, and neither of them can fully succeed without another.

In individual countries, CBRNE incidents, whether they are emerged threats, accidents, attacks or planned strikes, always require authorities' investigation and involvement. The most extensive and complicated situations may also require joint operations by many authorities. Detailed operating procedures may vary in different countries, and authorities may have different roles, especially between peacetime and wartime operations. Also, the location of the incident and the environment where the harmful materials are found define which authorities are involved in the incident and in which roles. Responsibilities may also be divided between different authorities depending on whether the emerged CBRNE threat is caused by chemical, biological, radioactive, nuclear or explosive matters.

In Finland, the responsible authority in peacetime CBRNE incidents is primarily the police. It is also possible that in actualized incidents the fire and rescue service is the first authority at the location by starting the rescue operation. At that time, the effecting agent may not necessarily be known, and it may also be unclear whether the incident is caused by an accident or crime. If the police or fire and rescue service need additional resources, the defence forces can also be called for help. CBRNE incidents can also be started by the appearance of illicit materials at the border or in the air. In these cases, additional authorities such as the border guard, customs authorities or radiation and nuclear safety authorities are involved in the case. Also, the health authorities may be engaged in managing the CBRNE threat and risk, especially when it is caused by biological agents.

In Finland, joint operations between authorities is obligated by law, and it usually works without problems, as can be witnessed publicly by various joint operation rehearsals and real-life situations where different authorities have worked together. Typical multi-authority operations, for example, are related to search and rescue operations, heavy storms and other natural disasters and forest and ground fires as well as with large-scale industrial accidents. Quite recently, in 2015, a joint operation was also needed for managing the overwhelming immigration at the ground borders of the country.

1.1.5 Detecting the threat

In the conduction of CBRNE countermeasures and defence, there are many different technologies available for carrying out, for example, detection and identification activities. Depending on whether the threat is caused by chemical, biological, radioactive, nuclear or explosive matters, different technologies and applications need to be used. Alternative technologies may also be needed for detecting the same substance, for example a chemical agent, at the different stages of the CBRNE incident before or after the incident is actualized.

When detection is being conducted to deter or prevent a CBRNE incident before it has realized, various remote sensing technologies are used, especially for detecting threats spread by the air, ground or open water. Remote sensing is usually carried out from satellites, helicopters and airplanes; fixed or mobile ground stations; maritime vessels or various unmanned vehicles. Pre-blast de-

tection can also be done at a close range, for example, if an undefined package has been found in a critical place and there is reason to suspect that it contains a CBRNE threat.

Actualized CBRNE threats can sometimes also be detected from long distance, but when the rescue operation is to be started at the site, rescuers need to know the exact identification, location, volume and concentration of the agent. At this stage, detection needs to be made at relatively short range, and, to minimize the contamination risk for rescuers, ideally no human should enter the location. Instead, automated or remotely operated devices, such as robots capable of carrying out the detection tasks, should be sent to the location. To minimize further escalation and contamination risks, and to protect forensic evidence, detection should in principle be carried out without touching the threat source at all, including that no physical sample be taken from the source or from anything else at the location, even though most of the current CBRNE detection, identification and investigation methods are based on taking samples. For example, the operation of many gas and biological detectors is based on inducing and collecting richened air in some kind of chamber, where it will be examined with various treatment and analysis methods. Also, many other chemical detectors are based on taking a sample of solid or liquid materials and on processing the sample in different ways to determine the chemical structure and content of the sample. All these methods require touching and intruding upon or breaking the target to obtain a sample. The sample may also need to be treated with some active method, such as radiation or fuming to reveal its characteristic features.

During and after the rescue operation, detection is also needed for forensic investigation and to support decontamination and cleaning. In addition, further detection procedures may in some cases support the treatment of patients if the initial information about the threat agent is inadequate and if additional information is needed to enable better medical help.

1.1.6 Managing the incident and warning people

Capability requirements for CBRNE defence and countermeasures also include management and information management activities and, within these, command and control, situational awareness and warning functions. These can be produced through many different technologies, such as CBRNE detection, as long as the common user interfaces of the technical systems at the reachback center are homogeneous. For example, the warning and command and control activities can be carried out in principle in the same way, irrespective of whether the threat is caused by chemical, biological, radioactive, nuclear or explosive matters. Also, the situational awareness may be presented at a certain level with the same methods, independent from the type of threat. The data behind the presentations will, however, be produced via different technologies and in different forms depending on the threat and the type of sensor that is being used. Various CBRNE detectors may indicate, for example, the presence or various qualities of solid, liquid and gaseous chemicals; microscopically small quanti-

ties of bacteria, radioactive or nuclear radiation; microscopically small particles of explosion residue or ammunition or containers or other types of equipment, vessels, laboratories and warehouses for spreading, transporting, producing or storing harmful materials. As the form and scale of many of the detected targets can be vary widely, it is difficult to visualize them all in the same way. As a result, various presentation techniques are needed even when all incoming data from the various sensors are received in digital form.

The command and control, situational awareness and warning activities are often performed with the authorities' internal specialized equipment and systems. They are built for authorities' own use only, which means that, with these systems, for example, CBRNE warnings can be given only for the authorities and not for civilians, whom the rescue and defence forces should protect. The authorities have other media for giving public warnings to private citizens, though. Communication with the citizenry may, however, be multi-staged and complicated, starting from the point when the CBRNE threat is detected through to the point when the warnings are given. Due to this communication process, it may take tens of minutes or several hours until all people are warned, which is too long considering how quickly and seriously CBRNE threats affect people. It is also possible that public warnings may be given with media that not all people can understand, access or notice or which that ignore or notice so late that the warnings are no longer useful.

The most common warning methods around the world have traditionally been mechanical and electronic sirens or certain kinds of voice signals. Over the last decades, warning notices have been given on the radio and television. Not all sirens, however, reach all people or give critical information regarding the type and exact location of the threat. The siren type of alerts may also be misunderstood, as people may not know whether they are a rehearsal or a real warning. In addition, sirens cannot indicate to people what they should do to protect themselves. Also, warnings given via radio and television do not reach the entire population, because people are not listening/watching radio and television at all times or because not all people have such devices. In Finland more households (99%) have mobile phones (SVT, 2015) than those who (95%) have televisions (Finnpanel, 2015). Unlike televisions and radios, mobile phones are personal devices and are almost always on. People also usually carry their phones with them all the time, whereas televisions and radios are mostly space-dependent devices that are accessed only part of the time and only in those places where they are installed, for example, at home, at the office or in one's car.

In recent years, many countries have started giving public emergency alert messages via mobile phones. Despite the high adoption rate of mobile phone devices, this is, however, not as common as one might expect. For example, in continental Europe it has not been adopted as widespread as in the Scandinavian countries and the UK. In giving mobile warnings, there are basically three competing technologies, of which short messaging service (SMS) is the oldest and simplest messaging technology. Compared with other technologies, its

communicative features are quite limited, and delivery costs in mass deliveries are relatively high. As an advantage, SMS operates on all mobile phone types, operating systems and telecommunication networks all over the world. The standardization of SMS (Hillebrandt, 2010) started in February 1985 as a part of the creation of the second generation digital cellular system, the Global System for Mobile Communications (GSM). In some countries, public warnings are also given through the cell broadcasting service, which was demonstrated in Paris for the first time in 1997 (Medlibrary, 2015). Cell broadcasting is faster than SMS but requires an additional nationwide infrastructure for mobile phone base stations. This does not exist in all countries. Building a new broadcasting infrastructure creates additional costs, and, depending on the technical features of the handset, messages cannot be received through all mobile phones. Whereas SMS messages are sent via the point-to-point method, cell broadcast messages are sent in point-to-area form. This is an unconfirmed push service, meaning that the originator of the message does not know who has received the message (Cellbroadcastforum, 2009). This also means that cell broadcasting is not an interactive communication method and that the authorities who use this technology for emergency alerting purposes cannot obtain reachback information from the emergency areas.

As a third alternative, public emergency alerts can be given to people through the push notification feature of smartphone technology, which is a more flexible communication method than the other two. The push notification method has been enabled since the earliest versions of the Android operating system (Verge, 2011), whose first commercial version was launched in 2008. Push notification (Rouse and Steele, 2014), also called server push notification, is the delivery of information from a software application to a computing device without a specific request from the client. The end-user must give an opt-in command (BusinessDictionary, 2015) to the sender for permission to send alerts, which usually takes place during the installation process. One important advantage of push notifications in mobile computing is that the technology does not require specific applications on a mobile device to be open for a message to be received. This allows a smartphone to receive and display alerts even when the device's screen is locked, and the application that is pushing the notification is closed (Rouse and Steele, 2014).

In regard to public emergency alerts, the push notification method is relatively cheap, as it does not require any additional telecommunication infrastructure for mobile communication base stations or specialized handsets for the users. Messages can be received and responded to with ordinary smartphone devices, which most people have anyway. Such commercial off-the-shelf (COTS) devices also offer an advantage to the authorities, and the delivery of warning messages to the masses is expected to be cheaper than sending them with SMS. Pricing policies may, though, vary in different countries and by different commercial service providers. Authorities can also form a situational picture of the emergency area and the people within or of their own staff or other resources with smartphone technology. The same technology can also be implemented in

such a form that it will send the same emergency alerts to other media, such as television and radio, social media and selected electronic bulletin boards, in addition to private citizens. Compared with SMS and cell broadcast, the advantages of smartphone messaging are its superior flexibility, interactivity, multi-channel transmission and other specific technical features.

In recent years, social media, which is a software application and not a technology, has also become popular in many areas of life, including during emergencies. In such use social media, however, is problematic, because not all people use it and because it contains a good deal of unconfirmed information and rumors. Rescue and safety alerts and advice should always be confirmed and true, and such information can only be received from authorized security organizations, such as the police, fire and rescue service, defence forces or health authorities.

1.2 The objectives and scope of the study

The objective of the study is to explore whether hyperspectral technology and smartphone technology are applicable in the field operations of the CBRNE countermeasures and defence in security authorities' single and joint operations. The discussed CBRNE incidents may be caused accidentally by humans or by nature or alternatively by a terroristic or other hostile attack within the homeland or another signed target. The study is focused on researching through practical experiments whether the two novel techniques, hyperspectral technology and smartphone technology, can support the acknowledged CBRNE countermeasure and defence operating concepts of NATO, EDA, Canada and Finland in countering CBRNE threats. The study covers the whole crisis management life cycle and CBRNE incident timeline by evaluating whether the two technologies can support preventive measures before a given CBRNE incident has actualized as well as support rescue and recovery activities after the CBRNE incident has already taken place.

The capability of the two technologies is tested in the study through several practical experiments carried out in tailored research designs with various CBRNE materials together with representatives of the police, defence forces and fire and rescue service. The research is directed primarily at capability requirements, which are related to the non-physical/immaterial functions of CBRNE detection, identification and monitoring; CBRNE assessment and intelligence; information management; CBRNE warning and reachback.

Hyperspectral technology refers in this context to 1) optoelectronic sensors and imaging devices, 2) software that analyses the data produced by hyperspectral imaging devices 3) other possible software and devices needed for producing hyperspectral imaging data and their analysis results. Hyperspectral imaging devices are also referred to as hyperspectral cameras. Smartphone technology refers here to 1) new generation mobile phones that have sophisticated programmable functionalities in the handset, 2) high-speed mobile 3G, LTE, 4G or newer broad-

band connection and 3) possible other smart built-in mechanisms such as digital cameras and video cameras, vibration and motion sensor mechanisms. In this context, smartphone technology also refers to 4) high-speed mobile broadband networks, 5) satellite connections, 6) WLAN wireless local area networks, 7) ad-hoc mobile networks, 8) mobile peer-to-peer data transmission and 9) other possible data transfer techniques that can be used for enabling the usage of smartphones in any given place. In addition, smartphone technology includes here 10) software applications, created to make smartphone devices usable for any given desired purpose and to make the devices function in a certain situation as desired.

The empirical research on how hyperspectral technology and smartphone technology can enable fulfilling the non-physical capability requirements of the CBRNE countermeasure and defence operating concepts is performed in the study through various practical experiments. The experiments were designed by the author at the Department of Mathematical Information Technology at the University of Jyväskylä and executed with the responsible authority's permission and with technical assistance from the Central Finland Police Department, National Bureau of Investigation, Police Board and some other units of the Finnish Police, Air Force Command of the Finnish Defence Forces, Rescue Department of Central Finland, Verifin and the leading Finnish explosives manufacturing company, Forcit. In the experiments, the two technologies are tested with particular handwritten research designs, where each experiment has its own research questions and technical setups.

During the research, altogether eight separate hyperspectral cameras and five different types of smartphones were used in various research designs. In the practical research projects carried out to enable this academic research, various software and algorithms have also been created and tested to find out the two technologies' technical capability to fulfill the functional requirements defined for the threat detection and incident management activities in CBRNE countermeasures. Separate analysis software and algorithms were produced for the hyperspectral analysis and for mobile emergency alerting and crisis management. The technical creation and testing processes of the software are not reported in this study, since the research interest is here focused on experimenting with wider systems, which the hyperspectral and smartphone technologies form together with the tailored software produced for this purpose in individual research and development projects.

The hyperspectral technology tests were carried out with tens of different CBRNE matters as pure substances and with more than one hundred variations of different substances on different matrices. The primary focus was on testing the detection of various CBRNE substances in solid, liquid and gaseous forms with different hyperspectral cameras from various distances in different setups. The tests included various laboratory assessments and field experiments carried out in outdoor conditions. The laboratory tests were carried out before the field experiments to control the testing process. The two most important field experiments were 1) the explosion tests, which were carried out together with the Central Finland Police Department and the Finnish Air Force Command in win-

ter conditions at an outdoor test area of the Defence Forces and 2) the airborne hyperspectral detection tests of explosives, which were carried out with an unmanned aerial vehicle (UAV) in summer conditions with the Central Finland Police Department and explosives manufacturer, Forcit, Vihtavuori plant. Of the hyperspectral laboratory tests, the most important were the toxic chemicals tests, including tests with CWAs with Verifin in Helsinki. Also, extremely valuable were the numerous hyperspectral laboratory tests with various crime scene details with the Central Finland Police Department and National Bureau of Investigation, especially those focusing on blood and other biofluids, shooting and gunshot residues, tear gas and other forensic marks.

The majority of the smartphone tests were carried out with two of the newest types of smartphones at that time, Sony Xperia Go and HTC Explorer, and, in some tests, with some additional mobile phone brands. All tested phones had an Android operating system and each had a similar commercial service subscription in one of the three leading Finnish telecommunication operators' 3G or 4G networks, which are Elisa, Sonera and DNA. The focus of the smartphone experiments was in testing the alerting, warning, command and control, situational awareness, communication, scalability, interactivity, traceability and lead time capabilities of smartphone technology in various situations and research setups. The most essential of these were 1) the police authority's internal tests with the Central Finland Police Department, Police Board and eight police departments in Helsinki, Espoo, Tampere, Jyväskylä, Joensuu, Vaasa, Kuopio and Oulu and 2) the police authority's external tests with the Central Finland Police Department and a test group of volunteer private citizens in Jyväskylä and some other locations around the country. In these tests, all the alerting, warning, command and control, situational awareness, communication, scalability, interactivity, traceability and lead time capabilities of the smartphones were tested with the specifically created software system for the first time ever, both in the authorities' internal communication and in the communication between the authorities and private citizens.

After completing these experiments, the authorities' crisis communication with non-authority organizations was tested in a rescue rehearsal and experiment involving a toxic chemical release at the Department of Chemistry of the University of Jyväskylä and in various test setups of school violence with the Kilpinen School of the City of Jyväskylä. The experiment of a toxic chemical release was carried out with the Rescue Department of Central Finland and the Department of Chemistry and University Communications unit of the University of Jyväskylä. In the experiment, smartphones were used for warning employees of the ammonia release in one of the university buildings. Mobile warnings were given in the same experiment in two ways, with the specifically created push notification-based smartphone application and with SMS. The performance of the two methods was then compared, for example, by the lead time of the emergency messages.

Warning messages were transmitted in the experiment by the crisis communication team of the university, and they were directed inside the university

only, not to other people outside the university nearby. Within the same test, the automated alerting was also tested by simulating the combined automated detection of a toxic chemical and automated alerting for the leak with the created smartphone system. Special interest was also paid to the interactive features of the smartphone system by analyzing how the feedback communication from the casualties in the emergency area fit with the existing rescue and crisis communication processes of the fire and rescue service. Also, in the other experiment with a civilian organization in the Kilpinen school, smartphone warnings were given only within that specific organization, except when a private security company was called for help at the school. If the police are needed, that is done by calling 112. In this experiment, various detection and alert systems were also tested, and a digital map of the school was made and integrated with the mobile alerting system.

As a part of the experiments, a tabletop rehearsal was also carried out to evaluate how the hyperspectral technology and smartphone technology would have been able to support the CBRNE rescue operation in a real explosion threat situation at an explosives manufacturing plant in July 2013. In addition, the harmonization and scalability of mobile alerting and warning in an international context and the vulnerability of wireless and mobile networks were evaluated at a conceptual level as part of the experiments of the study.

1.3 The research problem and the specified research questions

The research problem in the study is whether hyperspectral technology and smartphone technology are capable of supporting the field operations of CBRNE countermeasures and CBRNE defence in the security authorities' single and joint operations. (Further in the text the concepts of CBRNE countermeasures and CBRNE defence are used to refer to more or less same kind of activities in CBRNE protection, and they are also written in the text in form CBRNE countermeasures and defence.)

The research problem is formulated as the main research question as follows:

Can hyperspectral technology and smartphone technology be used for CBRNE countermeasures and defence?

To understand the motivation and formulation of this question and to be able to contemplate it, one must be familiar with both the information technology field and the security field. Within these two fields, one must also have knowledge of three special sectors, which are hyperspectral technology and smartphone technology in the information technology field and CBRNE protection in the security field. In addition, one must be able to realize how these two different technologies are connected with CBRNE protection. With this knowledge, one can understand why these three topics are connected within

the same study and why the two technologies are discussed within the same research question, even though they are different from their ground.

In the security field in regard to CBRNE protection, the main issue is how CBRNE incidents can be avoided and how people, the environment and property can be protected against CBRNE exposure. Some of the activities in this issue are focused on pre-incident/pre-blast measures, which tend to prevent all kinds of CBRNE incidents from taking place in the first place. Other activities include post-incident/post-blast measures, which are required when chemical, biological, radioactive, nuclear or explosive types of destructive materials have already been released into the environment, causing extensive human and material damage and the possible risk of spreading the contamination to a broader area. Post-blast activities include, for example, eliminating and containing the source of the contagious material, taking care of casualties, preventing the spread of contamination, protecting other people and areas and handling the recovery and cleaning of contaminated areas as well as conducting a forensic investigation of a possible crime. These issues belong within the realm of the security authorities' responsibility, which during peacetime include the police, fire and rescue service, other special agencies and the selected responsible ministries, such as the ministry of the interior. Accordingly, during a state of war, the defence forces have a special role in these issues. However, as CBRNE threats are very serious and complicated matters, the management of large-scale CBRNE incidents requires the involvement and joint operation of all the above-named authorities, including many others who are not mentioned by name in the list. Such incidents may also require the involvement of the defence forces during peacetime, not only during times of war. All these activities are covered in the civilian sector in the responsibility area of CBRNE countermeasures and in the military sector as a part of CBRNE defence.

From a technological point of view, CBRNE countermeasures and defence require many different technologies for carrying out different tasks. Many of the required tasks, such as building shelters as a precaution as well as clearing damaged areas, medicating victims and decontaminating people, buildings and the environment, are mainly physical activities carried out manually or with the assistance of mechanical devices. These kinds of physical tasks, or their main functions, cannot be carried out with information technology, although many devices such as bulldozers may contain embedded digital equipment and software. However, there are also tasks that do not require physical force and that are carried out with finer electronic devices. Such tasks are, for example, the detection of the CBRNE threat and the management of the CBRNE incident.

The detection of the CBRNE threat is carried out with specialized detection equipment that is capable of detecting and identifying different substances, such as toxic chemical agents. Such detection and identification of substances cannot be done with ordinary information technology but rather requires various sensors. As the operation of hyperspectral technology is based on detecting and identifying different structures, materials and substances on the basis of how they react on different wavelengths of light, hyperspectral technology is

studied in this research as a potential technology able to detect CBRNE materials. One should also note that even though hyperspectral technology constitutes optoelectronics, it produces its detection result in digital form, which needs to be processed and analyzed with specialized software. This software and all the processing of the digital data produced by the hyperspectral imaging and detection devices are clearly components of the information technology field. In this context, the information technology field is defined as covering information technological devices and information software and systems as well as data transfer and telecommunications.

The management side of the CBRNE incident is comprised of several subtasks, which all contain various information processing and communication tasks. Examples of these are the command and control of the operative forces that are carrying out the rescue operation on the CBRNE site; warning the civilian population of the threat; informing reinforcement, hospitals and other authorities of the situation and the possible need for help and forming and updating a situation picture of the incident and of the whole operation. On the authorities' side, most of subtasks are usually carried out with specialized handsets, peripherals and systems that are dedicated for the authorities' use only and protected from other unauthorized access from outside. The maintenance of such dedicated devices and systems is expensive, and it is often recommended that authorities replace at least some of them with COTS devices where possible. In these kinds of situations, where authorities should in addition to their mutual internal communication also be able to communicate directly with the civilians, especially for warning the population of a lethal threat, dedicated devices designed and authorized for the authorities' use only do not work. For these reasons, smartphone technology is studied in this research as a potential to for carrying out some of the information management tasks required as a part of conducting CBRNE countermeasures and defence.

To answer the main research question, it is discussed and tested in the study through separate sub-questions for hyperspectral technology and for smartphone technology. These are presented and explained below. The relevance of the main research question and all sub-questions for CBRNE countermeasures and defence is confirmed further in the text in chapters 3.2.1 – 3.2.3, where the results of each sub-question are presented in separate tables and text. The tables show at first for each sub-question, which of the individual capability requirements in the referred military and civilian operating concepts for CBRNE countermeasures and defence are related with that particular research question. In addition, the tables and text represent, how the individual research questions and the related capability requirements of the operating concepts are supported and fulfilled by the empirical experiment results, that are gained through the tests that are carried out with the police, defence forces and rescue service as a part of this study.

The sub-questions for hyperspectral technology are as follows:

HQ1. Can CBRNE substances be detected with hyperspectral technology in indoor conditions?

In the study, hyperspectral technology falls under the umbrella of detection technologies, which in this context and in the real user environment should be able to detect CBRNE substances especially in field conditions. To study hyperspectral technology's capability of detecting CBRNE substances in uncontrolled field environments, its performance should, according to a commonly approved research procedure, be at first tested and verified in a controlled laboratory environment. Only successful detection results in the laboratory give a grounded reason to carry on testing in the field conditions, although successful results in the laboratory do not ensure that detection will also be successful in the field environment. In this case, as CBRNE substances are highly toxic and lethal for humans, laboratory tests testing with simulants and the verification of the performance of the detection device in the laboratory are required, because the real substances cannot be released in the normal environment.

HQ2. Can CBRNE substances be detected with hyperspectral technology in outdoor field conditions?

To verify hyperspectral technology's capability of detecting CBRNE substances in the field environment, the technology should be tested in conditions that correspond with the circumstances of a real outdoor user environment and situation. In outdoor circumstances, environmental conditions cannot be controlled, and with a CBRNE situation particularly, the weather and ground materials affect both the CBRNE substances and the performance of the hyperspectral detection device. In addition, the weather affects the operating platform on which the hyperspectral device is being used. For example, with toxic chemicals, the weather affects the vaporization, degradation and spreading of the agent, which in turn all have an effect on how well and with which method the agent can be detected. The weather also affects the hyperspectral device, whose performance is particularly sensitive to the qualities of the light. In addition, in highly toxic environments, detecting devices are often operated with robotized or other unmanned platforms, which are also sensitive to weather conditions. For example, wind and rain may particularly disrupt the operation of lightweight, unmanned airborne operating platforms. Field experiments are therefore needed to define the technical specifications for carrying out CBRNE detection with hyperspectral technology in outdoor conditions and to have evidence of successful detection results in practice.

HQ3. Can hyperspectral detection technology be utilized at the different stages of the timeline of a CBRNE incident?

CBRNE detection as a part of CBRNE countermeasures and defence is not a single event that needs to be performed only once during a CBRNE incident. Instead, detection is needed many times at the different stages of the timeline of

the CBRNE incident, starting from the point when the incident has not yet even happened. In the case of deliberate offences, traces of the preparation of an attack with CBRNE materials should be detected as early as possible to be able to prevent it. At the different stages of the timeline, the situations and environmental conditions vary, so the detection needs to be carried out in a different way. In some situations, for example, a long-distance detection from the ground to the air is useful, while in some other cases, detection needs to be carried out from the air to the ground. Sometimes long-distance detection cannot be used at all, and a close range observation is needed instead. In the course of time and due to environmental factors, CBRNE materials may also change their form, so they may require different kinds of detection at the different stages of the timeline. It is an advantage if the detection technology can be used at the different stages of the timeline and in many different environments and situations. However, the technology may also be useful if it is capable of detecting CBRNE materials in only certain situations, especially if the alternative technologies are not sufficient for that purpose. For example, most of the current detection technologies for chemical agents are specialized in detecting chemicals in a gaseous or vaporized form, whereas additional technologies may be needed for the detection of CBRNE substances in a non-vaporized form.

The sub-questions for smartphone technology are as follows:

SQ1: Can mass alerts, warnings and command and control activities be issued with smartphone technology?

During a CBRNE incident and many other emergencies, authorities need to give alerts, commands, warnings, control messages and other notifications to the operative forces as well as to other authorities and other involved organizations to manage the crisis. They also need to warn private citizens about the threat. Usually different technologies are used to carry out communication with other authorities versus that with private citizens. Communication with authorities is carried out mainly with dedicated technologies and systems, and it is protected from access by private citizens. For private citizens, communication, including giving emergency warnings, is carried out primarily through public media. For emergency warnings, other technologies are also used. For example, mechanical sirens have been in use for a long time worldwide, and nowadays warnings on mobile phones are also being used.

Concerning CBRNE threats and other large-scale emergencies, one may ask whether it would be possible, economical and in other ways more reasonable for authorities to use similar technologies and systems for communication with other authorities and private citizens. One can also ask whether the current methods for warning people are sufficient and sophisticated enough. In this research, the usability of smartphones during emergencies is studied both in regard to the authorities' as well as private citizens' use. For private citizens, the usage is studied primarily from the perspective of whether the authorities can issue emergency warnings on their personal phones.

In regard to information technology, the issuance of emergency alerts, warnings, command and control messages and other notifications is technically quite similar among tasks. Therefore, from a technological point of view, there is in principle no difference as to whether the content of the message is a command or warning or whether the recipient of the message is an authority or a civilian as long as the authorities' own communication is protected from unauthorized use. For these reasons, smartphones should be able to be employed as "dual use," for both authorities and private citizens in CBRNE emergencies, and be operable for giving alerts, warnings, commands and control messages and other notifications regardless of whether recipients are authorities or private citizens.

SQ2: Can the intensity of alerting be adjusted with smartphone technology?

When alerts, warnings and other emergency communications are carried out with technical methods, the recipient's recognition and understanding of the message depends on the technical device with which the message is sent. For example, the sound of public emergency sirens can be heard only within a short range, and the information content of its sound signal without words is extremely limited. With the siren, it is, for example, impossible to tell clearly if the threat is a CBRNE emergency. The emergency messages given via radio and television can be heard and seen only near the receiver, which is often located at a fixed place, such as home. Emergency messages are also delivered through these channels in a standardized format, which often cannot be easily changed for a single message. Mobile phones are almost always available to users. However, the voice signal of the incoming message may not always be noticed and heard, and the urgency of the emergency messages may not be initially distinguished from among the other messages. It is also not possible for the sender to prioritize and intensify the message, such as SMS messages according to their urgency, so that the most urgent messages would be noticed immediately and understood better.

In this study, empirical tests are carried out to test whether the recipients' recognition and understanding of emergency messages can be influenced by the sender through smartphone technology according to the urgency of the message.

SQ3: Can mass alerts, warnings, command and control and other notifications be focused and scaled geographically and according to different recipient groups with smartphone technology?

Emergency communication via radio and television is often criticized for its weak scalability. Especially local emergency warnings given via a national broadcasting network are criticized for being sent to other parts of the country where messages are received unnecessarily. Moreover, the localization of emergency communication through regional broadcasting stations seems to be problematic. Similarly, the localization of SMS message emergency notifications on mobile phones seems to be complicated and slow. Delivering an SMS warning message to people's phones within one city may take several hours, which is too slow for CBRNE emergencies. In this study, the geographical localization

and scaling of emergency messages as well as the delivery of messages through profiled recipient groups are tested with smartphone technology.

SQ4: Can mass alerts, warnings and command and control functions be carried out interactively with smartphone technology?

Emergency warnings and notifications are usually anonymous one-way messages that cannot be replied to, including, for example, public warnings that are given via television and radio or as a cell broadcasting message to mobile phones. The delivery of one-way broadcasting messages is relatively fast, but with this method no information can be received back from the emergency area. However, in many situations, such as CBRNE emergencies, feedback information from the emergency-affected area is extremely important. In this study, interactive emergency messaging is tested with smartphones both in the authorities' internal use as well as in authorities' communication with private citizens.

SQ5: Can situational awareness and a common operating picture be supported or created with smartphone technology?

While managing a CBRNE incident or other emergency, it is extremely valuable to sustain situational awareness and a common operating picture, such as about the operative forces, reinforcement, victims and other endangered people in the emergency area. Such data can be collected, for example, through interactive devices that can automatically deliver essential information to the command of the operation or that people can use to personally report critical issues. In this study, smartphones' ability to return feedback and situational information to the command center is tested through empirical tests.

SQ6: Can the course of the operation be recorded and traced with smartphone technology?

It is important during the emergency that the course of the operation can be analyzed and traced for each person participating in the operation in a rescuer's role. To enable this, the operation of each person needs to be recorded and traced through an appropriate method. In this study, the recording, tracing and analysis of the course of the operation using smartphones is tested in empirical tests.

SQ7: Can mass alerts, warnings and command and control functions be integrated with other technologies and systems, such as detectors, sensors and digital maps, using smartphone technology?

In emergency management, practically all technologies and systems need to be integrated under the same digital command structure, and only few devices and systems are used independently from other emergency systems. In CBRNE situations, it is also important, for example, that stand-alone chemical,

biological and radiological sensors give automatic warnings of exceptional findings. Within large and complex buildings, it is also useful for the rescue operations to have a digital floor map available. If there is also an internal emergency management system for the building, it would be useful to have it linked with the digital floor map. In this study, the integrability of a smartphone-based emergency communication system with digital sensors and floor maps of buildings is tested through empirical tests.

SQ8: Can long-term health monitoring and other crisis follow-up be conducted with smartphone technology?

Serious events such as CBRNE incidents may easily get prolonged, and the involved people's resilience and physical and mental health need to be monitored during the acute stage of the emergency and possibly for a long time afterwards. Follow-up and counseling may be needed both for the rescuers and for the civilians who are involved in the emergency. In this study, the follow-up features of smartphone are tested in empirical tests.

1.4 The research approach and applied methods

1.4.1 The research approach

In the study, the research problem is examined with a dual approach by researching it simultaneously with a top-down approach from the perspective of security sciences and with a bottom-up approach from an information technology perspective. The overall result and contribution of the study are created as a result of the two research processes and with the more detailed results produced in each of the two processes. The dual research approach is illustrated in Figure 3.

In Figure 3, the security sciences cover the forensic and military sciences as well as the protection and rescue disciplines. These scientific fields form the research framework for the study, focusing on crime scene investigation, CBRNE countermeasures and crisis management and warning. All these activities describe different security authority sectors' work, which in the area of CBRNE have similarities in spite of whether the responsible authority is the police, defence forces, fire and rescue service, or the crime battle unit of the customs or border guard. They all investigate and counter some kind of unwanted incident, object or other target causing a serious security threat to the people and environment or one that has already actualized with a various number of casualties and material damage. The investigated incident, object or target can also be related to some other event, with the possibility for escalation and the spread of contamination to additional areas and people, including the rescuers who are working to resolve the case. The incident may be caused accidentally by humans or nature or by some people's deliberate act.

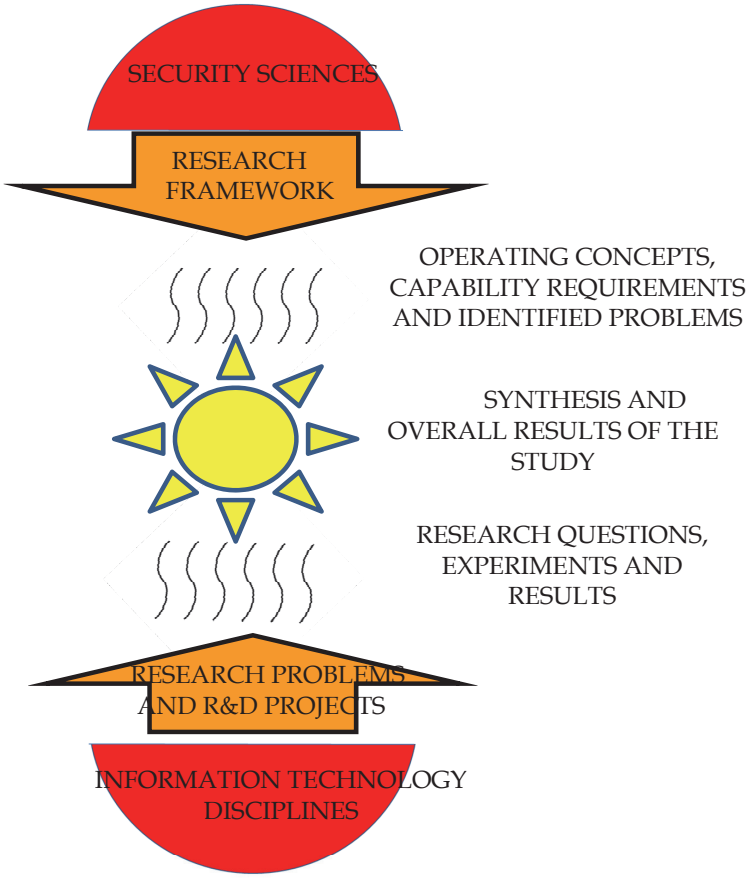


FIGURE 3 The dual research approach of the study

Within the security research framework, crime scene investigation, CBRNE countermeasures and crisis management and warning are examined in the study through their operating concepts and capability requirements along with some more detailed research problems. The results of this examination are then matched with the results of the technology experiments, which are carried out under the information technology discipline in the same CBRNE research area. The overall results of the study are created as a result of merging the results of the top-down approach of the main research problem from a security sciences point of view with the results of the bottom-up approach from the information technology perspective. In this respect, the merging of the research in the security and information technology sciences is carried out with the applied CD&E method, specializing in CBRNE countermeasures and defence.

The empirical research within the information technology discipline is carried out in practical research and development projects. The projects are directed toward technology and software development, laboratory tests and empirical experiments with hyperspectral technology and toward software development and empirical experiments with a mobile emergency alerting and crisis management system with smartphone technology. In addition, some tabletop experiments are carried out to evaluate the technical capabilities of the hyperspectral and smartphone technology.

The laboratory tests and hyperspectral technology experiments are focused on CBRNE detection and forensic investigation, particularly on crime scene investigation. Experiments are carried out with the police, defence forces and fire and rescue service. During the study, some interviews were also conducted with the crime battle units of the border guard and customs. The scientific research methods in this part of the study are laboratory tests and empirical experiments in controlled and semi-controlled environments.

The smartphone technology experiments are directed at mobile emergency alerting, warning and crisis management, and they are carried out with the police, civilian organizations and private citizens. In this part of the study, the case studies and tabletop testing are used as the scientific research methods.

The earlier work that was carried out within the research process prior to the technology experiments and that is not reported here contains the hyperspectral technology development work, the development of hyperspectral analysis algorithms and the programming of hyperspectral analysis software as well as the programming of the server-end and mobile-end software of the smartphone-based alerting and warning system. The hyperspectral technology development work was directed toward producing a prototype of a small field-fit hyperspectral camera, and it was carried out by an external research organization. The hyperspectral software development was directed toward producing mathematical analysis algorithms and software for examining CBRNE substances and other forensic targets with different hyperspectral cameras. The mobile software development was focused on creating a mobile emergency alerting, warning and crisis management system on smartphones for the authorities' and private organizations' use. The system also contains software for servers and other kinds of end-user devices.

1.4.2 Concept development and experimentation (CD&E)

CD&E is a development, experiment and analysis method applied widely, especially by NATO. CD&E (de Nijs, 2010) enables the structured development of creative and innovative ideas into viable solutions for capability development. Capability development covers strategic analysis, the identification of capability requirements, solution identification and solution implementation. Capability requirements may result from assessments of potential future requirements, medium-term defence planning requirements, lessons learned or urgent operational requirements. CD&E (de Nijs, 2010) is being used to find conceptual solutions to capability shortfalls and gaps identified through other processes, and it

also contributes to capability development through the introduction of previously unknown capabilities that result from new ideas, "out of the box" thinking or simply research and technology endeavors.

The role of (de Nijs, 2010) analysis in the CD&E process is to determine at an early stage the stakeholders' interests in and expectations of the concept and the operational value and feasibility of the concept. Analysis also determines possible venues for development by addressing operational validity and effectiveness through modeling. In addition, analysis supports the performance of experiments through the proper formulation of hypotheses and expectations to ensure that the outcomes of the experiments inform the concept development. As the development of a concept progresses, the analysis activities look to accumulate evidence to determine and demonstrate the validity and increased effectiveness of the proposed solutions. As such, the rigor of the analysis is important for increasing confidence in a conceptual solution and reducing the risk involved with its implementation.

The role of concept development (de Nijs, 2010) in the CD&E process is to identify recommended solutions to capability shortfalls or gaps. New problems may be brought about by some combination of political, social, economic, technological or doctrinal factors or by the introduction of new objectives to a preexisting situation. A new concept may also be developed to propose a better solution than that which currently exists. This solution may be delivered through technological, organizational, tactical, societal or other developments that did not exist before, or it may be required due to the failure of existing but sometimes obsolete concepts.

The role of experimentation is, according to de Nijs (2010), is

> primarily to determine whether a concept under development will achieve its desired aim. Results from experimentation inform the concept developer whether a whole concept (or elements therein) are sound or flawed. Experimentation reduces uncertainty as to whether a concept or parts thereof have reached the required level of maturity, helps to identify and solve problems that cannot be solved through studies and analysis alone and avoids those developments which do not offer added value. Moreover, experimentation, as a "trial and error" methodology, can also exploit a negative outcome as a way to refine concepts. Experimentation can occur at each stage of Concept Development so that a single conceptual idea could give rise to one or more discovery, hypothesis testing and validation experiments. Therefore, the conceptual rationale for Experimentation could range from an initial conceptual idea to an approved concept. The important aspect is that the process be cyclical: Concept Development provides the rationale for Experimentation, and Experimentation provides information to refine the concept. Assessment and refinement should involve subject matter experts and concept's customers to the maximum possible extent. Additionally, Experimentation can also be conducted throughout the implementation phase of a concept.

According to de Nijs (2010), the CD&E project can be subdivided into the following four phases:

a. Concept Initiation: the decision to start a CD&E project after the problem and customer requirement have been identified. Initial research and formulation of the problem is started.
b. Project Planning: the development of a concept development plan (CD Plan) for the coordination and management of the project. It is used to assign tasks and responsibilities, monitor the progress of these tasks, integrate and synchronize efforts of multiple teams or people with different competencies and coordinate and integrate activities.
c. Concept Development: the spiral process of the development and refinement of proposed solutions according to the CD Plan.
d. Concept Assessment and Validation: the integration of experimentation, providing opportunities to discover, speculate, hypothesize and validate conceptual ideas within the context and the progress of the concept.

De Nijs (2010) also notes that the analysis supports in its own way in each of these phases and that as defence problems nowadays are generally "wicked," normal solution methods appear not to be fitting with the problems. Most of the time the requirements are difficult to define, or the goals are difficult to formulate. Customers are not sure or do not know what they want exactly, and if a solution is found, it is difficult to test or verify whether that is the right solution. In general, it is hard to say whether the final concept with its solutions is "correct."

In this study, the main research question above all to be solved by individual research and development projects, and within them practical experiments, is whether hyperspectral technology and smartphone technology can be used for security authorities' CBRNE countermeasures and defence in field operations. This major question is examined with an applied CD&E method in a cyclic manner, as de Nijs (2010) suggests. In the study, however, the method is applied at the open sector within an academic research process with authorities and not exactly inside the authority sector as a part of authorities' own development process, for which the CD&E method is originally designed.

Within this research, the beginning of the CD&E process, although not yet mentioning it by name, can be dated to 2009, a time when there was an industrial and economic crisis due to the closing of Nokia's R&D unit in the City of Jyväskylä. At that time, a particular ideation process was launched at the University of Jyväskylä to identify new research and development ideas for government-funded projects. As a result, the research on the hyperspectral and smartphone technology was begun at the university, and the security field was selected as one of the key application areas for these two technologies and for information technology in general.

At the later stages of this research process, the development work on hyperspectral technology was directed to police work, in particular to crime scene

investigation. Accordingly, the development work on smartphone technology was directed to mobile warnings, which can in principle be carried out by many different authorities and also by other kinds of organizations. After a rough concept development with the tentative identification of user needs and definition of user requirements, separate software applications were developed for hyperspectral technology-based crime scene investigation and for smartphone technology-based emergency alerting and warning. These were necessary for the use of hyperspectral and smartphone technologies in the present context, as neither of the two technologies alone can be used by the authorities for the required tasks without particularly designed software, which has been created in this research or by someone else for the same purpose.

When the first prototype versions of the two software applications were ready, the concept development was moved into a new stage by carrying out especially designed practical experiments, in which the developed systems were tested with security authorities in practice by focusing on varying aspects of CBRNE emergencies and crimes. After the results of the experiments were evaluated, the experiences and results of the experiments and projects were again put through the concept development process, as the CD&E method implies (de Nijs, 2010). At this stage of the study, the experiment results of the two separate research and development projects were moved to an upper level, where they were combined and matched with more formal user requirements for managing CBRNE incidents by comparing the operation and performance of the two technologies resulting from the experiments with the capability requirements of the NATO-related CBRNE countermeasures and defense operating concepts of Canada (DND/CF, 2012) and with the corresponding operating concept of the EDA (EDA, 2014). The results and conclusions of this analysis then formed the overall results of the study.

As explained above, in this study the CD&E method is used creatively within the open university sector in a research and development process with authorities, not as formally and strictly as in the military sector's own development processes. The CD&E method here, however, describes well the many-staged development and research process and helps to understand and structure it. In this context, the usage of the CD&E method also shows that the whole development and research process can be formed of several side-by-side processes and of development processes that are carried out at different levels. In addition, the usage of the method in the study shows that the separate stages of the CD&E processes can be carried out at different times and by different people as long as the discussed technology or the created concept stays valid over the time period. In this case, there were at first two simultaneous research and development processes that were not connected at their initial stage. However, when they are revised by the same researcher with new external funding, interconnections between the two processes began to emerge, which at the same time brought forward the development of the initial two technological concepts. In addition, when the two development processes were taken further, there was a need to validate the usability of both technologies in the authorities' formal

CBRNE countermeasures. The proposed two technologies were then compared through an experimentation process with the capability requirements of the standardized operating concepts for CBRNE countermeasures, which had already been tested by international authorities, and conclusions and recommendations for further work were made as a result of this evaluation.

1.4.3 Experiments in controlled and semi-controlled environments

Hyperspectral technology is tested in the study through various carefully designed and prepared experiments. These are somewhat different from the methods that are referred to in the literature for studying causalities in natural sciences. According to Blakstad (2008), experimental research is a collection of previously planned research designs that use manipulation and controlled testing to understand causal processes. Often one or more variables are manipulated to determine their effect on a dependent variable. The method is commonly used in sociology and psychology, physics, chemistry, biology and medicine (Blakstad, 2008). According to Shuttleworth (2008), experiments and previously planned research designs are also used in qualitative research.

In this study the experiments with hyperspectral technology aim at answering the questions of whether this technology can detect various substances, and, if it can, which kinds of cameras are able to detect which kinds of substances in which kinds of environments. The major question thereby contains several smaller issues, which are tested via the experiments: the types of cameras, substances and their physical forms and matrices on which substances are being detected as well as other environmental factors, such as the volume and intensity of external light. By splitting the major research question into smaller pieces, the final basic question for each camera and substance in different research installations is whether or not the camera can detect the particular substance in the particular environmental conditions. Hyperspectral experiments can therefore be described and conducted basically as direct technical measurements in different research installations and environments.

External factors can be controlled best in the laboratory environment. However, in a field environment, a research installation can be designed, but external conditions, such as volume of light, temperature, humidity and wind, cannot be set. According to Shuttleworth (2010), field experiments still follow all the steps of the scientific process by addressing research problems and by generating hypotheses. He also sees as an obvious advantage of field studies in that they are practical and allow experimentation without artificially introducing confounding variables. Field experiments can still suffer from a lack of a discrete control group and often have many variables the researcher must try to eliminate.

Most of the hyperspectral experiments in the study are laboratory tests, and some are field experiments. Controlled laboratory tests are usually conducted first to ensure that the technology works with the selected samples in standard conditions. If the laboratory tests do not give positive results, there is no reason to conduct field experiments with the same camera and samples. In

some cases, other kinds of field experiments are needed first to produce the desired samples to be tested in the laboratory. For example, the study of gunshot and explosion residue requires outdoor tests first to produce such samples.

Concerning all the experiments conducted during the study, the hyperspectral cameras, investigated substances and research environments were changed for each experiment. Within individual laboratory experiments, however, the research environment was kept unchanged, and all the samples within the same research topic were measured one after another with two or three different cameras. In this kind of approach, the motivation for carrying out a large variety of altered tests is the exploratory nature of the study. This approach was chosen for the study to determine at a certain level the overall potential of hyperspectral technology in detecting CBRNE materials over the whole timeline of a CBRNE incident. For this purpose, it is more relevant to have some evidence of many different issues within the same topic than to gain highly qualified and statistically validated information about some narrow detailed question, which as such might not be able give sufficient information on the overall utility of hyperspectral technology in CBRNE countermeasures and defence.

During the experiments, all samples were measured in their natural form without treating them with any chemical, radioactivity or other method. In the laboratory tests, different samples were measured in the following ways:

- Small solid items were placed on the imaging scanner of the camera as they were, without preparing them in any other way. Small items refer to objects less than 15 cm high and less than 20 cm wide.
- Large items were cut for having a smaller sample that could be measured with the test equipment.
- Pure liquids were imaged in an open glass or plastic bowl, unless they were toxic and needed special arrangements.
- Samples of biological fluids such as blood and other biological liquids were prepared on different matrices. Samples were measured with the hyperspectral cameras as dry, and wet samples of biological fluids were not used.
- Small particles such as gunshot and explosion residues were also prepared on various matrices. Residues were produced by arranging shooting and explosion experiments where the residues were collected on selected matrices. The first test for collecting gunshot residue was organized indoors by a police officer firing a police pistol at the shooting range of the local police department and by collecting residue on a glove made of textile and leather. All other experiments for collecting gunshot and explosion residues were organized in authorized test areas outdoors.
- Toxic chemicals were measured in a solid, liquid and gaseous forms in an airtight glass bowl within a fume cupboard. These tests were performed in an authorized laboratory.

In the field experiments, samples were measured outdoors directly at their original place in their natural form. Identical samples of selected substances were prepared side by side on three different soils, sand, asphalt and grass, where they were measured with the hyperspectral camera as they were. Toxic chemicals were not used in open air field tests.

Laboratory tests were carried out with seven different hyperspectral cameras. In each testing session, the same samples were measured with one, two or three different cameras. The six camera types were of the following types: 500–800 nm and 450–850 nm Fabry-Perot type of visible light and near infrared VIS/NIR cameras, a 400–1000 nm push-broom type of visible light and near infrared VNIR camera, a 900–1700 nm push-broom type of near infrared VNIR camera, a 1000–2500 nm push-broom type of short wave infrared SWIR camera, a 3000–6000 nm push-broom type of mid wave infrared MWIR camera and an 8000–1200 nm push-broom type of long wave infrared LWIR camera. In the field experiments, only a small 450–850 nm Fabry-Perot type of visible light and near infrared VIS/NIR camera was used for airborne imaging tests.

In addition to standard cameras and standard-sized samples, the laboratory tests were controlled by several other factors, such as lighting, ambient light, imaging distance and temperature. The measurement distance and lighting were fixed according to each camera and its optics. All laboratory samples were measured at approximately a 5–20 cm distance. Disturbing ambient light was prohibited as much as possible. The quality of measurements was checked during each measurement, and, where possible, measurements were repeated three times to validate the imaging results. Explosives' residues were also examined with a high-quality spectrometer to control the hyperspectral imaging results. Room temperature as taken into account with samples that were sensitive to changing temperatures. For example, blood samples were prepared on matrices soon after donation, and the temperature was held constant until the samples were measured. With toxic chemicals, other controls were also applied in the laboratory, and the samples were handled only by authorized people in a specialized laboratory. In addition, these samples were imaged in an airtight glass bowl in a fume cupboard. For the mid- and long-wave infrared imaging, an IR window was also placed in the measurement bowl.

1.4.4 Case studies

In scientific research, small-scale experiments in designed testing environments are often more qualitative than quantitative in nature. According to Shuttleworth (2008), qualitative research design is used extensively by scientists and researchers studying human behavior and habits. It is also often regarded as a precursor to quantitative research to generate possible leads and ideas for formulating a realistic and testable hypothesis. The hypothesis can then be tested comprehensively and analyzed mathematically with standard quantitative research methods. For these reasons qualitative methods are often closely allied with interviews, survey design techniques and individual case studies as a way to reinforce and evaluate findings over a broader scale. Shuttleworth (2008)

notes also that the design of qualitative research is probably the most flexible of the various experimental techniques, encompassing a variety of accepted methods and structures. Including individual case studies and extensive interviews, this type of study needs to be carefully constructed and designed, but there is no standardized structure. Case studies, interviews and survey designs are the most commonly used methods.

One of the advantages of using qualitative techniques (Shuttleworth, 2008) is that they are extremely useful when a subject is too complex to be answered by a simple yes or no hypothesis. These types of designs are much easier to plan and carry out and are possibly useful for budgetary reasons. The broader scope covered by these designs also ensures that some useful data are always generated, whereas in a quantitative experiment an unproved hypothesis can mean that a lot of time has been wasted. Qualitative research methods are not as dependent upon sample sizes as quantitative methods, and a case study, for example, can generate meaningful results with a small sample group. The counter sides of qualitative methods are that (Shuttleworth, 2008), even though they are not as time or resource consuming as quantitative experiments, qualitative methods still require a lot of careful thought and planning to ensure that the results obtained are as accurate as possible. Qualitative data can also not be mathematically analyzed in the same comprehensive way as quantitative results, so they can only give a guide to general trends. Additionally, these data are much more open to personal opinion and judgment and can only give observations rather than results. A given qualitative research design is also usually unique and cannot be exactly recreated, meaning that it lacks the ability to be replicated.

In this study, the case study method was used to gain information of user experiences in smartphone experiments for mobile emergency alerting and crisis management. The experiments were organized in different environments with different users, and they simulated different kinds of emergencies and crises. The research interest in the experiments was focused on the operation and usability of smartphone devices and of the mobile emergency alerting and crisis management system, which was developed as a part of this research. The smartphone experiments were arranged with the police, a volunteer test group of private citizens, a local school, the department of chemistry, the crisis communication unit of the university and the fire and rescue service. Before the experiments were started, background information about the study and experiments was given to the test-users in face-to-face meetings and by video conferences, phone calls and emails where necessary. In the meetings, the operation of the developed mobile system was also demonstrated and explained, and the smartphone test devices were delivered to the users. Also, the operation of the system with other models of smartphone devices was presented in the meetings, as some test-users participated in the experiment with their own devices, which constituted different models and brands than those provided to the users by the project. Carrying out the experiments took from one week to a couple of weeks, or only one day, depending on the nature of the individual test and the threat scenario simulated in the test.

The research data were collected from the test-users in some of the tests before and after the experiment and in some tests only after the experiment. The data collection methods were questionnaires and personal interviews. The questionnaires were of two types. Quick information about the test environment and users' opinions about the security situation were collected in face-to-face meetings with short questionnaires answered anonymously on paper. More thorough data about the user experiences of the tested mobile system and smartphones were collected after the experiment with a longer questionnaire on the Internet. In the smartphone and mobile emergency alerting experiments, data were also collected in the system's log on the server. The server information revealed, for example, the exact points in time when the alerts and warnings were given and when they were received and signed by each user and response times by each user as well as the lead times of each warning and alert in both directions.

The first experiment was arranged with the national crisis communication preparedness group of the police, which also included members of the special forces of the police. The test contained representatives from eight different police departments around the country. In the experiment, emergency alerts and other commands and messages were given inside the national police organization by the Central Finland Police Department, which was in charge of the practical performance of the experiment. Also, the situation picture was created regarding the police officers' situation. The first situation picture was created immediately after sending the first alert, and the picture was updated gradually while the experiment was proceeding. Log information about each police officer's operation during the experiment was available for the debriefing and analysis of the operation after the rehearsal was over. The log was created automatically on the basis of incoming and outgoing communication on each police officer's smartphone. The user experiences were collected with a questionnaire on the Internet after the experiment. Also, personal interviews were conducted at the police department, which was in command of the operation during the experiment. The questionnaires and interviews focused on the police officers' opinions about the function of, usefulness of, need for and improvement suggestions for the developed mobile emergency alerting system. The technical data of the execution of the experiment were recorded and collected on the system's server.

The second experiment was also arranged with the police with the same police department being in charge of the operation. In this experiment, emergency messages were not sent within the police organization but rather from the police to the private citizens. As the user group was outside the police organization, the content of the messages was different. With private citizens as the test group, and with the different data content in the system, the same smartphone system was transformed from the alerting, command and control system of the police into a public warning system for the civilians. User experiences were collected from the civilian users with a questionnaire on the Internet after the experiment, as was done in the first experiment with the police officers. The data content of the questionnaire, however, was different, because the function and data content of the system in the experiment were different from

the system's usage as the command and control system of the police. The experiment and questionnaire with the private citizens were focused on the threat scenarios, conditions of giving public warnings on private citizens' personal phones, data content and formulation of warning messages. The technical data of the experiment, including the lead and response times etc., were collected automatically at the server.

The third smartphone experiment was organized within a private organization in a public school where there were 500 children. The experiment was organized with the same system and same smartphone devices as with the police but with different threat scenarios and data content in the system. In this case, warning messages and other crisis communication were given by the rector or by another crisis communication manager of the school. Warning messages were given only to the teachers and other staff of the school to avoid anxiety and panic amongst the children. For the experiment, additional emergency call buttons were also installed so that alerts could be given by various methods in different places by other teachers and staff. Fixed emergency call buttons were installed in classrooms that had greater safety risks than others, and mobile emergency call buttons were given to personnel who needed to work in and move about various locations around the school or city during the day. In addition, a digital emergency call button was implemented on the test phones given to the teachers for the experiment. The research data were collected from the users with a questionnaire before and after the experiment. The first questionnaire was focused on evaluating the security situation in the school and on the personnel's opinions regarding the need for installing an emergency alerting system in the building. The second questionnaire focused on the user experiences of the tested system and on inquiries of whether the tested system would be useful in the school.

In the fourth smartphone experiment, the same system was tested in a rescue rehearsal of a toxic chemical release with the fire and rescue service, department of chemistry and crisis communication team of the university. Compared with the test environment in the local school, the university area was wider, and the number of staff and students was higher: nearly 20,000 people. Unlike in the school experiment, there were no underage persons in the university buildings. In this experiment, the crisis communication team at the main campus of the university was in charge of the system, and the emergency alerts were given to the test group of personnel at the department of chemistry at another campus. The interactive features of the system were also tested in this experiment. This was done by simulating an emergency call and rescue of persons trapped in the building, who could not get out because of the toxic chemical in the building. Before the test, a face-to-face meeting was organized with the personnel, and user experiences were collected with questionnaires and personal interviews afterwards. Different questionnaires were given to the personnel who participated in the simulated chemical accident at the department of chemistry and to the personnel of the communication services of the university who were in charge of the management of the crisis communication during the experiment.

1.4.5 Tabletop experiments

Tabletop exercises are various mental or manual visualizations, simulations or rehearsals of an examined situation, where the course of action is brought out without simulating it via computer or actually executing it. Exercises can be supported with different physical materials or without them. Such exercises can be used as a training method to prepare for a potential situation or as an analysis method for a potential or a situation that has already happened. For example, Tracy (2012) has applied a manual approach for researching already actualized real-life emergencies in the 1990s by analyzing 911 field notes and interviews using differently colored pencils, numbers, marks and other codes. According to McLaughlin (in Violino, 2014), tabletop exercises enable organizations to analyze potential emergency situations in an informal environment, and they are designed to foster constructive discussions among participants as they examine existing operational plans and determine where they can make improvements. Such exercises seem to be a natural fit for information and physical security, because they provide a forum for the planning, preparation and coordination of resources during various kinds of attack. Referring to McLaughlin (in Violino, 2014), tabletop testing generally takes the form of a discussion-based exercise and involves reviewing the roles, responsibilities and response efforts required to respond to a given security incident. McLaughlin (in Violino, 2014) sees an advantage in emergency-related tabletop exercises in that the testing tends to provide a high-level estimate of the potential for success in the event of such an incident. The major benefit of using these types of exercises is that they provide real scenarios in a non-threatening and non-disruptive format and can be rather economical to conduct. The goal is that participants and management become more aware of possible gaps or weaknesses that may exist in the incident response plan. Tabletop exercises are also used by the UW-Madison Police Department (2012), where they are defined as follows: "The tabletop exercise is a meeting to discuss a simulated emergency situation. Members of the campus review and discuss the actions they would take in a particular emergency, testing their emergency plan in an informal, low-stress environment. Tabletop exercises are used to clarify roles and responsibilities and to identify additional campus mitigation and preparedness needs. The exercise should result in action plans for continued improvement of the emergency plan."

In this study, the tabletop method is used to evaluate how the hyperspectral technology and smartphone-based emergency alerting and crisis management system could have been used in a real-life CBRNE emergency situation in Laukaa, Finland, in July 2013. An explosion threat situation began in an explosives manufacturing plant when an external partner's container full of an unknown mixture of chemical waste started heating in the warehouse area, causing an explosion threat to the surrounding explosives equating 150 tons of TNT. The threat situation set off a high-priority alarm by authorities, and all civilians around the area were evacuated. Various methods were used to defuse the unstable chemical and to eliminate the explosion threat for the stored explosives at the plant. The joint

operation of the local fire and rescue department, police and defence forces was conducted successfully, and no human or material losses were incurred. This well-documented incident offered the researcher a good opportunity to evaluate how the situation could have been handled with alternative technologies and methods. A tabletop rehearsal of the incident for evaluating the usability of the hyperspectral technology and smartphone-based emergency alerting system in the situation was carried out by going through the course of the incident step by step on the basis of personal experiences, media sources, authorities' reports and documented material of the real-life events and by evaluating how the two technologies could have been used in each phase of the three-day-long situation. Detailed reporting of the incident was given by the local authorities in a face-to-face meeting after the incident and also through the public media, which reported on the incident actively for several days. The reporting given by authorities to a selected audience after the incident included the involved authorities', civilian aid organizations' and private citizens' reporting of having been involved in the incident as a rescuer or rescuee or as a representative of crisis communication, the public media or some other immediate stakeholder of the situation. A detailed report of the incident by the Finnish Safety and Chemicals Agency Tukes was also made available.

Tabletop exercises are also used in the study to evaluate the international scalability of the smartphone-based emergency alerting and warning system in an international environment and the possible roaming of mobile alerts into other areas. Moreover, the vulnerability of the system and possible risks especially in the case of technical breakdowns of mobile communication infrastructures are evaluated in the study with this method.

1.5 The research process and structure of the dissertation

The research on hyperspectral technology and smartphone technology was first initiated during a large innovation and development project called *Scientific innovation product concept, Scope*, which was carried out with funding from the Finnish Funding Agency for Innovation (Tekes), the University of Jyväskylä, the City of Jyväskylä and private companies from 2009 to 2011. The project was started to boost new technology and business innovations in the Jyväskylä area after the multinational mobile phones manufacturer Nokia closed down their R&D unit in Jyväskylä in 2009.

After the *Scope* project, a separate project called *Situational awareness through proactive risks and opportunities, Sapporo* was initiated to develop and test a smartphone-based mobile emergency management system in November 2011, and it was concluded in August 2013. During the project, empirical experiments were also carried out with the police and fire and rescue service. The project was funded by Tekes, European Regional Development Funds (ERDF), University of Jyväskylä and private companies. At the same time, a feasibility study called *Crime Scene Investigations by Spectral Imaging, SpeCSI* was also started to

examine hyperspectral technology's potential in crime scene investigation in December 2011, and it was concluded in June 2012.

After receiving encouraging results from the feasibility study *SpeCSI*, the main project, called *Hyperspectral Solutions for Crime Scene Investigation, SpeCSI Solutions,* was initiated to develop a prototype of a small hand-held hyperspectral camera and hyperspectral analysis software for hyperspectral crime scene investigation in May 2013. The project was carried out as two collateral projects by the University of Jyväskylä and VTT Technical Research Centre of Finland Ltd (VTT) over one and a half years, ending in October 2014. The VTT's project was focused on the development of a prototype of a new hyperspectral camera, whereas in the University of Jyväskylä's project new analysis software was produced for various hyperspectral cameras. In the University of Jyväskylä's project, experiments were also carried out with the police, defence forces and fire and rescue service to test the usage of hyperspectral technology in crime scene investigation, forensics and counterterrorism, including the detection of selected CBRNE substances. Both the feasibility study *SpeCSI* and the main project *SpeCSI Solutions* were funded solely by Tekes and the University of Jyväskylä except for the adjacent technology development project, which was carried out outside the university with funding from Tekes and VTT.

Along with the *SpeCSI Solutions* project in 2014, a four-year-long research and development project called *Toxi-triage* was also designed in the field of CBRNE by eight European countries, with the Loughborough University from the UK as the coordinator of the project. In 2015, the European Commission awarded funding of 12 million euros for the project for the years 2015 to 2019. One part of the project, led by the author at the University of Jyväskylä, is focused on the research and development of hyperspectral countermeasures of CBRNE.

Each of the empirical experiments in the abovementioned projects contains more than one test, and each experiment also has its own research questions, research design, organization and execution within the projects. The results of the experiments are reported and published internationally in separate scientific articles. Also, practical reports have been produced for the financier of the projects, and the results of the two main projects, *Sapporo* and *SpeCSI Solutions*, have been commercialized into private companies.

The agenda for the hyperspectral and smartphone technology-based software development and experimentation in the forensic and CBRNE countermeasures field is shown in Figure 4.

The experiments and tests on mobile emergency alerting, carried out within the research and development project *Sapporo*, are as follows:

1. Tabletop rehearsals for the international scalability and vulnerability of mobile emergency alerting systems in winter and spring 2012.
2. Internal alerting, command and control and situational awareness tests with the Central Finland Police Department, Police Board and members of a

communication preparedness group and special forces from eight police departments around the country in November 2012.

3. External public warning and situational awareness tests with the Central Finland Police Department and private citizens in December 2012.
4. Internal emergency warning tests and integrated emergency call button and warning tests with a civilian organization in the Kilpinen School of the City of Jyväskylä in January–February 2013.
5. Internal warning tests and a comparison of a smartphone system and SMS system during a rescue rehearsal of a chemical leak with the Rescue Department of Central Finland and the Communications unit and Department of Chemistry of the University of Jyväskylä in April 2013.
6. Tabletop rehearsal of crisis communication with smartphones in a real-life explosion threat situation and evacuation at an explosives production plant and its environment in July–September 2013.

The experiments and tests on hyperspectral technology, carried out within the hyperspectral technology and software development project *SpeCSI Solutions* and in the preceding feasibility study *SpeCSI* are as follows:

1. Tests with various crime scene samples and blood with the Central Finland Police Department and the National Bureau of Investigation in spring 2012.
2. Tests with various crime scene samples, tear gas, blood and marks of arsons, fires and contaminated soil with the Central Finland Police Department, Rescue Department of Central Finland and the Department of Chemistry of the University of Jyväskylä in July 2013.
3. Tabletop rehearsal of the hyperspectral detection of an unknown chemical in a real-life explosion threat situation in July 2013.
4. Tests with blood, other body fluids and drugs with the National Bureau of Investigation, Oulu Police Department, Terveystalo healthcare service company and the Department of Chemistry of the University of Jyväskylä in October 2013.
5. Shooting tests with pistols, rifles and shotguns at Korpilahti shooting range in October 2013.
6. Explosion tests with the Central Finland Police Department, Counter Terror Group of the Police of Finland, Finnish Defence Forces and the Department of Chemistry of the University of Jyväskylä in October 2013.
7. Laboratory tests with CWAs with Verifin in May 2014.
8. Laboratory tests with blood and drugs with the Central Finland Police Department in July 2014.

9. Laboratory tests with approximately one hundred explosives and explosives mixtures with the Central Finland Police Department and explosives manufacturing company Forcit Ltd. in July 2014.
10. Airborne detection tests for explosives and blood and flying tests with a lightweight hyperspectral camera and drone with the Central Finland Police Department and explosives manufacturing company Forcit Ltd. in July 2014.

After all the above-named government-funded development projects were completed (the last ended in October 2014 and was commercialized in June 2015), the research process was taken to a new level to produce the doctoral thesis of the research area. The two individual research processes of hyperspectral and smartphone technology were combined and related to the same academic research question concerning the usability of the two technologies in CBRNE defence. At this stage, at the turn of 2014–2015, the research seemed to be needing a stronger discussion on and contribution to the security sciences, and additional supervision was requested for the doctoral study from the National Defence University (NDU) in Helsinki. During these discussions, the main approach and structure of the thesis remained much the same by having the question of the two technologies' role in CBRNE defence at the top of the whole work and by questioning and reasoning out the main research question through the empirical experiments carried out during the government-funded development projects. The supervising professor at NDU proposed the use of the CD&E method in the study, and the method seemed to fit well with the research approach and with the structure of the work. As a result, it was taken as the primary research method for the study at the main level of the work. Taking on the use the CD&E method did not, however, diminish the role of the other research methods in the study, which were used inside the research projects and within the empirical experimentations that were carried out as a part of the study. Instead, the whole methodology of the study was created as a summary of all of the applied methods.

The entire research framework of the study as well as the comparison of the international CBRNE countermeasures operating concepts with the CBRNE-related hyperspectral and smartphone technology experiments with the authorities were produced after becoming acquainted with the CD&E method. Also, the introductory text of the thesis, including the summary and conclusions, were compiled after the completion of the development projects, with the exception of the included articles, which were produced during the government-funded projects (article PII was published afterwards).

The thesis is composed of four main chapters. In the first chapter, an overview is given about the research environment and background of the study as well as the objectives, research problem and research questions of the work. The research approach, methods and research process are also introduced in the first chapter. The second chapter presents the framework of the study. It contains two main topics, of which the first gives an introduction to CBRNE threats and the other to CBRNE countermeasures.

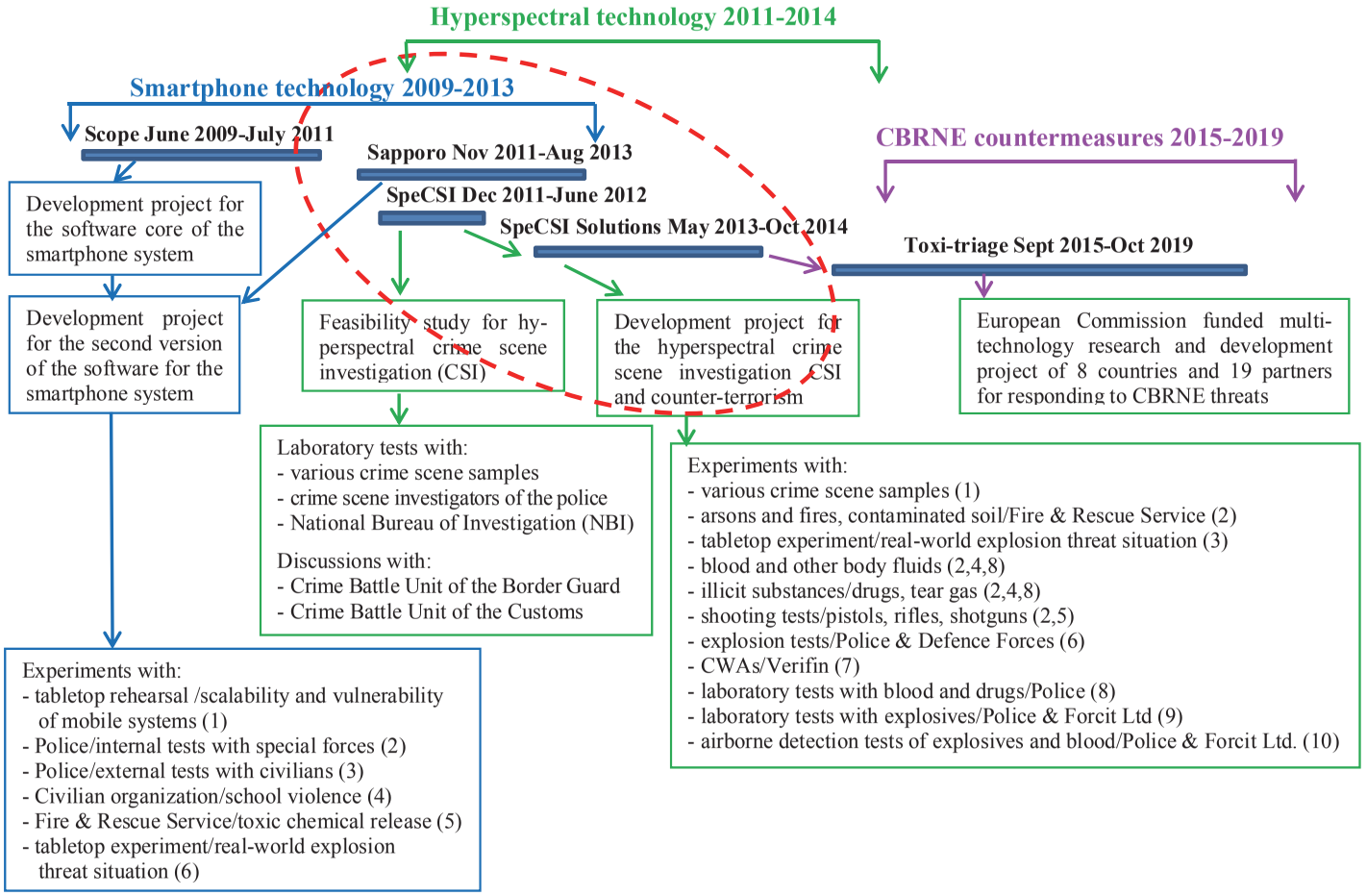


FIGURE 4 Research agenda for the technology and software development and CBRNE countermeasures experiments

The third chapter presents the empirical experiments and results of the study. The experiments are briefly introduced in 10 sub-sections, with references to the included scientific articles that were published earlier during the research process. The fourth chapter presents a discussion of the overall contribution and impact of the study. Chapter 4 also covers the validity and reliability of the study as well as recommendations for the future work. Included at the very end are a Finnish summary, references and the included scientific articles.

2 THE RESEARCH FRAMEWORK OF THE STUDY

2.1 CBRNE threats

CBRNE threats are caused by the presence of chemical, biological, radiological, nuclear and high-yield explosive substances (DOD, 2012), which can cause death or other instant and long-term injuries and damage to people and the environment. Such threats arise due to accidents as well as some people's deliberate actions. Most of the CBRNE materials are manmade, although, for example, toxic gases, biological threats and radioactive emissions do also exist in nature. Lethal exposure to nature-based gas and radiation can usually be expected and avoided, whereas the spread of and exposure to nature-based biological threats is more difficult to prevent. Particularly illnesses such as SARS (CDC, 2012) and Ebola (WHO, 2015) can develop into epidemics and pandemics and cause thousands of casualties in multiple countries. SARS (CDC, 2012) spreads in close person-to-person contact by respiratory droplets and Ebola (WHO, 2015) through human-to-human transmission via direct contact with the blood, secretions, organs or other bodily fluids of infected people and with surfaces and materials contaminated with these fluids.

Manmade CBRNE materials are developed and used for both civilian and military purposes. Outside war, they cause harm via accidents and by deliberate illegal acts. The most common accidents are caused by explosives and industrial chemicals, which are widely used for civilian purposes. Accidents also happen with old military ammunition that is not found and removed during wartime or that is kept as a keepsake or collectible in inappropriate places. Deliberate wide-scale destruction is most often caused by disturbed or radicalized individuals or by radicalized terrorist groups. Typically, this is done with firearms and explosives, which are most easily available to criminals. Over recent years, terrorists have also used chemical and biological agents to hurt large numbers of people. There are also examples of using radioactive agents on civilians, but usually this medium is employed against an individual and not large numbers of people. Due to their extensive destruction power, CBRNE materials are also called WMDs. These include (FBIb, 2015) destructive explosive devices; other weapons that are

designed or intended to cause death or serious bodily injury through the release, dissemination or impact of toxic or poisonous chemicals or their precursors; or any other weapons involving a biological agent, toxin or vector weapons that are designed to release radiation or radioactivity at a level dangerous to human life. Of these, chemical agents are also referred to as chemical warfare agents (CWAs), toxic industrial chemicals (TICs) and toxic industrial materials (TIMs) (Bennet, 2003).

To prevent or mitigate damage, CBRNE risks and threats need to be anticipated and detected. In regard to accidents, this means careful adherence to safety measures in all situations where CBRNE materials are handled, transported or stored. Intentional damage is prohibited by legislation by making the access to regulatory material difficult for unauthorized persons. This does not always work, and destructive compounds can also be prepared with freely available materials. Therefore, it is urgent for authorities to be aware of the preparation of destructive measures against society, and this is usually done by forensic or military intelligence or as a part of other forensic investigations. Set and released CBRNE threats also need to be detected, and this can be done with direct or indirect detection measures. Direct measures detect the influencing matter per se, whereas indirect measures find other indicators and marks that reveal the presence of threat. Threats that have not yet been released can often be detected on the basis of the package, container or shell that contains the influencing matter.

Materials that have already been released behave differently depending on whether the influencing matter is a chemical, biological, radioactive, nuclear or explosive threat. Explosives usually cause damaging effects instantly, and if all explosive matter blows up, it does not necessarily leave other immediate threats to life at the location in the form of explosive matter or its degradation products. Explosions can, however, cause after-effects in the form of building collapse and fire, and these in turn may produce toxic chemicals that are unsafe to inhale. Explosives can also be used as an ignition for releasing another fatal material, for example a chemical agent, which would be lethal even if the explosion had not already caused significant material destruction or fire. For these reasons, if all of the explosive material blows up, the post-blast detection of the explosives' residue may not be essential for the identification of an ongoing threat, but it is still needed for the forensic investigation and for preventing further risks.

Radioactive and nuclear materials, unlike explosives, form an immediate and lethal health risk, not only at the moment when they are released but also after the possible blast. If they are being spread through an explosion, they cause material damage and casualties at first and additional casualties for a certain time after the incident. Radioactive and nuclear radiation cannot be felt with the human senses, yet it is lethal. Therefore, it needs to be detected immediately when it is released, and there are multiple technical sensors and sensor systems available for doing this. Usually fixed ground-based sensor systems monitor the whole area at a certain accuracy, and they can be complemented with various air surveillance and mobile monitoring and detection systems. Wide-area systems typically detect airborne radiation, which may shift far from where it was released

and cause a threat in another place. However, radiation sensor systems do not necessarily detect sealed radiation sources, which are transferred from their origin to be released in some other place. For example, nuclear missiles require different kinds of countermeasure systems than radiation released in open air. In places where the source of radiation is nearby, more precise and mobile radiometers are needed for detection, and the radiation needs to be measured and identified before rescuers or investigators may enter the place. Radiation also needs to be measured several times afterwards in the exposed environment and in humans to monitor the changes in radiation levels. Radioactive clouds may also move away from the area with the wind, and the measures of radioactivity will in any case decrease over the time, although slowly. This process cannot be sped up, and radiation cannot be neutralized. Therefore, people who have had direct exposure or who live in fallout areas have a risk of getting sick even a long time after the radioactive release.

Chemical and biological threats are, like radiation, also lethal afterwards, not only at the time when they are released. Chemical agents are, however, more sensitive to environmental effects than radiation, as many chemical compounds may transform into other substances when they react, for example, with water, heat or air. Toxic chemicals can also be washed out and neutralized through specific chemical processes, even though such cleaning processes are time-consuming and difficult. When chemical or biological agents are released, they need to be detected immediately, and no rescuers may enter the site without appropriate protective gear. The detection of chemical agents can be challenging, as the agent may have evaporated by the time rescuers arrive on the scene and barely anything of the agent may be seen with the eye. Also, chemical sensors may not be able to detect the agent if there are not enough particles left in the air. Detection is, however, needed for finding traces of the chemical agents in any of the different forms in which they may exist. These can vary from solid to liquid and gaseous forms, and the agent may also be mixed with other substances. Agents may also decompose, and their precursors or degradation products can possibly be found instead of the pure chemicals. If deeper analysis is needed to identify the toxic agent, rescue and medical operations must be initiated on the basis of other indicators and symptoms of patients without first verifying the agent. Detection is also urgently needed for isolating the area and for protecting other people from contamination.

The detection of biological agents is even more challenging, because the particles are extremely small and lethal in very small quantities. Many biological sensors detect agents in the air like most of the chemical sensors, but not all biological agents are transmitted by air. In these cases, the potential source of contamination needs to be recognized first, and a physical sample needs to be taken into a laboratory for analysis to identify the potential agent. The preparation of terroristic chemical or biological attacks may be discovered with forensic or military intelligence, which are covered in the field of command, control, communications, intelligence, surveillance and reconnaissance (C4ISR). In general, there however are hardly any technological means able to directly or remotely detect

the shielded preparation or transportation of these kinds of agents, or possible to identify agents through an airtight container, package or other hidden place. However, chemical and biological agents are difficult to attain and handle, which diminishes the risk of having them released against civilian populations.

2.1.1 CWAs and TICs

The stockpiling, manufacturing and usage of CWAs is prohibited all over the world. The use of poisonous gases was for the first time banned (Bunn, 1969) with The Hague Gas Declaration in 1899, which held an agreement to abstain from the use of projectiles that are made for the diffusion of asphyxiating or deleterious gases. Poisonous gases were, however, used against the agreement during World War I in 1914–1918, starting (Ganesan et al., 2010) with the German gas attack with chlorine on April 22, 1915, at Ypres, Belgium, leading during the whole war to 100,000 deaths and 1.2 million casualties caused by toxic chemicals, including phosgene, sulfur mustard and lewisite. After this a new agreement on the prohibition of toxic gases was needed, and the Geneva Protocol (UNODA, 2015) for the prohibition of the use in war of asphyxiating, poisonous or other gases and of bacteriological methods of warfare was signed in 1925. Since then, toxic chemicals were used in World War II (Ganesan et al., 2010), when millions of civilians were killed by the Nazis with Zyklon B gas (hydrogen cyanide gas).

The Geneva Protocol (OPCW, 2015a) was extended in 1993 when the Chemical Weapons Convention (CWC) was signed by 130 countries. Soon after that an organizational body was also formed for monitoring and controlling the manufacturing and usage of CWAs, as The Organization for the Prohibition of Chemical Weapons (OPCW) was founded in 1997. OPCW works in relationship with the United Nations and is currently formed by 192 member states that represent 98% of the global population and landmass (OPCW, 2015b). There are also a number of states that have not signed the agreement, leaving a risk that some government-based actors might use chemical weapons. Among the countries who have signed the agreement, there are also member states that have production facilities of chemical weapons. In addition, it is possible that terrorists and other radical groups may gain access to CWAs or to TICs. Evidence of this kind of activity has been found within recent decades and years, especially in the Middle-East. After WWI, the first major incident of the use of chemical weapons (Ganesan et al., 2010) took place during the Iran–Iraq War in the 1980s, followed by the largest single CWA attack where Iraq used a nerve agent on its own Kurdish civilian population of Halabja, killing around 5,000 people.

After the Iran–Iraq War, including Iraq's attacks against Kuwait and its own Kurdish population from 1980 to 1988, the UN Secretary Council decided in 1991 (UN, 1991) that all chemical and biological weapons, stocks of agents, related subsystems and components as well as all research, development, support and manufacturing facilities must be destroyed and that a Special Commission would be formed and sent to Iraq to inspect the situation. The end of the international verification process (Hart, 2014) revealed a large-scale nuclear, biological and chemical weapons and ballistic missile programs, particularly containing nuclear

enrichment activity and the production of cyclosarin, sarin, sulphur mustard and tabun in Iraq. Similar events took place after the start of the civil war in Syria in 2011. Chemical weapons had been used in the country to kill civilians, for which reason the UN Secretary Council decided (UN, 2013) that the United Nations and OPCW would conduct the elimination of the Syrian Arab Republic's chemical weapons program. When the neutralization of the Syrian chemicals began (Garamone, 2014) on MV Cape Ray in July 2014, 600 tons of chemicals were loaded onboard to neutralize HD sulfur mustard gas and DF, a sarin gas precursor.

In addition to the state chemical weapons programs found in Iraq and Syria, a non-state group called Al Guida (Hart, 2014) has been suspected of having intentions of using chemical agents. Also, the terrorist group ISIS has been threatening several states with the use of chemical weapons. In spring 2015, ISIS was reported to have been using chlorine (BBC, 2015d), and in the summer of that same year sulfur mustard in Iraq (Kube, 2015; Naylor, 2015). A few months later, in December 2015, ISIS was claimed to have brought toxic gases to Europe (Wyke and Boyle, 2015), some claiming they included sarin, transported through Turkey to Switzerland (Hoft, 2015). In June 2015, the government forces in Syria have also been stated to have used chlorine on civilians (Reinl, 2015). Before the instability, civil war and terrorism in the Middle-East, the international usage of CWAs was more exceptional, and the threat of chemical agents was quite small. In other areas, one of the most widely known examples is (Osaki, 2015) the doomsday cult Aum Shinrikyo's sarin attack on the Tokyo subway system in 1995, which killed 13 people and left more than 6,000 sick or injured.

In scientific, industrial and medical uses, most of the toxic chemicals can be used legally in controlled and supervised conditions. Precautions are taken seriously, but as with all manmade devices and user environments, no one can fully guarantee that accidents will not happen. Also, if someone with access to the chemical agents would want to cause harm, intentional misuse cannot be fully prevented. Particularly TICs may cause a potential threat due to their availability to radicalized persons and groups. TICs are defined (Hart, 2014) as chemicals having a lethal dose 50% (LCt_{50}) of less than 100 000 mg-min/m^3 and are produced in amounts of over 30 tons annually at any given facility. The control and detection of the criminal usage of industrial chemicals may be difficult for the same reason as the prevention of the criminal usage of licensed explosives and homemade bombs. If WMDs are built with legal materials or if legal materials are stolen from their licensed owners, a major crime of harming property and people may not be detected in time.

CWAs can be classified (Ganesan et al., 2010) on the grounds of their volatility, chemical structure and physiological effects on humans. Based on their physiological effects, CW agents are classified by OPCW (OPCW, 2015) as follows:

- Choking agents,
- Blister agents,
- Blood agents,
- Nerve agents,

- Riot control agents,
- Potential CW agents,
- Mustard agents,
- Psychotomimetic agents and
- Toxins.

Hart (2014) uses in his classification the following concepts:

- Vesicants (blister agents),
- Blood agents,
- Choking agents,
- Incapacitants (psychotomimetic agents),
- Organophosphorus nerve agents,
- Tear gas (riot control agents) and
- Vomiting agents (toxins).

Most of these are also included in the Ganesan's classification (Ganesan et al., 2010), as follows:

- Nerve agents,
- Vesicants (blistering agents),
- Bloods agents (cyanogenic agents),
- Choking agents (pulmonary agents),
- Riot-control agents (tear gases),
- Psycho(to)mimetic agents and
- Toxins.

According to these classifications (Hart, 2014), CW agents cause, for the most part, irritation of the skin and blistering; uncontrolled tearing; severe damage to the eyes, throat and lungs, leading to intensive long-term treatment; the inability to transfer oxygen from the blood to the body's tissue, rapidly becoming fatal; interference with breathing; physical disability; mental disorientation; constipation; headaches; hallucinations; the slowing of mental thought processes; respiratory failure and cardiac arrest, leading to death if the exposure to the agent occurs at high doses, in enclosed areas or for extended periods. Also, dual-purpose chemicals (Hart, 2014) that have been used as both TICs and CWAs have similar effects. For example, chloropicrin, hydrogen cyanide, PFIB, phosgene and acetone are used by common industries such as mining and in the production of insecticides, acrylic fibers, nylons, synthetic rubber, Teflon, polyurethanes and plastic products as well as plastic additives and other feedstock, solvent and drying agents. The same chemicals have earlier been used as warfare agents, causing uncontrolled lachrymation, respiratory failure and death. In general, pathogenic exposure to CWAs and TICs can happen in the form of physical skin contact by absorbing through the clothes and skin or by inhaling or swallowing toxic gas, liquid or other poisonous materials. The tox-

icity of chemical agents, the dose and length of exposure and the way in which they invade the human body and organs together define what kind of treatment casualties need. If the toxic mixture is not known when casualties are found, treatment will be initiated according to the symptoms and biomarkers that known chemicals typically have. Biomarkers are also used for defining and verifying the chemicals having caused the dramatic incidence with a varying number of casualties.

The threat caused by CWAs and TICs can be detected either by directly noting the presence of bare chemicals or by observing various shells or containers; dispersing, launching, transportation or manufacturing equipment; or stores or other related articles indicating the current or recent presence of these chemicals. The presence of bare chemicals can be identified via various monitoring systems and automated or human-operated sensors, which are installed and used for protection, rescue and defence purposes. The active searching and investigation of related materials requires authorized permission for forensic investigation in domestic cases and an international agreement and resolution by the United Nations for inspectional interventions into other countries. CWAs and other toxic chemicals appear in their basic forms, according to each chemical's characteristic features in a solid, liquid or gaseous form, and they can be dispersed (Ganesan et al., 2010) as a gas, liquid or aerosol or as agents adsorbed into particles to become a powder. When they are released in the open air, some evaporate or degrade into other components. Degradation products can also be toxic. Their typical physical form, persistence, volatility and solubility in water define how they can be used, stored, transported, dispersed and exposed. The same features also determine how long, whether at all, how and with which technologies the toxins can be detected, identified and verified during and after a chemical accident or attack and how the contamination can be defined and cleaned. If the primary agent no longer exists in a pure form at the location, the detection of precursors and degradation products can help in defining the influencing agent.

Based on their volatility (Ganesan et al., 2010), CWAs are classified as persistent or non-persistent agents. The more volatile an agent, the quicker it evaporates and disperses. For example, for the organophosphorus nerve agents, sarin (CDC, 2013) is the most volatile, soman the next and tabun the third most volatile nerve agent, whereas VX is a less volatile and thus persistent agent. Of other types of CWAs (Ganesan et al., 2010), for example, chlorine, phosgene and hydrogen cyanide are more volatile and non-persistent agents, and sulfur mustard is less volatile and a more persistent agent. On grounds of its chemical features and its being the most volatile (CDC, 2013), the nerve agent sarin will remain on exposed surfaces for the shortest period of time, while soman and tabun will remain on surfaces longer compared with sarin and for a shorter period of time compared with VX. As sarin (CDC, 2013) evaporates quickly from a liquid into a vapor, it spreads easily into the environment, especially to low-lying areas, by creating a greater exposure hazard there. People can be exposed to it through skin or eye contact, or by breathing contaminated air. Sarin also

mixes easily with water, and following the release of sarin into water, people can be exposed by touching or drinking water that contains sarin. In general (CDC, 2013), people may be exposed to the agent in a liquid or vaporized form by inhaling, swallowing or having other skin contact with contaminated air, water, food or other contaminated surfaces or objects. Also, people's clothing can release sarin after it has come in contact with sarin vapor, which can lead to the exposure of other people. In a container, sarin has a relatively short shelf-life (NWE, 2008) and will degrade over a period of several weeks to several months. The shelf-life may be greatly shortened by impurities in precursor materials. Sarin (NWE, 2008) can also be found stored as its two precursors, methylphosphonyl difluoride and a mixture of isopropyl alcohol and isopropylamine, which form the ingredients of a binary chemical weapon.

The most important chemical reactions (OPCW, 2015) of nerve agents take place directly at the phosphorus atom. The P-X bond is easily broken by nucleophilic reagents, such as water or hydroxyl ions (alkali). In an aqueous solution at neutral pH, the nerve agents decompose slowly, whereas the reaction is greatly accelerated following the addition of alkali. The result is a non-toxic phosphoric acid. The formation of the non-toxic phosphoric acid (OPCW, 2015) is also accelerated by a rise in temperature or by a catalyst (e.g., hypochlorite ions from bleaching powder). This hydrolysis forms the basis of most decontamination procedures utilizing decomposition. It can also be assumed that an area exposed to high volatility (G-series) nerve agents decontaminates itself within a few days. However, low volatility (V-series) agents may remain on the ground for several weeks because of their greater stability with respect to water and their much lower volatility. At pH-levels between 7 and 10, large quantities of VX are transformed into an extremely non-volatile product of hydrolysis, which is incapable of penetrating skin. This is less toxic than VX but still implies a risk during decontamination.

2.1.2 Explosives

Explosives are substances or devices that can be made to produce a volume of rapidly expanding gas in an extremely brief period (Johnson, 2015). This sudden release of a large amount of energy also creates a shock wave that can cause substantial damage in the environment (Welker, 2016). Explosives are the most common and easily available type of CBRNE materials and thereby pose a considerable security risk in all societies. In some classifications, explosives are separated from other types of destructive materials with indications such as CBRNe or CBRN. Nevertheless, explosives are powerful materials that can produce extreme material damage and large numbers of human casualties and injuries. Explosives can also be used and placed in a way that they cause large-scale further damage by secondary causes. Outside the military sector, explosives are used widely, for example, in the mining and construction industries. Civilian and commercial use is regulated by law, and for a grounded reason private citizens may be granted permission to buy and use them to a limited extent. Explosives can also be created from other ordinary substances whose

availability is not controlled by law. For example, ammonium nitrate (Pubchem, 2005) and potassium nitrate (KNO3, 2015) are easily available compounds that are known for their dual use as a fertilizer and industrial component; however, they are also know particularly as a source material for explosive mixtures.

There are three fundamental types of explosives: mechanical, nuclear and chemical (Johnson, 2015). Related to these explosive types, there are also three different kinds of explosions, including (Welker, 2016) nuclear, chemical and physical explosions. Nuclear materials are a special type of explosives that are usually not available to civilians, and it is also very difficult to create nuclear explosions without special knowledge and facilities. Nuclear explosions also produce huge human and material damage, and, outside of nuclear tests, they have been used only in warfare in WWII. In this text, nuclear explosions are discussed further in a section related to nuclear materials. The most common type of preplanned explosions are chemical explosions, evidently because of their relatively easy access and ease of use. Many explosives are, however, unstable compounds (Welker, 2016), and when their chemical reaction has started, it can usually not be stopped.

Chemical explosions (Welker, 2016) can be decomposition or combination reactions. Both are heat-producing exothermic reactions where the released energy causes the wanted effects. Decomposition reactions occur in materials that contain oxygen. Some examples of these are trinitrotoluene (TNT) and nitroglycerine. The decomposition of molecules creates high temperatures, producing combustion gases. The volume of gases is much larger than the volume of the explosive, which generates high pressures at the reaction zone. The rapid expansion of gases forms a shock wave that provides the explosive effect. Also, some hydrocarbons that have no oxygen, such as acetylene, can decompose explosively. In combination reactions (Welker, 2016), two or more components react together exothermically to produce hot gases. Some examples are ammonium nitrate and fuel oil (ANFO), gunpowder (potassium nitrate, carbon and sulfur) and fireworks.

In physical explosions (Welker, 2016), no chemical or nuclear reaction occurs. They happen usually when either gas or liquid exists under high pressure in a container, and the container breaks. In a broken container, the pressurized content is free to expand, and a shock wave is formed. Liquids that have a normal boiling point well below ambient temperatures (Welker, 2016) are sometimes stored under their own vapor pressure at pressures well above atmospheric pressure. If the tank bursts, part of the liquid vaporizes extremely rapidly and expands, forming a shock wave. This process is called a boiling liquid expanding vapor explosion (BLEVE), and the resulting explosion can be very destructive.

Explosions can also be classified as detonations and deflagrations. Explosions (Welker, 2016) where the shock wave moves faster than the speed of sound are called as detonations, whereas explosions with shock waves slower than the speed of sound are called deflagrations. Detonations also are more destructive than deflagrations because of their stronger shock waves. Detonations (Johnson, 2015) are usually produced by detonating high explosives and defla-

grations by deflagrating low explosives. Typical examples of detonating explosives are TNT and dynamite, which are characterized by extremely rapid decomposition and the development of high pressure. Common type of deflagrating explosives, black and smokeless powders, merely involve fast burning and produce relatively low pressures. Under certain conditions, such as the use of large quantities and a high degree of confinement, some normally deflagrating explosives can be caused to detonate.

The damage (Welker, 2016) caused by an explosion depends partly on how fast the explosive reaction occurs. Decomposition reactions generally occur much faster than combination reactions. They also have a stronger shattering effect (called brisance) than combination reactions. Decomposition reactions are more likely to be used for military applications and combination explosions in mining operations. There is also (Welker, 2016) a vapor cloud explosion that can occur when a fuel, for example propane, is mixed with the atmosphere. If the cloud is ignited, the burning rate may be fast enough to form a shock wave. The shock wave may be lower compared to other explosions, but it is still strong enough to damage or destroy structures.

Explosives cause accidents in industry and agriculture, defence and security and traffic and transportation as well as in individuals' personal lives. Also, old unexploded ammunitions from wartime cause accidents, either because they have been left unnoticeably in the environment or because people illegally collect and store them. In addition, other accidents such as fires and earthquakes can create massive explosions if they reach explosives stockpiles. Explosives are also quite commonly used to deliberately cause harm, confusion and destruction for various targets. General reasons for delinquencies with explosives are homicide, suicide, extended suicide, sabotage, criminal damage, terrorism and war. Quite often criminal acts are made with homemade bombs. Of these, two of the most disastrous examples from recent years were made of ammonium nitrate and fertilizers, such as the one used in the Oklahoma bombing in 1995 and the other in Oslo in 2011 (Lallanilla, 2013).

In addition to the immediate threat that explosions cause with the shock wave, fire, shrapnel and collapsing constructions, the toxicity of explosives may also create a health risk for people and the environment. Health risks may appear immediately or over the long term in direct or near contact with explosives, their source materials, decomposition products or explosion residues. In principle, there may also be a chance that toxic agents are able to transfer to humans through the food chain. Typically, the toxicity of explosives is found in soil in military test areas and in current and former war areas. The effects of the toxicity of explosives can be researched, for example, through the reproduction and mortality of species in contaminated soil. For instance, Phillips et al. (2004) investigated the toxicity of RDX and TNT to soil invertebrate Collembola in five natural soils and came to the conclusion that the soils' physical and chemical properties may alter the toxicity of RDX and TNT. The investigation indicates also that the soil with the highest organic matter and clay contents sustained the least and the soil with lowest organic matter and clay contents the greatest RDX

or TNT toxicity to Collembola reproduction. Relating to mining environments, Harris et al. (2003) have studied the suspected carbon monoxide poisonings and fatalities near blasting areas in the U.S. and Canada and carried out further tests with the gaseous detonation products from emulsions, a water-gel and ANFO blasting agents as well as gelatin dynamite, TNT, and Pentolite boosters. In the study, the main finding for these explosives is the high CO production associated with the lack of afterburning in an oxygen poor atmosphere.

Explosives manufacturing plants, mines and other licensed blasting sites, warehouses and transportation create a risk for severe accidents, where the explosion risk and involved toxic chemicals are usually known. Elsewhere, the usage of explosives is oftentimes illegal and hazardous, and it is urgent to detect explosives before they burst. The problem is that if someone wants to cause a disaster, explosives are rarely left openly within sight. More likely, explosive devices are packed in a bag or package, and basically no explosive matter is left outside the package. Explosive devices can also be hidden in the ground, a car, a building, an airplane or other places where the package may not be seen without searching and without knowing what to search for and why. In routine inspections, such as in border control, explosive devices may be found on the basis of their cover material, form and other indication, which gives a reason for suspecting the presence of explosives. These inspections are usually made with metal indicators, physical inspection, X-rays and signal detection. Also, trained animals are used widely, especially dogs in urban areas and rats in mine fields, where a rat can search a 200 m^2 area of landmines in only 20 minutes compared with doing the same with a metal detector taking usually two to four days (CNN, 2015). Outside routine inspections, in ad hoc situations, suspicious packages are possibly noticed first and explosives after that in a deeper inspection. If there is no warning or hint of explosives, there is, however, a risk that they will not be noticed before they explode. Screening devices are able to detect many kinds of explosive devices and substances, but seemingly none of them can reveal all possible explosives in all thinkable situations. If, for example, there is no metal in the explosive device and if it is hidden, many detection methods will be unable to find it. Some detectors may also be built for identifying some certain explosives only and cannot detect other explosive mixtures. If, despite camouflage, some traces of the explosive matter are exposed on the package, the chances for detection are better. Even a small volume of explosive matter may help identification, and precautions can be taken to prevent damage. Identification may be based, for example, on a physical sample of the trace or on an air sample of the vapor.

2.1.3 Biological, radioactive and nuclear agents

Biological, radioactive and nuclear materials and agents are extremely disastrous when they are misused and released into the environment. Many of them are pathogenic to humans and are classified as WMDs. Biological agents (OSHA, 2016) include bacteria, viruses, fungi, other microorganisms and their associated toxins. They have the ability to adversely affect human health in a variety of ways, ranging from relatively mild, allergic reactions to serious medical condi-

tions, even death. These organisms are widespread in the natural environment, and they are found in water, soil, plants and animals. Because many microbes reproduce rapidly and require minimal resources for survival, they are a potential danger in many environments. Biological warfare agents (Thavaselvam and Vijayaraghavanare, 2010) are micro-organisms, such as viruses, bacteria, fungi, protozoa or toxins produced by them, which give rise to diseases in man, animals or plants when deliberately dispersed in an area. These agents can incapacitate a large number of people in the shortest possible time by causing large-scale mortality, morbidity and other adverse effects on human health.

The use of bacteriological methods of warfare was prohibited by the Geneva Protocol in 1925 (UNODA, 2015). However, the agreement did not ban the possession or development of biological weapons, and therefore a process for a new agreement was started. A draft (UNOG, 2016) of the Biological Weapons Convention (BWC) was opened for signature in 1972, and it entered into force in 1975. The multilateral disarmament treaty bans the development, production, acquisition, transfer, retention, stockpiling and use of biological and toxin weapons and is a key element in the international community's efforts to address the proliferation of WMDs. As of 2016, BWC (UNOG, 2016) has 173 states parties and nine signatory states.

Radioactive agents are, according to U.S. law (Justia, 2015), any radioactive substances, materials or products, or any components or compounds thereof, which are naturally occurring, cultivated, engineered, processed, extracted or manufactured and which are capable of causing death or substantial bodily harm, the substantial deterioration or contamination of food, water, equipment, supplies or material of any kind, or substantial damage to natural resources or the environment. Radioactive agents also have useful purposes such as in medicine. Their usage has been guided since 1928 by the International Commission on Radiological Protection (ICRP) (ICRP, 2016), which is an independent, international, non-governmental organization for providing recommendations and guidance on radiation protection. There are also national bodies, such as the Radiation and Nuclear Safety Authority (STUK) in Finland (STUK, 2016), that supervise nuclear and radiation safety. The purpose of STUK is "to protect people, society, the environment and future generations from the detrimental effects of radiation."

Nuclear materials are sources for or by-products of producing nuclear energy, which is liberated (NTI, 2016) by a fission or fusion nuclear reaction or by radioactive decay. Nuclear energy is produced and used for industrial purposes, and the production is regulatory. Against international recommendations, nuclear materials are also used for the production of nuclear weapons. Regulated nuclear materials are (NRC, 2015) special nuclear material that consists of uranium-233 or uranium-235, enriched uranium, or plutonium, source material which is natural uranium or thorium or depleted uranium that is not suitable for use as reactor fuel and by-product material, which, in general, is nuclear material (other than special nuclear material) that is produced or made radioactive in a nuclear reactor. By-product material also includes the tailings and

waste produced by extracting or concentrating uranium or thorium from an ore processed primarily for its source material content. A nuclear weapon is (NTI, 2016) a device that releases nuclear energy in an explosive manner as a result of nuclear chain reactions involving the fission, or fission and fusion, of atomic nuclei. Such weapons (NTI, 2016) are also sometimes referred to as fission-based atomic bombs, as boosted fission weapons that are fission-based weapons deriving a slightly higher yield from a small fusion reaction or as hydrogen bombs/thermonuclear weapons that are weapons deriving a significant portion of their energy from fusion reactions.

In 1957 (IAEA, 2016), the International Atomic Energy Agency (IAEA) was established under the mandate of the United Nations to encourage the development of peaceful applications for nuclear technology, provide international safeguards against its misuse and facilitate the application of safety measures in its use. A key motivation for this was the need to prevent the usage of nuclear weapons after the nuclear bomb used in WWII in 1945. Eighteen ratifications by independent countries were required to bring the IAEA's statute into force, and as of 2016 the number of memberships is 167. Since 1957, several other agreements have been signed for banning, for example, nuclear missiles and nuclear tests. Nuclear tests were at first banned partially in 1964, and in 1996 (NTI, 2016) a Comprehensive Nuclear-Test-Ban Treaty (CTBT) was opened for signature at the UN General Assembly for prohibiting all nuclear testing in all environments. Signatures and ratification are required from, for example, North Korea, Pakistan, India and Saudi Arabia for the agreement to enter into force.

Biological agents have been used in recent years in terrorist attacks in the U.S. related to the September 11th attack in 2001, when letters with anthrax (FBI, 2015a) were mailed to various people, killing five and infecting 17 people. Several pathogenic bacteria such as Ebola and SARS also exist in nature and can develop into serious epidemics and pandemics. The most recent Ebola outbreak in West Africa (WHO, 2016) was declared to be over by WHO on January 14, 2016, but new flare-ups are likely to occur. It was possible to make the announcement as within over two years' period no new cases had emerged in any of the three epidemic countries in 42 days.

One of the very first known cases of radiation as a cause of death can be found in the experience of Marie Curie (BIO, 2016), who died of aplastic anemia in 1934, evidently caused by prolonged exposure to radiation in her scientific work. Also, her daughter, Irène Joliot-Curie (Encyclopedia Britannica, 2015), was exposed to radiation and died from leukemia in 1956 after working as a scientist with radioactive substances like her mother. In addition to these kinds of occupational accidents, radioactive agents have been used to cause deliberate deaths. In 2006 (BBC, 2015d), Russian dissident Alexander Litvinenko died from radioactive polonium-210 poisoning, claiming to have been murdered. Also, the Palestinian leader Yasser Arafat (Berenson, 2015) was claimed to have died from radiation in 2004, as high levels of polonium where found in his personal effects after his death. Arafat's body was exhumed for investigation in 2012, and in 2015 French judges ruled that there was not sufficient evidence to prove

that he had been poisoned. Earlier (Chrisafis and Sherwood, 2013), Swiss scientists had found in forensic tests unexpectedly high levels of radioactive polonium-210, at least 18 times higher than usual, in Arafat's ribs and pelvis and in soil that had absorbed his bodily fluids, suggesting the Palestinian leader could have been poisoned with the rare and lethal substance.

Massive amounts of radioactive material were released into the environment unintentionally in a nuclear power station accident and fire in Chernobyl, Ukraine, in 1986 (NRC, 2013) and after an underwater earthquake and tsunami in Fukushima, Japan, in 2011 (IAEA, 2011). The human, material, environmental and economic effects were huge. There have also been several smaller nuclear and radiological accidents around the world in which IAEA has provided support and assistance to its member states. Reports (IAEA, 2016b) have been made of the following accidents:

- radiological accident in Nueva Aldea, Chile, 2005
- accident involving an industrial radiography source containing Ir-192 in Cochabamba, Bolivia, 2002
- radiological accident in Lia, Georgia, 2001
- accidental overexposure in an oncology center's radiotherapy in Bialystok, Poland, 2001
- radiological accident in Samut Prakarn, Thailand, 2000
- serious radiological accident when a welder in error put an Ir-192 industrial radiography source in his pocket for several hours, Yanango, Peru, 1999
- serious radiological accident when two packages used to transport Co-60 teletherapy sources were sold as scrap metal, Istambul, Turkey, 1998 and 1999
- physicist severely exposed as a result of a criticality accident with an assembly of highly enriched uranium at a nuclear center, Sarov, Russian Federation, 1997
- radiological accident when sealed radiation sources were abandoned by a previous owner at a site against regulatory safety procedures, Lilo, Georgia, 1997
- serious accident at a combined cycle fossil fuel power plant in Gilan, the Islamic Republic of Iran, 1996
- accidental overexposure of radiotherapy patients at a hospital in San José, Costa Rica, 1996
- three members of the public entered a radioactive waste repository without authorization, removed a metal container enclosing a radiation source and one put it in his pocket in Tammiku, Estonia, 1994
- major radiological accident at a plutonium extraction facility in Tomsk-7, Russian Federation, 1993

- radiological accident at an electron accelerator facility in Hanoi, Vietnam, 1992
- fatal radiological accident at an industrial sterilization facility in Nesvizh, Belarus, 1991
- fatal radiological accident at an industrial irradiation facility in Soreq, Israel, 1990
- radiological accident at an industrial irradiation facility near San Salvador, El Salvador, 1989
- tragic accident resulting from the misuse of a strongly radioactive medical teletherapy source not under radiation protection surveillance in Goiânia, Brazil, 1985.

Moreover, large amounts of radioactive materials have been released into the environment deliberately in warfare and in nuclear tests. Nuclear weapons (UNODA, 2016) are the most dangerous weapons on earth, and they can destroy a whole city, potentially killing millions, and jeopardizing the natural environment and lives of future generations through their long-term catastrophic effects. Although nuclear weapons have only been used twice in warfare in the bombings of Hiroshima and Nagasaki in 1945, reportedly about 22,000 nuclear weapons still remain in the world today. There also have been over 2,000 nuclear tests conducted to date. Disarmament is the best protection against such dangers, but achieving this goal has been a tremendously difficult challenge.

One of the most recent (IAEA, 2016c) nuclear tests was conducted on January 6, 2016, by North Korea with a claimed hydrogen bomb, and it was internationally strongly condemned. Hydrogen bombs, also called thermonuclear weapons, are fusion bombs and thus more powerful than the fission type bombs used in WWII. With this test (Taylor, 2016), North Korea possibly became the ninth country in the world to have tested the fission bomb. Also, India's (Levy, 2015) strong intentions toward nuclear weapons have caused international concern of late, as they are suspected to be building a massive facility to produce thermonuclear weapons. Due to this substantial amount of nuclear activity around the world (Borger, 2016), the risk of a nuclear catastrophe is, according to former U.S. Defense Secretary William Perry, who served in the Pentagon, greater than it was during the Cold War and is still rising. Perry has listed Pyongyang's aggressive atomic weapons program as one of the greatest global risk factors, and in his view the nuclear catastrophe may incur in a regional war or a terrorist attack or by accident or miscalculation.

Biological, radiological and nuclear threats have in common the fact that they can be detected as bare substances at the stage when they are released into the environment. None of them can, however, be detected with human senses such as sight or smell. A special technology is needed for the detection, and if biological agents or radiation appear in unexpected places where automatic detectors or routine inspections do not exist, contamination will possibly be noticed only after symptoms appear on people. Control inspections can also be

performed if the threat has been detected somewhere else and if there is a reason to believe that it can also exist in another place. Radiation will usually be measured from the air, surfaces or other objects that have been exposed. Also biological agents can be measured from air samples, surfaces or other contaminated materials and objects.

Biological agents and radiation spread through the air, touching, inhaling and through food, and at this stage they can basically not be stopped. In open air, radiation can drift long distances with the wind and contaminate the environment, people, livestock, food and other materials in areas far from the original source. If, however, biological or radiological sources are released in smaller doses indoors, the building can be isolated and the threat diminished. Nuclear radiation is usually released in an explosion, which produces a huge toxic cloud that will drift in various directions with the wind. In nuclear energy power plants, smaller doses of radiation may also be released accidentally inside the building, where it can be isolated if the process is not overheated and out of control and if higher volumes of radiation are not released into the environment, such as in the ventilation or cooling water.

2.2 Responsible authorities and generic models for CBRNE countermeasures and defence

2.2.1 Getting prepared for emergencies

CBRNE countermeasures are organized and pre-planned safety measures, which are carried out to prevent, to mitigate and to respond to the consequences of CBRNE disasters during the whole life cycle of crisis. The term CBRNE defense is also used. The time scale of carrying out countermeasures can vary, because some crises escalate and last longer than others. Societies also need to be continuously prepared for CBRNE threats. Precise countermeasures are decided upon and carried out according to the actualization and development of each crisis.

Generic life cycles of the management of emergencies

In generic emergency and crisis management models, crises are often described as happening in cycles. In this way of thinking, the management of crises is also seen as a cyclic process, which entails the continuity of moving on from one crisis and being prepared for another. A plain version of a generic cyclic model contains the following four stages:

- preparedness,
- response,
- recovery and
- prevention.

Variations of the generic model exist depending on the context and user, and, for example, the prevention stage is sometimes presented together or instead of mitigation, such as in the model of the University of California, Davis (UC Davis, 2011). In addition, recent discussion on the management of disasters and crises has emphasized the importance of resilience, especially in relation to the underwater earthquake, tsunami and nuclear disaster near the Honshu Island and Fukushima in Japan in 2011 and the earlier Asian tsunami in 2004. After the multi-catastrophe in Japan, the significance of early planning and investing in building up resilience was also noted in the global framework for disaster risk reduction 2015–2030 (UNISDR, 2015), which was adopted and published in the Third UN World Conference on Disaster Risk Reduction, held in Sendai City, Japan, in 2015. In generic crisis management models, resilience may be included, for example, in the stage of preparedness or as a part of prevention/mitigation of the effects of crises.

Generic crisis management models seem to refer more to frameworks of managing injurious incidents in formal organizations and societies that have clear borders rather than to open communities without any formal connections. In these models, crises are assumed to happen in established societies more or less frequently, although generic models cannot define the exact point in time of the next emergency, or the type, frequency or likelihood of the possible crisis. With the crisis management models implemented, organized societies are to some extent able to deal with earlier known threats and less prepared for rare and unexpected risks. Known risks can be forecasted, budgeted for and prepared for with some certainty in advance according to earlier experiences and frequently repeating incidents. Some major risks may also be prepared for by knowledge that is obtained and maintained for particularly disastrous and potential events, even if they would never have taken place in the area. For example, societies are experienced in and prepared for the management of natural disasters that take place frequently in the same areas. States with chemical industries, atomic energy production and the like are also prepared for industrial and nuclear disasters, even if no major accidents have taken place on their own premises. However, societies may invest less in preparing for unlikely events such as extreme changes in the weather, big objects falling from the sky or radical terrorism in historically peaceful and democratic societies.

In general, preparing for crises is the mathematical, economic and value-based balancing between the severity and likelihood of threats, average human and material losses, costs for preparing for threats, the wealth of the society and all other investments and services that societies need to pay for on a regular basis. Choices need to be made between investments in certain and uncertain incidents, of which some would be useful, whereas the others would have a chance to prevent greater loss while simultaneously holding the risk of losing the entire amount of money. For example, if a new public emergency warning system would cost 100,000 monetary units per year, equating two million over 20 years, the society needs to decide whether it is worthwhile to pay the 100,000 per year and warn people immediately of possible emerging threats or whether

it would be more profitable to spend the money on something else, such as on people's wages, healthcare or elderly care. If the money were to be put, for example, into people's wages or elderly care instead of emergency warning, people would have in total 100,000 more monetary units more to spend in a year, or some of the elderly people would have a little bit better care, while at the same time some people might die or become permanently injured, or houses might be burned down, because the citizens were not warned in time of the threats due to the lack of a warning system. If, however, money were be spent on the warning system, people's wages and elderly care would stay as the same, and possibly a few or more human lives would be saved and injuries and material losses prevented thanks to being able to warn people in time with the new system. If instead no emergencies were to take place during the year, or if people failed to heed the system, the payment on the system would be lost.

In the U.S., the Federal Emergency Management Agency (FEMA), which operates under the management of the Department of Homeland Security, applies a five stage model for missions on emergencies and crises (FEMA, 2010):

- preparedness,
- protection,
- response,
- recovery and
- mitigation.

This is a broad approach to crises and covers all domestic disasters, whether natural or manmade, including acts of terror. The primary mission of all stages is to reduce the loss of life and property and to protect the nation from all hazards. The University of California, Davis (UC Davis, 2011) applies a narrower and more specific variation of the cyclic crisis management model of FEMA, as their emergency and continuity management plan focuses on the named threats that have been identified as possible and likely for their organization. Based on organizational analysis, the UC Davis emergency management plan prepares for countering specifically the following six kinds of crises:

1. Animal/Crop ecoterrorism,
2. Workplace violence,
3. Fires in lab buildings or residential halls,
4. Disturbances at public events,
5. Active shooters, car bombs and
6. Wildland fires, high winds and flooding.

The management of unexpected emergencies

Outside generic cyclic models and implemented emergency management plans, there are also crises that are exceptionally difficult to handle and of which most societies do not have previous experience. Reasons for such extreme disorder

are, for example, sudden natural disasters that have not been forecasted, expected or prepared for. Excessive harm can also be caused by unconventional, mixed and bizarre forms of violence, which strain the society with several means, targets and dimensions at the same time. Some of these are so obscure that military scientists have been re-thinking the definition of war and the signs of the start of war. These kinds of phenomena are typically related to the concepts of terrorism, hybrid warfare, asymmetric warfare, information warfare and cyber warfare, which have all dominated headlines in the media and professional discussion, especially in 2015 (ISMS, 2015; NBC, 2015; NOAS, 2015).

Compared with homeland security and conventional warfare, mixed and bizarre types of violence blur the line between internal and external threats and between a stable state and a state of emergency. A mixed situation can take place, for example, when a foreign state conducts cyber-attacks and information warfare against the government, private organizations and civilian people within another country by causing operational, economic, political and mental harm at all levels of the society. In a more severe form, these operations can also include physical provocation or terrorism, possibly conducted by third parties. Non-cyclic and unexpected disorder can also arise when the crises become prolonged and do not end within a reasonable timeframe. Governments can also become involuntarily mixed up in international crises when criminals enter the country through dishonest means. An overwhelming situation may also be created when masses of people enter the country on humanitarian grounds, triggering riots and additional social and economic problems in the area. Prolonged crises are exceptionally difficult if they lead into a permanent state of fear or if they change in a negative way the political system, societal order or the international relations of the country. Due to international interdependences, in a broad context the crisis is also always on, although not all the time at the same level on each country's own ground.

Many of the unexpected emergencies are likely to involve CBRNE, which requires broad and highly specialized preparedness by many authorities and organizations. Readiness for and knowledge about managing and countering CBRNE crises cannot be created/obtained easily and quickly, and they also cannot be maintained without continuous training. True practice is created only through real rescue operations and rehearsals, which all require different measures depending on whether the crisis is caused by chemical, biological, radioactive, nuclear or explosive matters. Recent international events, especially in 2015 and 2016, have shown that the security situation may also change rapidly in areas that had previously been considered safe, and severe CBRNE risks may suddenly appear in unexpected areas. Signs of this in 2015 were, for example, the existence of chemical weapons outside government programs in the Middle East, the increase in terrorism and the threat by ISIS to use the chemical weapons in Europe.

In severe and overwhelming CBRNE incidents, governments may request additional help from other countries and areas. However, as in CBRNE incidents, the first response is critical for survival and the mitigation of injuries. It is urgent that CBRNE knowledge and preparedness be available in every country.

It should also be noted that CBRNE knowledge and preparedness is needed in modern societies not only for homeland security but also for delivering aid in international crises. Many governments have joined various allies in international humanitarian aid, peacekeeping and defense, and, due to these connections, practically no countries are solely involved in their own domestic crises. The same interdependences may also imply that, if a major security incident were to take place on a country's own ground, other nations might accordingly participate in solving the crisis.

Another reason for the increased need for CBRNE knowledge and preparedness is that in the international context, the number and forms of military actors have increased. Along with these players, the possibility of even more brutal forms of hostile actions toward governmental and civilian targets has also increased. International agreements for peace and the prohibition of WMDs have not been fully followed, especially in the Middle East, over the last few decades and years, which in turn increases the risk for CBRNE threats in other areas as well. Terrorist attacks are also often internationally planned and managed through the Internet, which increases the risk that CBRNE threats will spread from their original areas into more peaceful and neutral areas.

In homeland threats, the police are usually the managing authority, and along with them the rescue service, health authorities, hospitals, radiation surveillance organizations and defence forces are involved in taking control over the crisis. In the prevention of CBRNE threats, international cooperation is usually needed, especially in the form of intelligence services. International cooperation may also be needed in the management of actualized large-scale CBRNE emergencies. A recent example of this is the nuclear power plant crash and radioactive release in Japan after an underwater earthquake and tsunami in 2011. Various crises also tend to become extended, as has recently happened in Syria and Iraq. With these kinds of crises, the international peace keeping operations also become dragged out, and frequent CBRNE incidents are possible. The responsible actors in international operations are particularly the United Nations and humanitarian organizations, with the help of international operative forces.

2.2.2 Strategies and joint operation for CBRNE countermeasures and defence

The execution of CBRNE countermeasures is based on appropriate and comprehensive strategies and operating concepts. These are needed as normal procedure in civilian societies in case of accidents, and they are also covered in military defence strategies. In general, the countering of CBRNE incidents belongs to the responsibility of homeland security, with the police in charge. The role of civilian and military actors, however, seems to be emphasized differently in CBRNE strategies depending on the experience, potential risk and the defence strategy of the country. Guidelines for national CBRNE strategies are typically formed according to memberships in wider alliances such as the European Union and NATO, even though individual countries may still have their own features in their strategies depending on local conditions.

The European Union, NATO and some other individual states have a slightly different emphasis in their CBRNE defence/countermeasure strategies and operating concepts. In the NATO alliance countries, the military actors' role is strong, as they follow the operating concepts of NATO, where military expertise and joint operations with ally countries are emphasized strongly. NATO also aims at predicting and preventing CBRNE incidents (Lefebvre, 2015), which is the European Union's goal as well.

The European Union is not a military alliance, so there is no clear and common CBRNE defence strategy for these countries. The European Commission (EC, 2014) is, however, promoting and conducting member states in following good practices in detecting and mitigating CBRNE risks. It is also convinced that, if necessary, effective and professional relief can be brought to a member state in need through the coordinated support from the commission and other member states. According to the gap analyses conducted by the commission, CBRNE preparedness is very different in individual member countries, and each country has been advised to improve their capabilities in case of these risks. Many EU countries are also members in NATO, which offers them the chance to utilize both NATO's CBRNE strategy and the European Commission's support. The European Union (EC, 2014) aims at better CBRNE risk assessment and the development of new countermeasures that take into account, for example, the following:

- the efficiency and capability of the detection equipment and processes;
- substances that create a new risk;
- new operating procedures and behaviors related to CBRNE strikes;
- new covering methods used in security inspections and
- new targets, such as soft targets, critical infrastructure, public spaces etc.

The neutral and non-allied countries follow varying strategies. For example, Austria (Baum, 2015) is trying to prevent nuclear accidents by fully declining the production and usage of nuclear energy, and Switzerland (SFOE, 2015) has announced plans to phase out nuclear power after the crisis at Japan's Fukushima nuclear plant in 2011. Before the peacetime accident in 2011, Japan had also experienced major nuclear catastrophes during the war in 1945. Evidently for that reason, Japan has shared their experiences in crisis management internationally, especially after the Fukushima accident. In overall safety, Japan has built a post-war alliance with the United States in addition to their Self-Defence Forces (Marcus, 2015).

The two other neutral countries in Europe, Finland and Sweden, have a different nuclear energy policy from those of Switzerland and Austria as well as a different defence policy from that of Japan. In Finland and Sweden, nuclear energy is used for peaceful purposes, and preparedness for nuclear accidents and radioactive releases is maintained in any case. Thus far there have been no serious INES-rated (IAEA, 2015) nuclear accidents in the two countries, yet radioactive fallouts have taken place, caused by severe CBRNE incidents across borders. Nuclear radiation fallouts have drifted to Finland from other countries,

for example in 1986, after the Chernobyl accident and earlier after foreign nuclear tests in the 1980s and in 1945–1963 (STUK, 2016b). The radiation level was highest one year after the Chernobyl accident in 1987, when the average country-wide cesium-137 fallout was around 11 kBq/m^2 (STUK, 2016c). The average cesium-137 level in each person in the country in that year was around 2,000 becquerels and in the highest radiation areas around 4,000 becquerels per person. Currently (in 2016) the average cesium level per person is approximately 200 becquerels (STUK, 2016b).

For updating preparedness, in Finland a CBRNE joint operation forum was formed and a national counter-terrorism strategy (Intermin, 2010) was created in 2009–2010 for managing criminal CBRNE risks as a part of the government's second homeland security program for 2008–2015. A new strategy for national counter-terrorism (Intermin, 2014) for 2014–2017 was published in 2014. Together with the foundation of the CBRNE joint operation forum, the cooperation, preventive measures and joint operation models of different security authorities were developed for various threat scenarios. Practical development work in this area was based on previous incidents of bomb threats, suspicious postal matters and letters containing what turned out to be flour (Heiskanen, 2010). Operative work has been carried out by the Helsinki Police Department, the Preparedness Group and the Counter-Terror Group of the police. Also, the Helsinki City Rescue Department and many other CBRNE specialists from various authority organizations have participated in the development work of the CBRNE joint operation forum and in the creation of the counter-terrorism strategy. At the government level, work to create a new national CBRNE strategy was started in spring 2015 (Nerg, 2015). There are also other national strategies and documents on internal, external and comprehensive security, which complement and support the countering of CBRNE threats.

In general, CBRNE threats practically always necessitate authorities' joint operation in some form, regardless of whether the operation is domestic or expeditionary in nature. Joint operation partners can be domestic and foreign military or civilian authorities or other civilian organizations. The strategy must also be supported with an approved written operating concept. The operating concept includes, among other things, the capabilities and technologies needed for taking care of a given CBRNE situation. The strategy should also be proactive rather than reactive. Proactive refers to the newest high quality detection technologies (EC, 2014), intelligence activities (Lefebvre, 2015) and sound overall preparedness. Executing a CBRNE strategy also means that it is always in play. Although the generic crisis management concepts of prevention, preparedness, response and recovery may give the impression that societies return to a normal state after crises emerge and are handled, with CBRNE threats there is no non-active state. The threats exist in many ways and in many places, and societies need continuous multidimensional operations for detecting and preventing the multiple risks.

CBRNE strategies must also be continuously developed further (EC, 2014). Although the possible risks of industrial facilities, such as nuclear energy power

plants, are well known and covered, the current world situation has become so unpredictable in CBRNE matters that new operating procedures and new detection and safety technologies need to be developed and implemented all the time. One essential reason for this is the internationally rapid increase of overall terrorism, which reached the highest recorded level ever in 2014. The dramatic incidents in Europe in 2015 are not included in the statistics, but as early as 2014 (GTI, 2015) the total number of deaths from terrorism increased by 80% from 2013 in the reported 162 countries, which also is the largest yearly increase in 15 years. In 2014, as much as 32,685 people died from terrorism globally, compared with only 3,329 deaths in 2000. According to the broadest systematic coding, the number of all registered deaths from terrorism globally in 15 years or more is around 140,000 and probably higher including the deaths that have not been booked (GTI, 2015). For a comparison, in total 437,000 people get murdered each year, which is over 13 times more than how many die from terrorism globally. Also, compared with the death rate of 32,685 from terrorism in 2014 globally, in the U.S. in 2013, 41,149 (about the same rate) people died from suicide, 56,979 from influenza and pneumonia, and, much more, 611,105 from heart disease and 584,881 in cancer (CDC, 2015). To compare with Finland, counting all causes of death, in total 51,500 people died in the country in 2013, of which around 19,500 died from cancer and 12,300 from cardiovascular and heart diseases (STAT, 2014).

Terrorism (GTI, 2015) has for several years been focusing intently in five countries: Iraq, Nigeria, Afghanistan, Pakistan and Syria. The violent activity, however, is spreading rapidly, and in 2014 nearly 60% of the reported countries experienced some kind of terrorist incident. Such incidents took place in 2013 in 88 and in 2014 in 93 of the reported 162 countries. The number of killings from Boko Haram increased aggressively by 317% in 2014, resulting in more than 6,600 deaths, whereas at the same time ISIS caused the deaths of over 6,000 people. At the international scale, additional safety measures need to be taken, especially because of the increased criminal and brutal activity in areas such as the Middle East, which also induces additional criminal acts in other parts of the world. Criminality has also become technically more intelligent, which together with the large economic funds obtained by criminal means creates an even bigger risk. With these resources, criminals can develop new threats and new ways of hiding their operations and of encrypting their discussions and plans until it is not possible to prevent these devastating acts.

To keep CBRNE strategies up-to-date and ready for action, CBRNE operations must also be rehearsed repeatedly with multiple threat scenarios and operating procedures. If the procedures are not exercised, especially with joint forces, they will not work properly in a real situation (Valtonen, 2010).

To summarize, well-developed national CBRNE strategies call for the following:

- authorities' joint operation,
- an approved operating concept with acknowledged capabilities and technologies,

- a proactive approach,
- be always in play,
- continuous development and
- continuous training and rehearsals.

2.2.3 Operating concepts for CBRNE countermeasures and defence

The need for and nature of CBRNE countermeasures operating concepts

Military actors traditionally have had the greatest knowledge of CBRNE materials, as many of these are not used at the civilian sector. Military actors have also for the same reason produced specific operating concepts for CBRNE countermeasures and defence. Due to the dual use of explosives, toxic chemicals and radioactive materials for industrial purposes, knowledge of CBRNE materials has also been created outside the military sector. This knowledge may, however, not always be organized as particular operating concepts in the civilian sector, and in countries such as Greece, the responsibility of countering CBRNE threats has also been left to the defence forces during the peacetime.

In the light of history since World War I, and due to the accidents and deliberate usage of CBRNE materials against civilian populations, it looks like the need for qualified and organized CBRNE countermeasures operating concepts outside the military sector would have been increasing. For example, after World Wars I and II since the 1980s, chemical weapons have again been used repeatedly against civilians in the 1990s and after year 2000, especially in the Middle-East area. After the 2010s, chemical weapons have also ended up in organized terrorists' hands, which significantly changes the nature of the CBRNE threat. There are also reported cases of private activists, such as the usage of sarin in the Tokyo metro, who have been able to produce toxic gas to violate the civilian population. Along with these incidents, WMDs are no longer in the control of governments only, and for this reason their usage is neither negotiable nor controllable in the same way as earlier with government operators. Instead, with the increase and rise of organized terrorist groups and their knowledge and facilities to gain and produce chemical weapons and other WMD materials as well as due to the appearance of technically advanced lone wolf extremists, the CBRNE threat has become even more unpredictable and is also found in areas and targets where it had not previously been expected. At the same time, the nuclear threat has not ceased either, as it is currently being used in political rhetoric by more than one state as a deterrent for other nations. Also, nuclear weapons tests are still carried out, even though they are prohibited. Meanwhile biological weapons have also been used against civilians, particularly in 2001. In addition, the industrial risks for CBRNE exist and are increasing rather than decreasing all the time, and even nature's role in igniting CBRNE disasters, such as in Fukushima in 2011, cannot be ignored. All these reasons point out that the CBRNE threat, even in its worst form as the deliberate usage of WMDs against civilian populations, is possible at any moment basically in any country, regardless of whether it is a time of peace or war. For this reason, the knowledge and practice of CBRNE countermeasures

need to be extended from the military sector to the broader society, and valid operating concepts need to be brought into use by the civilian protection and rescue authorities as well.

When the needs and requirements for CBRNE countermeasure and operating concepts are considered, one should also note the different nature of various countermeasures. Even though these activities are mainly physical actions for protecting and rescuing people from a physical threat, they also include technology assisted processes. Technologies that can support particularly knowledge-based and mental processes needed in CBRNE countermeasures may, according to common knowledge, include particularly digital, electronic and optical devices and applications. On these grounds, CBRNE countermeasure and defence procedures are divided into a) physical and b) information technology assisted activities. Accordingly, capability requirements for CBRNE countermeasures and defence are classified further in the text as a) physical capability requirements and b) information technology assisted capability requirements.

In this context, information technology assisted activities and procedures refer to tasks that can, on the part of their core activities, be fulfilled with the assistance of information technology, with information systems and/or with electro-optical devices and systems, whose data can be assessed, processed, presented, stored and delivered digitally in many ways and for many audiences and purposes.

Here, as a part of the broader category of digitalized information technologies, electro-optical devices and systems are (Farlex, 2016) technologies associated with components, devices and systems designed to interact between the electromagnetic (optical) and the electric (electronic) state. In this context, electro-optical devices are also capable of producing digital data that can be processed with other information technology devices and systems. As a comparison, optoelectronics (Merriam-Webster, 2016) refers to a branch of electronics that deals with electronic devices for emitting, modulating, transmitting and sensing light. These devices are also capable of producing digital data to be processed with other information technology devices. In this context, electro-optical systems include but are not limited to optoelectronic devices and systems.

The share of information technology-assisted activities of CBRNE countermeasures is significant, and due to the overall digitalization of society, it can be expected to continue to increase. Compared with physical activities, information technology-assisted activities' importance is also emphasized by their capability of being operable both on-site at the place of the emergency as well as at a distance in different places, especially in the incident's reachback center. In this context, attention is paid particularly to information technology's role in the assessment and detection of the CBRNE threat and to the information technology-assisted management of CBRNE emergencies.

In the following, the generic features of military CBRNE defence operating concepts are presented with the reduced versions of the EDA's and Canadian Armed Force's CBRNE defence operating models and the main principals of civilian CBRNE countermeasures with NATO's countermeasure guidelines for

civilian actors in case of CBRN incidents. In these models below, such activities which can, according to the author's evaluation, be carried out with the assistance of various information technologies are printed in *italics*, as a separation from physical countermeasures. In addition, activities which can be supported with detection technologies are marked by the author with *(d)*. Accordingly, activities which can be supported with more ordinary information technologies are marked by the author with *(i)*. Activities which are printed as normal text without other notes are classified as physical activities. Activities related to the medical treatment of victims and patients are not dealt in a more detail in this context.

Military operating concepts for CBRNE defence

The European Union has been moving toward an executable operating model through various steps for several years. For example, in 2008 the EDA carried out a multinational rehearsal of a combined IED/CBRN threat situation (EDA, 2008), which showed that a multinational mission is a tough call to make and that there is no single simple solution available. In the following year, in 2009, a CBRN Action Plan (EU, 2009) was published for the following three to five years. The document was mainly a political agenda and a development plan of the identified weaknesses and desired objectives of the CBRNE protection of that time. By 2015, more progress had been achieved, as can be seen in the EDA's approved outline of the new CBRNe Defence Concept from 2014 (EDA, 2014).

The CBRN Action Plan (EU, 2009) defines the capabilities that are required at the main level for CBRN protection in Europe. The three main strands are:

- Prevention: ensuring that unauthorized access to CBRN materials of concern is as difficult as possible.
- Detection: having the capacity to detect CBRN materials to prevent or respond to CBRN incidents.
- Preparedness and response: being able to efficiently respond to incidents involving CBRN materials and to recover from them as quickly as possible.

The outline of the new CBRNe Defence Concept from 2014 (EDA, 2014) updates and upgrades the three strands and defines five stages of countering a CBRNe incident, on which appropriate countermeasures are built. The stages are

- Deter,
- Prevent,
- Protect,
- Respond and
- Recover.

Of these, "Deter" is not mentioned in the earlier Action Plan, and also the other stages are defined more precisely in the new text. In addition, the outline

of the new CBRNe Defence Concept identifies the capability requirements for individual soldier protection, for non-specialist unit protection and for the protection provided by specialist CBRNe defence capabilities. The main level capability requirements of the European model are presented in Table 1.

TABLE 1 The main level capability requirements of the CBRNE defence concept of the EDA

CAPABILITY REQUIREMENTS FOR CBRNE DEFENCE (EDA)
• *Detection, Identification and Monitoring (DIM) (d)*
• Physical Protection
• *CBRNe Advice and Assessment, including CBRNe Intelligence (i)*
• *CBRNe Information Management (i)*
• *CBRNe Warning and Reporting and CBRNe Reachback (i)*
• Hazard Management, including Decontamination
• CBRNe Consequence Management
• CBRNe Hardening
• CBRNe Medical Counter Measures

In Table 1, the requirements are divided into two categories: Those capabilities that are produced mainly by physical activities, for example fortification of buildings (hardening), are printed as normal text. As a separation from physical activities, those capabilities that can be produced with the support of various information technologies, are printed in *italics*. This classification is made on the basis of the author's previous knowledge. Evaluations are arrived at mainly by considering whether either various CBRNE detection technologies or data communication technologies are possible or required for carrying out the required tasks.

The Canadian CBRNE defence operating concept (CF, 2012) determines that to accomplish the CBRN defence mission and mandate, the capabilities described in Table 2 are necessary for fulfilling the required tasks. The requirements in the table break down into more detailed qualifications.

TABLE 2 The main level capability requirements of the Canadian CBRNE defence concept

CAPABILITY REQUIREMENTS FOR CBRNE DEFENCE (Canada)
• *Detection, Identification and Monitoring (DIM) (d)*
• *Information Management (IM) (i)*
• Physical Protection
• Hazard Management
• Medical Countermeasures (Med CMs) and Support

In the CBRNE Defence concept of the EDA in Table 1 and in the corresponding model of the Canadian Chief of Force Development in Table 2, the information technology-assisted requirements are printed in *italics*. Of these, *Detection, Identification and Monitoring (DIM)* deals mainly with the detection of CBRNE substances, whereas *CBRNe Advice and Assessment including CBRNe Intelligence, Information Management (IM)* and *CBRNe Warning and Reporting and CBRNe Reachback* are activities carried out with more ordinary information technologies, such as focusing primarily on assessing, processing, transferring, delivering, representing and storing information and data. From here forward, the classification of information technology-assisted activities, and the capability requirements within them, are therefore simplified in the text into two categories, those focusing on CBRNE detection and those focusing on the information management of a CBRNE incident, as follows:

- Detection, Identification and Monitoring (DIM) and
- Information Management (IM).

This classification into two categories is also applied below to the civilian CBRNE countermeasures by identifying information technology-assisted activities with *italics*, detection tasks with (*d*) and information management activities with (*i*).

Civilian operating concepts for CBRNE countermeasures

In the CBRNE defence operating concepts above, the military actors' role is emphasized more than in ordinary homeland security issues. In this form, the countermeasure models do not take the civilian actors' role much into account. Within inhabited areas, the core protection activities in CBRNE incidents are still much the same regardless of whether the incident is caused by an internal or external threat. However, in homeland security, the civilian actors need to take a greater role than in the military operating models.

After the large scale terrorist attack in the U.S. on September 11th, 2001, the Euro-Atlantic Partnership Council (EAPC) nations decided (NATO, 2008) in the following year, 2002, to develop countermeasure guidelines for civilian actors in the case of CBRN incidents. The guidelines (NATO, 2008) were created and published by NATO's Civil Emergency Planning in 2008, and they are designed to improve multi-agency interoperability in the first response phase of a CBRN incident and to provide guidance on when regional, national or international assistance may be required. The response guidelines focus on actions required during the initial response phase in the first 20 minutes, and they are divided into the following four sections:

1. Information gathering: Gather, assess and disseminate all available information
2. Scene management: Isolate scene to mitigate consequences
3. Saving and protecting lives: Save lives, give warnings or manage evacuation
4. Additional/specialist support: Alert specialists, notify appropriate authorities, integrate specialist advice and resources

The required procedures within these sections are described in tables 3–6. In the tables, response procedures that can be produced with the support of information technologies are indicated by the author with *italics*. Procedures that require detection technologies are marked with *(d)*, and procedures that are carried out with other kinds of information technologies are marked with *(i)*.

TABLE 3 Required CBRNE response procedures for information gathering

1. INFORMATION GATHERING: Gather, assess and disseminate all available information
Call centres and mobilizing centres
• *Recognise that a CBRN incident has or may occur (i)*
• *Gather, assess and disseminate all available information to first responders (i)*
• *Establish an overview of the affected area (i)*
• *Provide and obtain regular updates to and from first responders (i)*
First responders/approach and arrival at scene
• Approach scene with caution and upwind
• *Carry out scene assessment (d)*
• *Establish Incident Command (each responding agency) (i)*
• *Recognise signs and indicators of CBRN incidents (d)*
• *Determine whether CBRN or hazardous material incident (d)*
• Estimate number of casualties/victims
• Estimate resource requirements
• Consider specialist advice/resource requirements
• *Provide situation report to emergency control rooms etc. and request assistance if necessary (i)*
• *Carry out risk assessment (d)*
• *Undertake hazard identification (d)*
• Do not approach or touch suspect objects/packages – do not operate radios, mobile phones or other electronic devices within vicinity (safe distance +/- 400 m)
• *Consider secondary devices/targets (d)*
• *Establish and agree upon multiagency response plan (i)*
• *Identify safe areas for additional first responder vehicles (d)*
• *Search for secondary devices (d)*
• Critical infrastructure considerations

TABLE 4 Required CBRNE response procedures for scene management

2. SCENE MANAGEMENT: **Isolate scene to mitigate consequences**
Initial
• Consider wind direction • *Establish multi-agency command point in safe area (cold zone) (d)* • *Establish inner and outer cordon (hot/warm/cold zone) (d)*
Containment
• *Contain contaminant material/liquid (d)* • *Establish quarantine (holding) area for contaminated victims/casualties (where necessary) (d)* • *Establish decontamination and triage areas (d)* • *Cordon off contaminated areas (d)*
Additional considerations
• Identify and establish multiagency marshalling area for additional resources • Establish traffic cordon • *Preserve scene and maintain evidence to the extent possible (criminal investigation) (d)* • *Carry out coordinated evidence collection (d)*

TABLE 5 Required CBRNE response procedures for saving and protecting lives

3. SAVING AND PROTECTING LIVES: **Saving lives, giving warnings or managing evacuation**
• Determine immediate actions and priorities • *Evacuate inner cordon (to quarantine area) (d)* • Restrict inner cordon access (protected first responders only) • Provide safe working methods for rescuers • Carry out necessary rescues • *Implement decontamination as appropriate (emergency, mass, clinical) (d)* • *Consider decontamination of personal property (d)* • *Implement medical triage and treatment (d)* • *Implement responder/rescuer decontamination (d)* • Consider requirements and provide transport for victims/casualties • *Provide timely warnings and advice to the public (immediate vicinity and beyond as necessary) (i)* • Consider evacuation (immediate vicinity and beyond as necessary) • Consider utility shutdown • Consider public order • Consider hospital defence (self-presenters)

TABLE 6 Required CBRNE response procedures for additional/specialist support

4. ADDITIONAL/SPECIALIST SUPPORT: **Alert specialists, notify approp. authorities, integrate specialist advice and resources**
Notification

Continues

Table 6 continues

- *Notify appropriate authorities at local, regional and national levels (governmental and responder agencies) (i)*
- *Notify specialists (chemical, biological, radiological/nuclear, medical) (i)*
- *Consider international support and conventions (IAEA, WHO, OPCW) (i)*
- *Provide situation reports to all notifications (i)*

Assessment

- *Prepare impact assessment (en route/on site) (i)*
- *Establish effect on population (i)*
- *Establish effect on critical infrastructure (i)*
- *Establish effect on environment (i)*
- *Carry out incident-specific and environmental sampling (d)*
- *Hazard prediction (i)*
- *Dispersion modeling (i)*
- *Radiation monitoring (d)*
- Consider emergency provision requirements for immediate and wider area
- *Assess resource requirements (short, medium and long term) (i)*

Integration of support

- *Specialist advice and/or additional resources to be incorporated into incident plan (i)*

Substance identification

- *Substance confirmation (d)*

Victim/casualty support

- *Provide information to hospitals (i)*
- Provide clinical countermeasures
- *Provide information to general practitioners (i)*
- *Provide health surveillance (short–medium term) (i)*
- Provide emergency accommodation
- *Establish casualty bureau (i)*

Information to public

- *Implement communication plan (i)*
- *Provide timely warnings or advice to public (i)*
- *Provide regular updates (i)*
- *Provide health advice to public (i)*

Site decontamination/restoration and remediation

- *Decontaminate responder vehicles/equipment (d)*
- *Decontaminate hospitals (d)*
- *Recover and decontaminate contaminated bodies (d)*
- *Decontaminate/restore affected buildings (d)*
- *Decontaminate and remediate impact on environment (d)*
- Dispose of medical waste
- Dispose of site waste/rubble

Post-incident and long-term considerations

- *Provide multi-agency debriefings for all responders (i)*
- *Provide psychological counseling for victims and responders (i)*
- *Provide long-term health monitoring (victims and responders) (i)*

In the following, the capability requirements for detection-based DIM and information management-based IM procedures are viewed in a more detail in sections 2.3 and 2.4. In both sections, requirements are presented separately for military and civilian procedures.

2.3 Capability requirements for the detection, identification and monitoring (DIM) of CBRNE threats

2.3.1 Capability requirements for CBRNE detection in military models

In the CBRN defence operating concepts of the EDA (EDA, 2014) and Canadian Chief of Force Development (CF, 2012), detection, identification and monitoring (DIM) cover three major responsibility areas, which include

1. reconnaissance and survey,
2. identification and
3. monitoring.

These responsibility areas (with explosives [E] added by the author) include more detailed capability requirements (CF, 2012), which are presented in Table 7. Requirements are coded by the author with DIM M1-9, where DIM indicates that the requirement deals with CBRNE detection, whereas M notes that the requirement is defined in the military CBRNE defence operating concept. Individual requirements are numbered 1–9.

TABLE 7 Capability requirements for the military CBRNE detection

CAPABILITY REQUIREMENTS FOR MILITARY CBRNE DETECTION
CBRNE reconnaissance and survey
• DIM M1: Verifying the hazard prediction area • DIM M2: Surveying to determine the extent of liquid and particulate CBRNE hazard • DIM M3: Operating in built-up areas
CBRNE identification
• DIM M4: Identifying CBRNE agents • DIM M5: Stating the concentration of the identified hazard • DIM M6: Indicating the greatest risk • DIM M7: Providing spectral data
CBRNE monitoring
• DIM M8: Monitoring contaminated areas and • DIM M9: Operating in built-up areas

2.3.2 Capability requirements for CBRNE detection in civilian authority models

CBRNE response procedures in the civilian guidelines for CBRNE countermeasures (NATO, 2008) that can be carried out with the support of detection technologies are presented in Table 8. In the table, requirements are coded by the author with DIM C1-29, where DIM indicates that the requirement deals with CBRNE detection, whereas C notes that the requirement is defined in the civilian CBRNE countermeasures operating concept.

TABLE 8 Civilian CBRNE countermeasures that require detection technologies

1. INFORMATION GATHERING:
Gather, assess and disseminate all available information
First responders/approach and arrival at scene
• DIM C1: Carry out scene assessment (d)
• DIM C2: Recognise signs and indicators of CBRN incidents (d)
• DIM C3: Determine whether CBRN or hazardous material incident (d)
• DIM C4: Carry out risk assessment (d)
• DIM C5: Undertake hazard identification (d)
• DIM C6: Consider secondary devices/targets (d)
• DIM C7: Identify safe areas for additional first responder vehicles (d)
• DIM C8: Search for secondary devices (d)
2. SCENE MANAGEMENT:
Isolate scene to mitigate consequences
Initial
• DIM C9: Establish multi-agency command point in safe area (cold zone) (d)
• DIM C10: Establish inner and outer cordon (hot/warm/cold zone) (d)
Containment
• DIM C11: Contain contaminant material/liquid (d)
• DIM C12: Establish quarantine (holding) area for contaminated victims/casualties (where necessary) (d)
• DIM C13: Establish decontamination and triage areas (d)
• DIM C14: Cordon off contaminated areas (d)
Additional considerations
• DIM C15: Preserve scene and maintain evidence to the extent possible (criminal investigation) (d)
• DIM C16: Carry out coordinated evidence collection (d)
3. SAVING AND PROTECTING LIVES:
Saving lives, giving warnings or managing evacuation
• DIM C17: Evacuate inner cordon (to quarantine area) (d)
• DIM C18: Implement decontamination as appropriate (emergency, mass, clinical) (d)
• DIM C19: Consider decontamination of personal property (d)
• DIM C20: Implement medical triage and treatment (d)
• DIM C21: Implement responder/rescuer decontamination (d)
4. ADDITIONAL/SPECIALIST SUPPORT:
Alert specialists, notify approp. authorities, integrate specialist advice and resources
Assessment

Continues

Table 8 continues

• DIM C22: Carry out incident-specific and environmental sampling (d)
• DIM C23: Radiation monitoring (d)
Substance identification
• DIM C24: Substance confirmation (d)
Site decontamination/restoration and remediation
• DIM C25: Decontaminate responder vehicles/equipment (d)
• DIM C26: Decontaminate hospitals (d)
• DIM C27: Recover and decontaminate contaminated bodies (d)
• DIM C28: Decontaminate/restore affected buildings (d)
• DIM C29: Decontaminate and remediate impact on environment (d)

2.4 Capability requirements for the information management (IM) of CBRNE incidents

2.4.1 Capability requirements for the information management of a CBRNE incident in military models

The information management type of requirements of the military CBRNE defence operating models of the EDA (EDA, 2014), NATO (Lefebvre, 2015) and the Canadian Chief of Force Development (CF, 2012) are presented in Table 9.

TABLE 9 Capability requirements for information management in military CBRNE defence

CAPABILITY REQUIREMENTS FOR INFORMATION MANAGEMENT IN MILITARY CBRNE DEFENCE
Information management requirements in Canadian operating concept
• IM M1: Warning troops endangered by CBRN hazard in near real time
• IM M2: Making a rough estimate of CBRN hazard area in near real time
• IM M3: Making an accurate hazard prediction
• IM M4: Determining the source of contamination
• IM M5: Distinguishing between an instantaneous hazard release and a continuous hazard release
• IM M6: Applying changing weather conditions to an existing hazard prediction area
• IM M7: Providing CBRN situational awareness applicable at strategic, operational and tactical levels
• IM M8: Providing CBRN-related decision support to commanders and staff at each level of command
• IM M9: Providing guidance for planning and execution of CBRN defence in all phases of operations at each level of command
• IM M10: Reaching back (to Canada) for specialized analysis and advice
• IM M11: Providing the means to manage the CBRN defence resources
Increments in the EDA's operating concept

Continues

Table 9 continues

• IM M12: CBRNe advice and assessment, including CBRNe intelligence
• IM M13: CBRNe warning, reporting and CBRNe reachback
Increments in NATO's operating concept: **Reachback**
• IM M14: Support across the full spectrum of operations
• IM M15: Provide CBRN-related technical and scientific reachback
• IM M16: Provide CBRN information service
• IM M17: Access to CBRN-related information (knowledge base)
• IM M18: Support to operational planning
• IM M19: Support from secondary network
• IM M20: Limited 24/7 support
Predictions, Warning & Reporting
• IM M21: CBRN analysis
• IM M22: Warning & reporting
• IM M23: Warning messages

In the above Table 9, requirements are coded by the author with IM M1-23, where IM indicates that the requirement deals with information management of the CBRNE incident, whereas M notes that the requirement is defined in the military CBRNE defence operating concept.

2.4.2 Capability requirements for the information management of a CBRNE incident in civilian authority models

The information management types of requirements of NATO's guidelines for civilian CBRNE protection (NATO, 2008) are presented in Table 10. In the table, requirements are coded by the author with IM C1-31, where IM indicates that the requirement deals with the information management of the CBRNE incident, whereas C notes that the requirement is defined in the civilian CBRNE countermeasures operating concept.

TABLE 10 Civilian CBRNE countermeasure procedures that require other information technologies

INFORMATION GATHERING: Gather, assess and disseminate all available information
Call centres and mobilizing centres
• IM C1: Recognize that a CBRN incident has occurred or may occur (i)
• IM C2: Gather, assess and disseminate all available information to first responders (i)
• IM C3: Establish an overview of the affected area (i)
• IM C4: Provide and obtain regular updates to and from first responders (i)
First responders/approach and arrival at scene
• IM C5: Establish incident command (each responding agency) (i)

Continues

Table 10 continues

- IM C6: Provide situation report to emergency control rooms etc. and request assistance if necessary (i)
- IM C7: Establish and agree upon multiagency response plan (i)

SAVING AND PROTECTING LIVES:
Save lives, give warnings or manage evacuation

- IM C8: Provide timely warnings and advice to the public (immediate vicinity and beyond as necessary) (i)

ADDITIONAL/SPECIALIST SUPPORT:
Alert specialists, notify approp. authorities, integrate specialist advice and resources

Notification

- IM C9: Notify appropriate authorities at local, regional and national levels (governmental and responder agencies) (i)
- IM C10: Notify specialists (chemical, biological, radiological/nuclear, medical) (i)
- IM C11: Consider international support and conventions (IAEA, WHO, OPCW) (i)
- IM C12: Provide situation reports to all notifications (i)

Assessment

- IM C13: Prepare impact assessment (en route/on site) (i)
- IM C14: Establish effect on population (i)
- IM C15: Establish effect on critical infrastructure (i)
- IM C16: Establish effect on environment (i)
- IM C17: Hazard prediction (i)
- IM C18: Dispersion modeling (i)
- IM C19: Assess resource requirements (short, medium and long term) (i)

Integration of support

- IM C20: Specialist advice and/or additional resources to be incorporated into incident plan (i)

Victim/casualty support

- IM C21: Provide information to hospitals (i)
- IM C22: Provide information to general practitioners (i)
- IM C23: Provide health surveillance (short–medium term) (i)
- IM C24: Establish casualty bureau (i)

Information to public

- IM C25: Implement communication plan (i)
- IM C26: Provide timely warnings or advice to public (i)
- IM C27: Provide regular updates (i)
- IM C28: Provide health advice to public (i)

Post incident and long-term considerations

- IM C29: Provide multi-agency debriefings for all responders (i)
- IM C30: Provide psychological counseling for victims and responders (i)
- IM C31: Provide long-term health monitoring (victims and responders) (i)

2.5 Additional requirements for the coverage of CBRNE countermeasures and defence

In addition to the functional requirements described above, there are also some other operative and technical requirements for CBRNE countermeasures. The applied technologies must, for example, be able to operate in many different environments and many environmental conditions. They also need to be operable over the entire timeline of the CBRNE incident, which is a much longer period of time than just the immediate operation at the CBRNE site. The timeline may also be divided into several different environments and places, depending on how early the threat is discovered and where. Also, the length and required workload of the recovery stage may vary, as some CBRNE sites can be cleaned and returned back to ordinary use, whereas others need to be closed and isolated for decades.

When CBRNE incidents take place in inhabited areas among the civilian population, CBRNE countermeasures and defence need to also take into account many issues and counterparts other than just the threat and the rescue/defence forces. The number of counterparts is large, especially in joint authorities' rescue operations among the civilian population, where non-authority civilian organizations and other volunteers may also act in a rescuer's role.

In the following, the technical requirements during the different stages of the timeline of a CBRNE incident are discussed in section 2.5.1, whereas the relations and roles of the different counterparts of a CBRNE incident are presented in section 2.5.2.

2.5.1 Technical requirements at the different stages of the timeline of a CBRNE incident

CBRNE detection, identification and monitoring systems must be able to operate at the different stages of the timeline of a CBRNE incident. Environments and other conditions at the different stages may vary, which also may require using different detection technologies and methods, including different operating platforms for the detecting devices. Concerning the feasible distance of CBRNE detection, different requirements can dictate the use of long-distance remote sensing devices or very near precision detection devices. In addition, the toxicity of the environment may necessitate the use of remotely controlled operating platforms instead of human-operated devices. During the timeline, there are also situations that require confirmation of the detection results in the laboratory.

The timeline of a CBRNE incident can be defined roughly in three stages. These are events that take place 1) before, 2) during or 3) after the blast, where the blast refers to an explosion or other type of release of CBRNE materials. Events that take place before the release of CBRNE materials are called pre-blast (or pre-incident) events, and things that take place after it are referred to as post-blast (post-incident) events. The starting and ending point of a distinct

CBRNE incident can usually be defined, for example, on the basis of the operating records of responsible authorities. For instance, the immediate incident may be defined as having started at the moment when the threat is noticed. Accordingly, it may be declared as having ended at the time when the immediate danger was over or when the place has been cleaned and the evacuation is over. It is also possible that the immediate incident is declared over even though the place is being isolated for several years due to the high toxicity, which cannot be neutralized or cleaned.

Referring to the cyclic crisis management models discussed in section 2.2.1, the countermeasures for CBRNE incidents can sometimes be understood as a continuous activity, or as a series of linear or cyclic events, which do not have an exact beginning or end. Even though the actualized incidents require immediate rescue operations, the countering of CBRNE threats also requires many other procedures long before anything happens and for a long time after it. Some of the most important beforehand activities are surveillance and intelligence, which in principle are carried out all the time, including during and after a concrete CBRNE incident. In addition, the monitoring of the threat may be carried out for a long time after the CBRNE release. In radioactive fallouts, the monitoring may continue for decades or years.

The detection, identification and monitoring tasks may be carried out in any or in all of the three stages of the timeline, before, during or after the CBRNE release, depending on

- how the CBRNE incident is happening,
- how strong it is,
- what the threat model is and
- what the reason for and objective of the detection are.

Pre-blast detection can be conducted, for example, as a result of active surveillance or search or on grounds of coincidental observation. At this stage, the detection of a leak or other traces of CBRNE materials is made before any major event has taken place. It is also possible that in a pre-blast situation, CBRNE materials do not appear as bare substances. Instead, they may be hidden or packed in some kind of containers or shells. They may also appear as precursors or other kinds of source materials or as parts of CBRNE production facilities. After the blast or major release has taken place, CBRNE materials are detected as bare substances, although many times in an altered form. For example, explosives appear at that stage usually as residue, whereas nuclear materials transform into radiation and smaller particles. In addition, chemicals may vaporize or degrade from their earlier form. The time scale for the vaporization and degradation depends on the chemical, volume and environmental conditions.

The following technical requirements in the Canadian CBRNE defence operating concept (CF, 2012) indicate, that the operative forces need to be prepared for the detection in various environments and conditions. All these qualities are also needed for covering the detection needs at all stages of the CBRNE

incident. In general, the detection, identification and monitoring system must be capable of (CF, 2012)

- providing systematic observation of aerospace and surface areas;
- examining objects to determine the presence of CBRN(E) hazards;
- passive and/or active operation;
- detecting while on the move;
- being locally or remotely controlled;
- operating with unattended sensors, which all must be networkable;
- detecting biological and chemical hazards and all levels and types of radiation, including when shielded, in liquid, solid and vapor forms and
- discriminating between local background activity and CBRN(E) threat activity, airborne CBRN(E) agents and airborne TIMs.

To cover the different needs at the different stages and environments of the timeline, detection technologies and systems must also, on grounds of the nature of CBRNE hazards and the practical knowledge of common technologies, be capable of

- long-distance remote detection and very close range on-site detection;
- human operated hand-held detection and automated/robotized ground-based and airborne detection;
- detection in all directions and not only, for example, downwards on surfaces;
- operating both indoors and outdoors;
- operating by taking samples and detecting targets directly without touching and
- transforming the sensor data into digital form and transferring it unaltered into alerting, reachback, documenting and other systems relevant for the management of the CBRNE incident.

Figure 5 lists the reasons and primary tasks for the detection at the different stages of the timeline of the CBRNE incident. At the pre-blast stage, detection and monitoring are carried out primarily for preventing major CBRNE incidents and for revealing accidents, criminality or the planning of a crime. When the CBRNE material has been already released, detection and monitoring are carried out for other purposes. At first, the released material needs to be detected and identified to protect first responders and other people nearby and to determine the appropriate rescue and medical countermeasures for casualties. At the same stage, identification and monitoring are also required to define the concentration, volume and spreading model of the released agent and to determine the hot spot or hazard zone, contamination and the actual spread of the contamination.

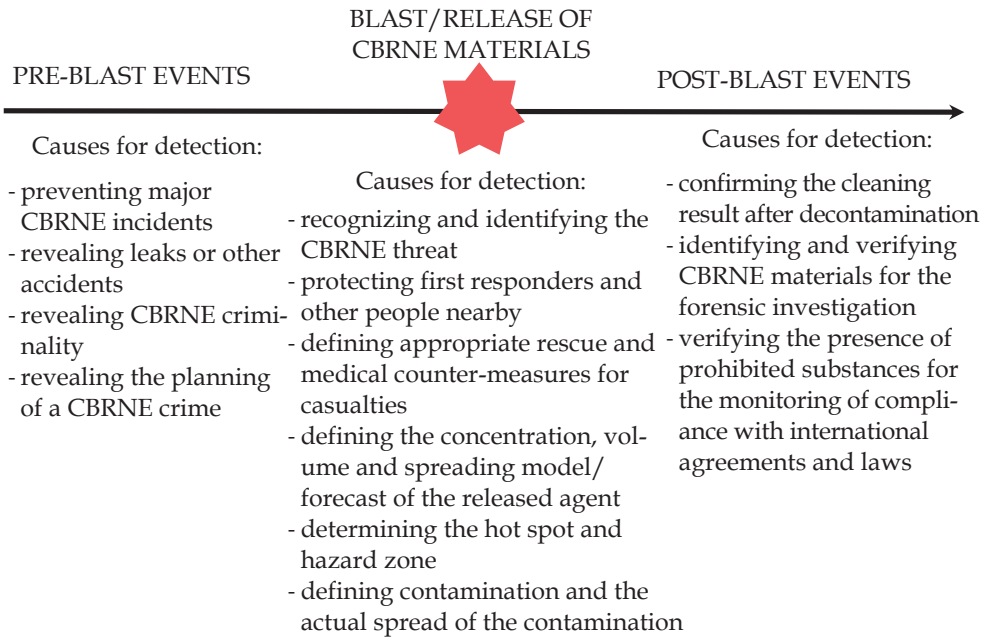


FIGURE 5 The causes for CBRNE detection at the different stages of the CBRNE incident

Later on, detection is needed after decontamination and cleaning to control and confirm the cleaning result. In addition, detection, identification and verification of CBRNE substances are required for forensic investigation and for the verification of the presence of prohibited substances. For the investigation, also other forensic marks than CBRNE traces are important, and, in principal, any details at a CBRNE site can be crucial evidence for solving a crime.

2.5.2 The roles and main DIM and IM activities of the involved counterparts

The previous sections discussed the CBRNE countermeasures and defence operating concepts of the EDA, NATO, Canadian Chief of Force Development and NATO's Civil Emergency Planning (EDA, 2014; Lefebvre, 2015; CF, 2012; NATO, 2008), presenting different models for the military and civilian detection of CBRNE threats and for the information management of CBRNE incidents. The main issue in all these models is the countering of a CBRNE threat, but the actors and their activities may vary between the models.

One part of the variance is related to the role of civilian actors and the civilian population during a CBRNE incident. In the military models, these are not much noted, obviously because military models were originally developed for battlefield situations, where the civilians should not exist. Severe CBRNE emergencies, however, also take place in the middle of the civilian population, and, in such situations, civilians need to be regarded in the countermeasures regardless of whether the rescue forces are military or civilian authorities.

During large-scale CBRNE incidents among civilians, rescue and defence organizations need to work together, and help may also be needed from various

civilian aid organizations. Assistance may also be needed from private citizens, who may be taken into account in the countermeasures not only as victims but also as individuals who can potentially support the management of the rescue operation. It is therefore necessary to view the military and civilian countermeasures operation models at the same time to see what kind of counterparts and roles are involved in the CBRNE incident. It is also useful to consider how the CBRNE detection and information management tasks are related among the different actors as well as what kind of information and communication needs the different counterparts have during the incident.

In the following, the military and civilian countermeasure models are merged into the same picture in Figure 6 first by selecting the key entities and actors from the four models (CF, 2012; EDA, 2014; Lefebvre, 2015; NATO, 2008) and by analyzing the different roles each counterpart may have during a CBRNE incident. After this, all studied counterparts and their different roles are represented visually in the same picture in Figure 7 by also including the previously discussed capability requirements and key detection and information management tasks. These holistic picture will facilitate a better understanding of the different actors' roles, relations and activities during a CBRNE incident.

As the counterparts, key actors and entities of the four military and civilian countermeasure models (CF, 2012; EDA, 2014; Lefebvre, 2015; NATO, 2008) are analyzed via the CBRNE detection and information management activities, presented above in tables 1–10, they can be categorized roughly as a) human actors, b) material entities and c) immaterial entities. The most relevant actors and entities of the models are classified into the three categories in Figure 6.

Human actors

- Troops
- First responders
- Commanders
- Staff
- General practitioners
- Specialists
- Resources (people)
- Authorities
- Hospitals (personnel)
- International support (IAEA, WHO, OPCW)
- Casualties
- Victims
- Public

Material/physical entities

- Hazard
- Source of contamination
- CBRNE agents
- Suspect objects
- Evidence
- Contaminated waste
- Contaminated bodies
- Affected buildings
- Scene
- Hazard prediction area
- Devices and Phones
- Resources (materials)
- Vehicles
- Hospitals (buildings)
- Environment and Wind
- Critical infrastructures
- Multi-agency command point
- Casualty bureau
- Quarantine area

Immaterial entities

- Notifications
- Messages
- Information
- Advice
- Reports
- Spectral data

FIGURE 6 Key actors and entities of the military and civilian CBRNE countermeasure models

After further analyzing the different counterparts of the four countermeasure models in Figure 6, one can notice that the listed entities and actors have different roles and forms during a CBRNE incident. For example, the CBRNE threat appears in Figure 6 at least in the following places and forms:

- source of contamination,
- hazard area,
- CBRNE agents,
- suspect objects,
- affected buildings,
- triage area,
- quarantine area,
- contaminated waste,
- contaminated bodies and
- evidence.

Also, the human actors have a variety of different roles during the incident. First, they can be classified in two main categories as a) rescuers and b) as those who are being protected and rescued. Both the rescuers and the protected and rescued individuals can be divided into further groups. Listed below are the different counterparts from the four countermeasure models in Figure 6, who represent in some way the rescuer's role. Some of them are carrying out immediate rescue operations at the emergency site, whereas others are conducting and giving specialist advice for the operation remotely from a safer location:

- troops,
- first responders,
- staff,
- commanders,
- general practitioners,
- specialists,
- resources (people),
- authorities,
- hospitals (personnel) and
- international support (IAEA, WHO, OPCW).

For conceptualizing the different duties of the rescuers, their operations can be described through the following generic roles:

- operative forces,
- command of the operation,
- operation management,
- reachback,
- reinforcement,
- (CBRNE) specialists,

- joint forces (national),
- (other/involved) authorities,
- (the personnel of) hospitals,
- international support (joint forces) and
- international (CBRNE) agencies (e.g., IAEA, WHO, OPCW).

The protected and rescued people in the countermeasure models in Figure 6 are the

- casualties,
- victims and
- public.

Of these, the casualties are dead and victims injured people. Both are present at the beginning of the immediate CBRNE incident in the hazard zone and can possibly be transferred into other areas during the rescue operation. The public usually means private citizens in general. During the CBRNE incident, the public can, depending on the situation and context, refer to the following groups of people:

- (alive) casualties/victims,
- survivors (who remain uninjured from the hazard),
- people in risk areas (to which the contamination may spread) and
- people who are in safe areas (where the contamination is not spreading).

As can be seen in Figure 6, there are also material and immaterial entities in CBRNE incidents. Material entities are various physical targets such as equipment, buildings, critical infrastructures, vehicles, substances and various other items such as suspected objects, evidence and contaminated waste as well as different environmental areas and natural targets, such as the wind. Immaterial entities are items that have a certain information content or other value and that do not necessarily have a physical form. In this context, immaterial entities refer mainly to relevant information and data, which can be transferred in a digital or other form.

All the actors in a CBRNE incident and their mutual relations and roles are described visually in the same chart in Figure 7. Also, the main capability requirements for the CBRNE detection and information management for each actor, selected from the four countermeasures models (CF, 2012; EDA, 2014; Lefebvre, 2015; NATO, 2008), are presented in the figure. Figure 7 is not meant to be a complete list of all potential real-world entities and actors or of their possible relations and capability requirements in a full-scale CBRNE incident. Instead, it demonstrates some essential features both of the military and of the civilian countermeasure models in the same view.

When the four models (CF, 2012; EDA, 2014; Lefebvre, 2015; NATO, 2008) are merged into the same schema, as in Figure 7, they form a new comprehensive

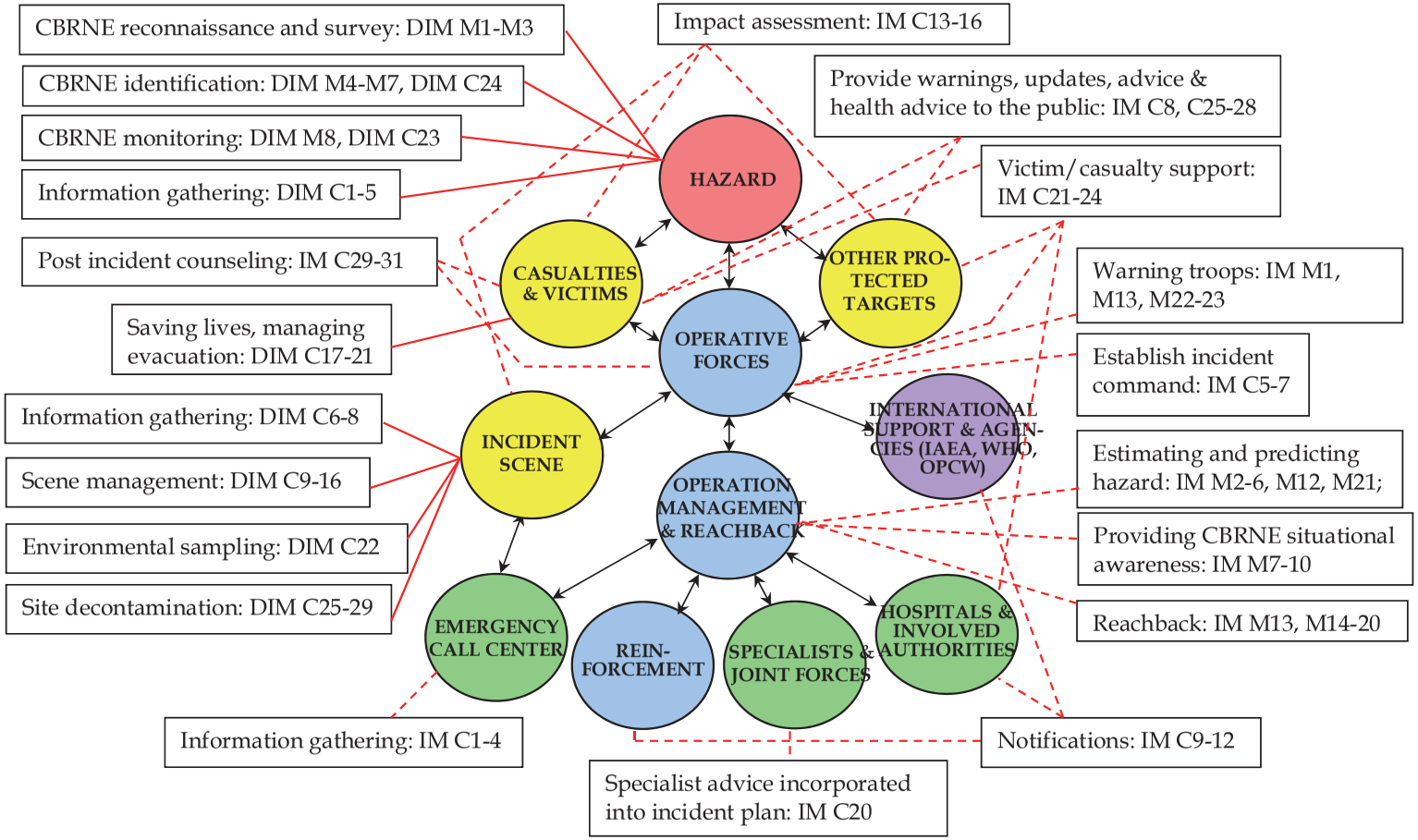


FIGURE 7 The main roles and detection and information management activities of the involved counterparts in a CBRNE incident

multi-authority approach to CBRNE threats, which covers all different threat scenarios and stakeholders of the four models at the same time. In principle, the merged model describes a maximal joint-authority countermeasure situation, where a severe CBRNE incident takes place among civilians and where different national authorities and international support are needed for help. The combined model also demonstrates the civilian non-authority counterparts', critical infrastructures' and environment's situation and role during the CBRNE incident, which is not necessarily seen clearly in the military models.

The model is capable of serving both single-authority and multi-authority CBRNE operations as well as internal and external threat situations. It is also capable of serving both the military and civil emergency authorities as well as civilian rescue and aid organizations such as the Red Cross and the like. Furthermore, it is able to take into account in various forms the civilian population, which is usually in a weak situation in a crisis. In this form, the merged comprehensive model is the broadest possible perspective of CBRNE countermeasures for a single state. Compared with this, more complex cooperation procedures are required only when international actors are needed for help in a domestic crisis or when domestic forces are called for help in an international crisis.

2.6 Feasible technologies for CBRNE detection

2.6.1 The background of the detection methods

The identification of substances within technical detection methods is traditionally based on analytical chemistry, which gives the most reliable result for the identification. Analytical chemistry is capable of defining through various qualitative and quantitative analysis methods the type and amount of smaller components in the researched sample, thereby identifying characteristic features that indicate the constitution of the sample. There are also instrumental methods, which identify substances on a basis of their physical features, such as absorption, photoluminence or conductivity.

Chemical analysis methods have traditionally been used in the laboratory, and they cannot always be used for the detection of CBRNE materials in the field environment. Transferrable mobile CBRNE laboratories are, however, built into a truck or a container, but these cannot always be brought into the CBRNE site. Due to the enormous destructive power and time-criticality of CBRNE materials, there is also a great need for reliable and rapid field detection methods. Many kinds of methods have already been developed and are in use, but it seems that the current methods are not satisfactory for all situations or are not feasible for other reasons, for example, by their lack of accuracy, lack of reliability or price.

When a toxic agent has been released, symptoms may appear on casualties after the exposure before the agent has been detected with a technical method. Symptoms can also indicate the possible agent, which can then be confirmed

with appropriate methods. The average rescue personnel may not, however, be able to identify at once the reason for symptoms, especially if they are not experienced in dealing with such agents. Due to these agents' rare and unlikely appearance, it is also possible that in many places there are no specified detection methods immediately available for all kinds of toxic agents.

2.6.2 Common technologies and methods in detecting CBRNE substances

The presence of CWAs can be recognized with various rapid on-site methods. Those available are (Ganesan et al., 2010), for example, handheld rapid detection devices, such as Three Color Detector (TCD) paper, the Residual Vapor Detection (RVD) kit and the Water Poison Detection Kit (WPDK). The TCD paper sticks to any surface and the color changes according to the specific agent within 30 seconds. However, according to Ganesan et al. (2010), the reliability of this method is not the best possible, as it may give false-positive results with many other substances. The RVD kit is a portable, disposable CW agent detector kit that can detect CW vapors in the air with a high specificity. The detection tubes are made of glass with break-off tips and are filled with impregnated chemicals on silica. A certain volume of air is sucked in via pump strokes, and the color change of the silica indicates the presence of a particular agent. Detection tubes are available for individual agents so that blister and nerve agents, such as phosgene, cyanogens chloride and hydrogen cyanide, in the atmosphere can be detected with this method. Similarly, poisonous substances present in water sources can be detected with the help of WPDK. This kit contains different reagents marked with numbers, test procedures for known CW agents and an indication of results based on simple color change for detection. All these devices (Ganesan et al., 2010) have several limitations, such as low specificity and inability to detect all CW agents. Definitive identification of an agent can be carried out on-site in a mobile analytical laboratory or in an off-site laboratory, and this will generally take many hours.

Other types of hand-held detection instruments are mainly based on three principles (Ganesan et al., 2010): ion mobility spectrometers (IMS), gas chromatographs (GCs) and surface acoustic wave sensors (SAWS). Hand-held chemical agent monitors, based on the principle of IMS, are the most common devices used for the detection of CW agents, particularly blister and nerve agents. The GID-3 (Smiths) is a British IMS for the on-site detection of common CW agents, whereas the GID-2A is another version for fixed locations designed for unattended operation and continuous monitoring. The hand-held improved chemical agent monitor (ICAM) is a portable IMS device. The M8A1 is another IMS-based automatic CW alarm detector that was used during the 1991 Gulf War, and it has been replaced with the Automatic Chemical Agent Alarm (ACADA), which is a high-resolution IMS. ACADA can detect agents in a few seconds and can clean itself for fresh detection within one minute. RAID (Bruker's) and M-90 (Environics) are other variants of IMS. Also, frequently used handheld detectors such as AP2C (France) and CHASE (Israel) are based on the flame photometry principle. The technology can detect the chemilumi-

nescent reactions of sulfur or phosphorus-containing organic compounds in a hydrogen/air flame. SAWS work in the same manner as quartz crystal microbalances (QCMs) but at higher frequencies and with greater sensitivities. The Joint Chemical Agent Detector (JCAD) employs a SAWS-based technology and it is hand-held and lightweight and combines with an electrochemical cell.

Portable gas chromatographs (Ganesan et al., 2010) are used for automatic, real-time, continuous agent monitoring where air is used as carrier gas and the air sample is drawn through a pre-concentrator loop filled with an adsorbent material. A photoionization detector (PID) is used to detect the agents, and the entire cycle from sample collection to detection takes about 5–10 minutes. A gas chromatograph coupled with mass detector (GCMS) fitted on a vehicle can be used for unambiguous detection of most organic compounds, including CW agents, at very low concentrations. However, this hyphenated technique is complex, requires a skilled operator, is difficult to maintain and does not provide much advantage in comparison with off-site analysis, especially when the chemical incident occurs at a remote site, where the mobile laboratory cannot approach easily. The commercially available portable GCMS-based instruments include HAPSITE (Inficon's), EM series (Bruker's), MM1 or MM2. No suitable on-site detection equipment or methods for the detection of psychomimetic agents are available except GCMS. In addition to electrochemical-based detectors for nerve agents (NAD) (Ganesan et al., 2010), standoff detection instruments (M21, RAPID) are also available. The M21 remote sensing chemical agent alarm (RSCAAL) is based on a passive infrared detector and is capable of detecting nerve and blister agents in the vapor phase from a distance of up to 5,000 meters. Development work has progressed on instruments that are based on other techniques, such as molecularly imprinted polymer (MIP) sensors, biosensors, surface plasmon resonance (SPR), conductive polymer sensors, etc. All detection methods (Ganesan et al., 2010) have susceptibility to interferences or false-positive results, and the best way is to use two types of detectors working on different principles to obtain accurate data.

Instrumental analysis methods also include hyperspectral imaging technology, which, in the identification of substances, utilizes their physical ability to absorb, transmit or reflect various wavelengths of light. The technology is widely used especially in remote sensing (Chang, 2003; Smith, 2012), where it can be used, for example, for the detection of minerals on the ground and for analyzing vegetation. Hyperspectral remote sensing applications can also detect other features and changes in the environment, such as (Telops, 2016) methane emissions, gas leaks, pollution, forest fires, industrial flares and the emission characterization of smokestacks. Hyperspectral defence and security applications include, for example (Telops, 2016), standoff chemical detection and the identification of surface contaminants, infrared countermeasures for ballistic threats, illicit and clandestine laboratory detection for explosives and drugs, unexploded ordnances detection, surveillance, explosion and material characterization and combustion and fluid dynamics as well as (ChemImage, 2016) non-contact, reagentless detection of multiple explosives simultaneously, in-

cluding their precursors and degradation products. In addition, hyperspectral technology has been demonstrated (ChemImage, 2016) for the rapid, non-contact optical sensing of chemical agents and hazardous materials, including CWAs, TICs and TIMs, and of biological agents without the use of reagents or enhancements.

2.6.3 Comparison of common field detection methods

When the traditional field-fit detection techniques for CBRNE are compared to define their capability for on-site CBRNE detection, the following pros and cons are found (Ganesan, 2010):

Three color detector papers

+ small, field-fit and inexpensive
+ fast, result obtained in 30 seconds
- requires physical contact with the agent
- works for certain agents only
- low specificity, may give false-positive results with other substances

Residual vapor and water poison detection kits

+ portable and disposal
+ high specificity
- requires an air/water sample being sucked with a pump in a glass tube
- water poison detection kit also requires reagents in the tube
- works for certain agents only

Ion-mobility spectrometry

+ most commonly used field-fit devices for CW agents
+ fast, result obtained in a few seconds
+ high-resolution versions available
+ self-cleaning versions available with ability for fresh detection within one minute
+ different versions available for hand-held and unattended fixed location detection
- requires an air sample drifted into the analyzer containing an electric field
- works for defined agents only
- works for vapors only

Portable gas chromatography and gas chromatography with mass spectrometry (GCMC)

+ portable gas chromatograph capable of automatic real-time continuous agent monitoring
+ relatively feasible sample collection and detection time (portable device), about 5–10 minutes
+ GCMC capable for unambiguous detection of agents at very low concentrations
- a photoionization detector is required for the detection of agents (portable device)
- adsorbent material required (portable device)
- air sample required (both solutions)
- GCMC complex technique, requires a skilled operator, difficult to maintain and does not provide much advantage in comparison with off-site analysis

Accordingly, on the basis of common knowledge and the author's own research on the generic features of the hyperspectral technology and the declarations of commercial technology providers having hyperspectral solutions on CBRNE (e.g., Telops, ChemImage), the various advantages and disadvantages can be found for the hyperspectral technology in this particular use:

+ non-destructive technology, capable of non-contact detection and identification without the need for reagents, other treatments or samples
+ capable of detecting substances in gaseous, liquid and solid forms
+ capable of defining contamination
+ capable of imaging investigated targets and for storing data for later use
+ capable of unattended stand-off detection, airborne detection and long-distance remote sensing
- sensitive to environmental conditions
- some of the commercial CWA detectors are built up of two different devices
- availability of small on-site detectors is limited

It should also be noted that with the generic hyperspectral technology, the term "detection" can refer in different contexts to different things, especially depending on the analysis software that the devices are associated with. Firstly, some hyperspectral devices and solutions may be able to notice the presence of substances, while at the same time not be able to identify and define them by name. Secondly, some solutions may be able to distinguish different substances from each other and yet not be able to identify them by name. Thirdly, hyperspectral technologies cannot alone, without dedicated analysis software, identify by name any substances unless a specified identification software is integrated or

embedded into the hyperspectral device. Fourthly, with the analysis software, hyperspectral technology can identify by name only those substances for which it has been built and trained in advance.

As all of the above-named technologies are either specified detectors or generic technologies capable of detecting (among other substances) CBRNE materials, they all can, within their own limits, identify at least some of the CBRNE substances, which is the minimum requirement for such devices. Most of them can also be expected to be suitable to be used in the three pre-blast, on-time and post-blast stages of the CBRNE incident timeline, described in Figure 5. However, it is obvious that not all of these detectors are capable of performing all of the previously described multidimensional functions or of fulfilling other technical requirements, which are defined as specific capability requirements for CBRNE reconnaissance and the survey, identification and monitoring of the Canadian (CF, 2012) or any other detection, identification and monitoring system of a CBRNE countermeasures and defense operating concept.

2.6.4 Conclusions on the instrumental CBRNE detection methods

Of the discussed CBRNE detection technologies, the instrumental analysis methods ion-mobility spectrometry (IMS), portable gas chromatography (GC), gas chromatography with mass spectrometry (GCMC) and hyperspectral imaging are the on-site CBRNE detection technologies with highest potential in terms of being able to produce a qualified detection result and being operable with various platforms in different situations and forms. However, they cannot perform exactly the same detection, identification and monitoring tasks, and possibly none of them alone can give the maximum potential protection against CBRNE threats.

Being used as widely as professional laboratory technologies, gas chromatography and mass spectrometry have high potential in giving reliable and qualified identification results. However, both are destructive analysis methods, which require a sample of the investigated target. They also cannot be operationalized easily for time- and mission-critical CBRNE field work. Ion mobility spectrometry (IMS) has been adapted to field use more successfully, and currently it is evidently the most widely used on-site technology for CW agents and is also able (Rapiscan, 2016) to detect explosive traces. One of the limitations of ion mobility spectrometry in field use, however, is that it can analyze only air samples and vapors, except for wiping samples of surfaces such as in the case of identifying explosive traces.

In addition to the primary detection and identification of substances, hyperspectral technology can, based on its general features, author's own research and information that is reported by commercial technology providers, be expected to be capable of performing the following detection, identification and monitoring tasks, which the other technologies discussed, for the most part, cannot do:

- detect and identify substances without taking a physical sample
- detect and identify substances non-destructively without contact, reagents or other treatments

- in addition to vapors, also detect and identify liquids and solid materials
- in addition to air, detect and identify substances on surfaces, with and without taking wiping samples
- image the detected targets and store both the images and the spectral identification data of the targets in a reusable digital form for later use
- operate in a laboratory form, as an unattended standoff, hand-held and ground-based robotized device, on a manned and unmanned airborne operating platform, and as a remote detection device with variating distances from ground to air and from air to ground
- detect, define and monitor contamination in a scalable manner from microscopic details to large environmental areas
- serve various motivations and needs for carrying out detection at all stages of the CBRNE incident timeline, for example:
    - before the blast in the early detection of threat to prevent a CBRNE incident
    - at the on-site stage for the detection of the presence of CBRNE substances to protect rescuers and the surrounding people
    - after the blast for the identification of toxic agents for prescribing appropriate treatment for casualties
    - before and after the blast for the detection of forensic details for preventing or solving a crime
    - after the blast for the verification of the use of prohibited materials as evidence for law enforcement and other related parties, such as international peacekeeping organizations

These expectations are based on a variety of technological options regarding different types of hyperspectral imaging devices and their many-sided modifications, analysis software and other relating software as well as on different operating platforms, which all together comprise the technological performance of an individual hyperspectral device in a certain situation of use. In addition, environmental conditions, for their own part, determine how precisely the detection can be done in practice.

Many of the CBRNE detection tasks can in principle be performed with COTS types of hyperspectral devices manufactured by different commercial technology providers. However, if the devices are not specifically prepared for tolerating extreme conditions and exposure to toxic materials, their usage may be limited. In addition, full turnkey solutions are not as of yet available as an off-the-shelf delivery for all possible options required in CBRNE countermeasures and defense. Further research, testing and development work is therefore needed to identify and validate feasible solutions for CBRNE detection and for developing them into commercial products.

2.7 Feasible technologies in the information management of CBRNE incidents

The information management, communication and warning procedures of CBRNE incidents are carried out in practice with several different technologies, media and networks. Appropriate communication equipment is selected in each situation according to the parties involved and the urgency and confidentiality of the information content to be exchanged. Also, secondary and backup media may be needed if the primary form of communication media is for some reason corrupted. The selection of an appropriate form of media may also be dependent on the point in the timeline of the CBRNE crisis in which communication is needed. For example, when the threat is discovered for the first time, more urgent and direct communication is needed compared with the recovery stage, when there is no acute emergency and when consultative information can be provided with alternative means without immediate time pressures.

At the time of immediate emergency, the primary operative communication between authorities is usually carried out through closed and secured authority networks. Closed communication may also be enhanced to be directed to other related professionals, such as hospitals. Worldwide, many of these systems are built on Tetra networks (ETSI, 2016). In Finland, the network was introduced under the name Virve for nationwide use in 2002 as the world's first nationwide TETRA technology-based radio telephone network (Virveverkko, 2016). Nowadays, Tetra networks (ETSI, 2016) also offer wideband high speed data communication services in addition to encrypted voice calls.

Outside operative and other forms of closed communication between authorities, it is often necessary in emergencies to also communicate with more open audiences, such as with the civilian population. This raises the question of with which end-user devices, systems and networks that can or should be done. For security reasons, access to authority systems cannot be given to civilians, and if authorities have their own specialized devices in use, they cannot be given to civilians, either. For development, procurement and compatibility reasons and costs, authorities also have in recent years favored using devices that are commercially available on the open market. These COTS necessities are defined (DAU, 2016) as "commercial items that require no unique government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency."

COTS devices and communication methods should, in principle, also be appropriate in emergency communication with civilians, although there is criticism about the use of COTS devices among security authorities. For example, the quality, continuity and reliability of COTS items may not always be satisfactory (Strickler, 2001), or the commercial product models may change so fast that the authorities' equipment cannot be updated with the same speed and budget (Keller, 2013). In emergency communication, however, the usage of COTS technologies may be more cost-effective as the handsets are relatively low-priced

consumer electronics. Also, even if the handset models change yearly, as with the 2G, 3G, 4G, 5G and LTE technologies there already are several different generation mobile networks in use at the same time, different phone models can usually be accessed with more than one generation of mobile networks. The information security of the usage of COTS communication technologies in the security sector can also be improved with encryption methods and, due to encryption (Dhillon and Kelly, 2013), the Internet Protocol is expected to become the dominant network protocol used, for example, throughout military communication networks.

2.7.1 Broadcasting and other traditional emergency communication methods

Referring to individual information management and alerting tasks in CBRNE countermeasures and defence, public warnings have traditionally been given to civilians through national and commercial radio and television broadcasting. In recent years, authorities have also started to give public warnings on mobile phones. Along with the development of the information technology and communication media, other technologies have also been brought into use for various types of crisis communication. According to the guidelines of NATO civilian emergency planning (NATO, 2008), in emergency communication with civilians, the following communication technologies are advised for use:

1. Voice calls and instant messaging:
   - Direct telephone lines
   - Dedicated telephone numbers/lines
   - Interoperable communications equipment (e.g., handheld radios)
   - SMS messages

2. Data communication:
   - Information technology
   - Website

3. Mass media:
   - Use of media (television, radio)

Of these CBRNE emergency communication types, voice calls and handheld radio connections offer one-to-one or limited, many-to-many types of communication. These are used basically for authorities' internal communication and for related discussion with authorized civilian organizations, such as hospitals. In emergencies, voice calls can also be utilized between authorities and civilian people, but to manage chaos, calls need to be organized. As a permanent procedure, most countries have established public emergency numbers, such as 112 and 911, which can be used for reporting an emergency and for calling for help. In severe emergencies, temporary dedicated telephone numbers and lines may also be opened, for example, for the casualty bureau's use. In principal, dedicated phone numbers enable one-to-many and many-to-one

communication in a crisis but not with many people at the same time. However, the people involved can reach the authority, and the authority can give relevant information to the people involved through those lines.

Along with voice calls and handheld radios, mass media, such as radio and television, have traditionally been used for emergency communication. For decades they have been the most efficient and most widely used electronic method for warning people, and it is likely that they will remain in use for a long time into the future. Although all media companies use the Internet, the major communication type in traditional radio and television communication is broadcasting, which enables fast and efficient one-to-many communication. In a public warning situation, this is an essential requirement, but the broadcasting technique also has disadvantages that reduce its usability for emergency communication. For example, as public broadcasting networks were originally built to be as efficient and far-reaching as possible, individual broadcasting stations serve relatively large areas at one time. In emergencies, this means that local warnings cannot be given to only the local emergency areas. Instead, people in safe areas outside the hazard zone unnecessarily receive the same warnings, which in turn may have some negative effects. Another disadvantage of broadcasting in emergency situations is that it enables only one-way communication. An appropriate emergency technology should also enable communication in the other direction, especially for assessing information from the emergency area for the rescue operation management's use.

2.7.2 Instant messaging and SMS

In addition to voice calls and radio and television broadcasting, there are in the abovementioned instructions of the NATO civilian emergency planning (NATO, 2008) communication types also examples of using data-based communication and instant messaging for emergency communication. Data-based communication is used in principle in all information technology-based information storage and transfer activities utilized during an emergency. All may not be exchanged directly between individuals, as emergency data may also be assessed with various sensors and other technological devices as well as be processed, analyzed and transmitted through various computer systems and software to the people who are in charge of utilizing it.

In the example of the NATO civilian emergency planning instructions (NATO, 2008), particularly websites provide an example of data-based communication, whereas SMS represents instant messaging. In CBRNE and other emergencies, websites are used, for example, for delivering emergency information to the people in risk areas, which is a form of one to many communication like radio and television broadcasting. There are, however, significant technical differences between broadcasting and websites that dictate the usability of the two technologies for authority-based emergency communication. In broadcasting, the initiative for emergency communication comes from the authority, and emergency messages are sent to the public unilaterally, regardless of whether people ask for it. It is, however, possible that people will not receive

the messages, because they are not following the media the authority is using. In radio and television broadcasting, real-time messages are also not stored, and they can therefore not be received afterwards at the time of accessing that particular media. However, when the authority gives the same information on a website, emergency messages can be retrieved later. Despite this, websites have a significant weakness in emergency communication, and particularly in public warning situations, compared with broadcasting, as people will not get the warnings and other information unless they somehow know that they should access that particular website.

Technically, in accessing webpages, the client "pulls" the communication, whereas broadcasting is a server "push" type of communication. In the former, information is accessed from the website only when the client desires it, whereas in the latter, information is delivered to the client without the client actively retrieving it. Due to this technical feature, websites are not useful for fast and efficient public warnings, but they can be used for the efficient and economical delivering of other kinds of emergency information that do not have similar time pressures as the high-priority warnings. Based on technical features, websites can also be built to be interactive, in which case they enable two-way communication. For example, people may ask questions and ask for advice from authorities on these sites or submit images and other information to the authority and other users from the emergency area. A typical problem in interactive authority-based emergency websites and other applications is, however, that when something happens, the data traffic on such applications exceeds feasible volumes, and authorities are not able to process and respond to all messages in real-time.

In NATO's guidelines for civil emergency planning (NATO, 2008), SMS messages present an example of instant messaging. Instant messages are typically short, and they are meant to be delivered to the recipients immediately. Compared with voice calls and interoperable handheld radios, the SMS type of instant messages similarly provide one-to-one, one-to-many or many-to-many types of communication. Instead of voice messaging, however, they contain only textual data. In comparing SMS with radio and television broadcasting, both can basically, in ideal conditions, be used for one-to-many communication with wide audiences. However, the technologies and data transmission methods are different, and, as SMS messages are transmitted through the same channel as mobile phone voice calls, the delivery of SMS messages to large numbers of recipients can be seriously weakened and delayed due to an overload of traffic on mobile phone networks. In addition, whereas the service area of mobile phone-based stations is crucially smaller than that in radio and television broadcasting, the dense and diverse structure of mobile phone networks and cells can complicate the transmission path and cause delays in the delivery of SMS messages. Furthermore, SMS messages are sent by individual phone numbers, which causes extra work by generating a tailored delivery list each time a mass delivery of SMS messages is needed. With anonymous broadcasting to all radio and/or television receivers in the service area, these kinds of recipient lists are not needed.

Particularly in mountainous landscapes and in built-up areas, the geography and buildings cause reception blackspots, in which mobile phone communication is inhibited. Blackspots caused by physical obstructions in terrain and buildings are usually corrected (Telco, 2016) with additional transmitting antennas, which, however, may lead to a weakening of the signal in the same location or another place due to an overlap and interference of crossing transmissions. Another substantial difference between broadcasting and SMS communication is that radio and television broadcasting are traditionally received via radio and television receivers, which are non-personal mass communication media. SMS messages, on the other hand, are received primarily via mobile phone handsets, which are personal communication media. For the user, there is often a significant difference between mass communication and personal communication, and, even though radio and television broadcasting can nowadays be received through personal communication media such as smartphones, this does not directly transform radio and television broadcasting into personal communication.

2.7.3 Cell broadcast

Mobile technologies also have two other techniques, cell broadcast and mobile push notification, which can be used for instant messaging and which also address the shortages of SMS. In cell broadcasting (Cellbroadcastforum, 2009), messages are transmitted on selected mobile phone cells and to the service area around each cell and are received via a personal mobile phone. In that these messages are carried out using a broadcasting method, cell broadcasting can be viewed as similar to radio and television broadcasting and to the mass delivery of SMS messages. Due to the broadcasting technique, however, messages are delivered at a higher speed than with SMS. Improvement in the delivery speed is also created through the feature of anonymously sending the messages to all active mobile phone handsets in the service area without the need to first create delivery lists for relevant phone numbers. In addition, when phone numbers are not needed to send messages to individual handsets, and when messages are sent on the basis of mobile network cells, the dense network of cells creates flexibility in messaging, although in SMS messaging this can also create a roadblock. In a dense cell network structure, the mass delivery of messages can also be directed to more focused areas, which is an advantage, for example, in local emergencies. In ordinary radio and television broadcasting, the range of a service area is on average 100 km from the broadcasting tower, and in mobile phone cell networks, depending on blackspots and the generation of the mobile phone networks, the range is on average 5–10 km from the cell tower. Based on this type of network structure, local emergency communication sent through mobile phone network cells will be received quite precisely where it is needed, and only to a small extent in areas where it is not relevant. However, when the same information is transmitted through local radio and television broadcasting stations, a large number of people will receive the emergency notifications unnecessarily. And the disturbance may be even worse if the emergency continues,

and notifications are sent several times per day and maybe even over more than one day. Moreover, with national radio and television broadcasting networks, the disturbance of unnecessary emergency alerts for the population is even greater, which over the long run may cause a decline in people's safety.

In general, cell broadcasts to anonymous receivers represents the one-to-many type of communication, which at the same time creates its weak points. This one-way type of transmission technology is not capable of sending back feedback information, which, however, is crucial in emergencies for the assessment of the risk area. The broadcasting type of cell-based transmission is also not flexible for messaging inside areas smaller than the service area around one cell tower. Transmission to the whole service area of a cell tower at one time may not be a problem in scarcely populated areas, but in densely populated areas, more focused alerting may be needed, particularly for emergency warning and rescue purposes.

2.7.4 Push notifications

The third type of instant messaging on personal mobile communication devices is mobile push notifications. Similar to the SMS and cell broadcasting method, and, unlike social media, it is a technological feature in mobile communication and not a mobile client application, although it is usable together with a client application on the phone. Mobile push notifications (Steele, 2014) are a form of server push notifications where information is delivered from the server to the end-user device without being retrieved actively by the user. They can be used on most mobile technology platforms (Urban Airship, 2016), such as Android and iOS. This method is used widely in marketing and news services (Digital Marketing Glossary, 2013), where it is considered to be an intrusive technique and thus needs to be managed carefully to prevent notification fatigue of the user.

Compared with SMS and cell broadcast messages, which are delivered through voice communication and broadcasting channels, push notifications are delivered on mobile devices as data transmissions. This means that on mobile phones push notifications are not, unlike SMS messages, delivered via the same channel mixed with speech-formed voice calls. This kind of data transfer gives multiple advantages (Kuula et al., 2013) compared with other technologies, such as the possibility of delivering information in much richer presentation formats. While the two other instant methods, SMS and cell broadcasts, enable the delivery of only short textual messages, push notifications can also be used for delivering images and stored voice messages. In addition, push notifications can be programmed to give commands to the end-user device for performing a variety of different technical operations. For example, the device can be commanded to play the wanted ring tone at the desired volume even if the phone is muted. In addition, the device can be advised to vibrate while delivering the message or to deliver a silent message.

Push notifications can also be used interactively on mobile phones, as recipients may be given the option to reply to the messages received. However,

technically, push notifications do not automatically suggest to the user the option to reply. Instead, the interactive functions are built into the phone as a combination of the commands that are sent from the server with the push notification and the knowledge that is preprogrammed into the client application. If the interactive feature is not programmed in the client application, push notification is merely a one-way message.

The interactive feature is another significant difference between push notifications and the two other instant messaging methods, because it also enables many-to-one communications. With cell broadcasts and the mass delivery of SMS messages, basically only one-to-many communication is possible. In principle, the SMS functionality on mobile phones also enables two-way communication, but due to practical and economic reasons, mass deliveries are often sent with SMS messages as one-way group messages without the option to reply to the message.

As with SMS messaging, each message costs, but the reply to the message is often made free for the recipient in cases where the reply-option is being used. In this case, the sender usually pays for both the sent and the received messages. In push notification-based messaging, both the sent and received messages are transferred through the data connection of the wireless device, in which case individual messages do not cause any extra fee in addition to the basic charge for the sender or receiver. The basic charge covers the data connection, which both parties pay for in any case to be able to communicate with their devices. However, costs may vary depending on the country and the user's subscription with the telecommunication service operator or on the service for which the interactive push notification application is used.

The many-to-one communication made possible by the interactive feature of mobile push notifications enables immediate feedback and information collection from large numbers of people to the service provider. This can be done anonymously or by identified users, as push notifications can be sent to the end devices either on the basis of their geographical location or on telephone numbers. When notifications are sent to the devices on the basis of their location, the reception area can be chosen very flexibly. Whereas SMS and cell broadcast messages are delivered with a fixed and limited range around the broadcasting or cell tower, with mobile push notifications the center point and range of deliveries can be chosen freely. In principle, any location in the world that can be defined with longitudinal and latitudinal measures can be chosen as the center point for push notification deliveries. Starting from that point, the range of the actual delivery area can be defined as any measurable distance on the globe, depending on the need. With this technology the targeting and delivery of messages is therefore not dependent on transmission towers or cells as long as the receiving devices have access to data transfer connections. Network connections can be created by mobile phone networks, wireless local area networks or other specific lines. Depending on the subject, reasonable delivery areas for localized communication are, for example, individual blocks, other parts of or the entire city, other parts of the country or any other international area.

2.7.5 Comparison of the usability of instant communication methods

When the capabilities of the three instant messaging methods, SMS, cell broadcast and mobile push notifications, are compared, they all may look relatively similar at first glance, as they all operate on COTS-type commercial mobile phones and can be used for one-to-many communication for broad audiences. However, cell broadcast falls behind the other two in regard to infrastructure requirements, as it requires additional investments in the national telecommunication infrastructure, unless the particular infrastructure has already been built in the country. For example, in Finland, cell broadcasting has been tested, but the infrastructure has not been built, in addition to the fact that the test network was pulled down several years ago. SMS and mobile push notification types of messaging operate in all common mobile phone networks and thus are usable without additional investments in areas where public or commercial mobile networks exist. However, push notifications operate mainly on 3G and newer generation handsets, but if 2G phones are still in use, automatic complementary SMS-based transmission can be used to improve the accessibility of older generation types of phones (Kuula et al., 2013).

In addition to infrastructure, the transmission technique also creates significant differences between the three methods. Firstly, the broadcasting type of transmission creates a barrier for the interactivity of the cell broadcast messaging, and secondly, the cell-based transmission amongst mobile phone voice calls deteriorates the delivery times of grouped SMS messages. For the same reason, high-volume SMS deliveries need to be created as one-way messages only and thus cannot be interactive. Also, with SMS messaging in voice call lines, richer representation forms such as voice and image cannot be delivered. Instead, the data transfer type of transmission of the mobile push notification-based messaging enables interactivity and the delivery of voice and images. The same transmission technique also makes it possible to deliver messages in extremely wide and flexible areas, independently from the location of broadcasting or cell towers. The same features also enable incident-based many-to-one communication, which is a valuable quality in emergency communication in addition to the more common one-to-many communication.

There is also a difference in the way the various types of instant messaging utilize the positioning feature of mobile devices. Even if the mobile phone can be localized, this does not directly mean that the different instant messaging formats are able to utilize that feature. There are also different methods, such as the terrestrial cell tower-based tracking, termed cell phone triangulation (Smith, 2008), and the satellite-based Global Positioning System (GPS) (GPS, 2016) for localizing the phone, which give different options for utilizing the user's position in mobile services. The cell broadcast and SMS messaging methods utilize the limited geographic area around the cell tower to locate the particular users, but in their basic forms they are not built for utilizing the precise position of the defined mobile phones in the service area. Instead, location-based mobile push messaging services (Kuula et al., 2013 deliver messages on the basis of the pre-

cise location of the handsets, and the most precise location can be defined with GPS. In principle, other positioning methods can also be utilized together with the push notification method, depending on the application and environment in which the service is being used. In hybrid positioning (Spirent, 2012), different locating methods, sensors and networks can also be combined, which improves accuracy, especially inside built environments. For the service provider, the utilization of the positioning feature provides multiple advantages. For example, in emergencies, victims and rescuers can be located and tracked using this feature in the messaging system, and also the location-based feedback information about the conditions in a certain spot can be assessed with this method.

In conclusion, of the COTS-type of instant messaging methods, the data transfer-based mobile push notification type of messaging appears to have the highest potential for fast, interactive, rich and geographically flexible communication. Due to their various technical capabilities, affordability, availability and possibility for encryption, mobile push notification-based applications can be expected to be usable in a myriad of emergency management and warning solutions, including in the information management and communication procedures of comprehensive CBRNE countermeasures and defence. In this user environment and context, the usability of mobile push notifications is not limited only to direct instant messages, which are sent from the server as forced commands and quick information to mobile devices. Instead, the multiple other functions that mobile devices are able to carry out after being commanded with push notifications are also essential for performing the required CBRNE countermeasures tasks. Technically, the performance of the mobile phone handset is created in this kind of situation together with the notification from the server and the client application and technical features of the handset, which can vary depending on the model and manufacturer of the device. It is possible to create many of different client applications for different purposes, and the same application can be used for different purposes as well, as long as the information content is changed according to the mission and users.

To be able to utilize the mobile push notification method in emergency management and defence applications, the end-user devices do not necessarily need to literally be mobile phones. Other smart devices can be commanded and directed from a distance via the same method through wireless communication networks as well, as long as the end device is operable and programmable in the same way as ordinary smartphones. The same method can also be applied even if there is no person at the end-user's location. This kind of user scenario is possible and likely in CBRNE defence, where it is necessary to carry out detection and rescue operations in the hazard zone even if it is not safe for humans. In these situations, unmanned devices, such as drones and robots, can be sent to carry out various CBRNE defence tasks, and the devices can be programmed and commanded to perform the desired tasks by utilizing the mobile push notification method.

2.7.6 Conclusions on the mobile methods in the information management of CBRNE incidents

In regard to the involved counterparts described in the comprehensive CBRNE countermeasures model in Figure 7, the threat/hazard, operation management, operative forces, joint forces, hospitals, public/casualties/protected targets etc., it is possible that useful applications can be built with the smartphone technology and mobile push notification method related to all these angles of managing CBRNE emergencies. For example, concerning the CBRNE source, the accurate geographical positioning and interactive elements of push notification applications enable a precisely focused threat and risk assessment of CBRNE as well as the estimation of casualties and material losses. Forced push notifications also offer a potential method for command and control and for giving warnings and updates to the operative forces. The same features also work well for giving warnings and updates, advice and other crisis management services to private citizens through their personal mobile phones. The interactive feature may also be useful in the impact assessment, directed to operative staff, inhabitants or some other selected groups in the area. The geographical positioning, forced push notifications and interactive features together also offer a convenient method for operation management to provide situational awareness through the staff, civilians and/or other contact persons or possibly through automated devices in the area. As inquiries can be sent to crowds spontaneously and quickly, and as feedback information can be collected promptly, the situation picture can also be updated relatively rapidly. For the reinforcement, joint forces, other related authorities, hospitals and external specialists, the direct push notification feature is useful for giving alerts and other updated information during the course of the incident. With these stakeholders, the interactive feature of push notifications is also valuable for obtaining quick responses regarding the availability, type and timing of additional materials and other help in the operation. The various properties of the mobile push notification method can also be applied by the establishment of the casualty office. For example, all people in the hazard zone can be given information about the existence and operation of the office. Later on, when those individuals' names are known, more focused messaging groups may also be created to direct further messages specifically to those people who need the services of the casualty office.

2.8 Summary of the research framework

This chapter introduced the research framework for information technology-based countermeasures for CBRNE threats. First the main types of CBRNE threats were introduced, followed by generic preparedness models and military and civilian operating concepts of CBRNE countermeasures and defence. The operative procedures were then divided into two groups, of which some can be

fulfilled through physical means and others with measures that utilize information technology. Information technology was viewed in this context broadly, also including electro-optical measures. After this, further discussion was focused separately on the military and civilian capability requirements of the detection, identification and monitoring of CBRNE threats (DIM) and of the information management and alerting type of countermeasures (IM). Different technologies were also presented for CBRNE detection and for the information management of CBRNE incidents. After evaluation and comparison, hyperspectral technology was found to have the highest potential to be able to fulfill the capability requirements for CBRNE detection, identification and monitoring. Similarly, smartphone technology, particularly the push notification type of instant messaging, was found to have the greatest potential to fulfill the capability requirements for the information management and alerting type of CBRNE countermeasures and defence.

3 EXPERIMENTS AND RESULTS

In the following, the experiments using hyperspectral and smartphone technology in CBRNE countermeasures and defence are introduced in section 3.1. For parts of the experiments, some of the previously published research articles are also included. In section 3.2, as a part of the research framework discussed in sections 2.2–2.5, the capability requirements of CBRNE countermeasures and defence are compared with the experimentation results, and the results of the entire study are produced on the basis of this comparison.

3.1 Experiments

Here, subsections 3.1.1–3.1.10 present the empirical experiments that have been carried out with hyperspectral and smartphone technology during the practical research and development projects on hyperspectral crime scene investigation and smartphone-based crisis management and warning from 2012 to 2014. In this study these experiments are used for evaluating the usability of hyperspectral and smartphone technology in CBRNE countermeasures and defence. The usability of hyperspectral technology is evaluated by its capability of detecting CBRNE substances in indoor and outdoor field conditions and at the different stages of the timeline of a CBRNE incident. Accordingly, the usability of smartphone technology is evaluated by its capability of being used to give mass alerts, warnings, command and control messages and other emergency notifications by the system and by its capability to create situational awareness following the course of operation, being integrated with other emergency management systems as well as monitoring the post-incident health situation after the crisis.

3.1.1 Hyperspectral detection and identification of explosives and explosives' residues

In October 2013, a series of explosion tests were organized in the *SpeCSI Solutions* project for simulating a terrorist attack with explosives in a shopping mall

and for testing the hyperspectral detection of explosives and explosives' residues in that environment. These tests provide an example of surveying to determine the particulate CBRNE hazard and providing spectral data with hyperspectral technology.

To carry out the experiments, four identically staged research designs were prepared outdoors, where concrete, plastic carpet, laminate and cotton fabric represented typical construction and furnishing materials for an average shopping mall. Outdoor tests were chosen, because there was no available, appropriate place for carrying out explosion tests indoors. Research materials were placed on four identical testing sites, as represented in Figure 8. A simulated improvised bomb prepared with an explosive charge, igniting wire, plastic bucket, cardboard box and plastic tape was placed in the middle of each design. The first design was built up with powder, the second with TNT, the third with dynamite and the fourth with PENO.

The tests were scheduled during dry weather before winter, but as the first snow fell right on the night before carrying out the tests, the weather changed conditions from that which was planned. The weather, however, did not change other parts of the tests. The four controlled explosions were conducted by the representative of defence forces sequentially one after another, and evidence was collected and stored by the forensic investigator of the police immediately after each explosion. The tests were carried out to determine whether explosives can be detected and identified with hyperspectral technology in a pure form in a pre-blast situation before the explosion and as explosives' residue in a post-blast situation after the explosion. In an authentic situation, detection should be carried out directly from the target at the CBRNE site, but as the tests were the first hyperspectral detection tests with explosives in the project, remains of the explosions were taken to the laboratory to be examined in a more controlled environment with three different hyperspectral cameras.

Expectations for the experiment were that, if the spectra of pure explosives were assessed with any of the tested hyperspectral cameras, and if explosives' residues were also found at least for one of the tested explosives, that would confirm the hyperspectral technology's capability to determine the particulate CBRNE hazard and to provide spectral data from it. From the practical research and development project perspective, such result would also give grounds for carrying on with the hyperspectral tests and the development of an affordable, small hyperspectral detection device, which was the technical target of that development project. The small detection device was supposed to be applicable for a forensic investigation at any kind of crime scene, including CBRNE sites (if made tolerant for contamination). Concerning the detection of explosives, the technology should have been able to detect homemade bombs, explosives and other types of improvised explosive devices both in built-up urban environments and in various field environments. It should also be capable of revealing traces, which would help in catching persons involved in terrorist attacks.

To find out which types of devices are capable of detecting the tested explosives and residues in the experiment, all samples were imaged and analyzed

with three different hyperspectral cameras in VNIR, SWIR and MWIR wavelengths. As a result, pure substances of all of the tested explosives of powder, TNT, dynamite and PENO were detected with all except for the VNIR camera, which was not able to detect PENO. Explosives' residues were more difficult to detect, as was expected in advance. Successful findings were derived primarily from TNT residues, which were produced in a deflagration type of explosion. Residues of powder, dynamite and PENO were created in detonation types of explosions and were thus more difficult to find.

TNT residues were detected best on the cotton fabric, which was the softest material in the research design. It was also located highest from the ground compared with the other materials on which residues were collected. As there was snow on the ground at the time the tests were carried out, especially thin and stiff materials were mixed with snow during the explosion. After collecting the samples in plastic bags, the snow melted and flushed the samples, and it is therefore likely that some of the residues disappeared before they were measured with the hyperspectral cameras. The residual findings on the cotton, however, were positive with all of the VNIR, SWIR and MWIR cameras, which supports the proposition that hyperspectral technology can be used for determining the particulate CBRNE hazard and for providing spectral data for the pre- and post-blast detection of explosives. The experiment is reported in included article PI:

Jaana Kuula, Heikki Rinta, Ilkka Pölönen, Hannu-Heikki Puupponen, Marko Haukkamäki and Tuomas Teräväinen. Detecting Explosive Substances by the IR Spectrography. *Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XV, edited by Augustus W. Fountain III, Proc. of SPIE Vol. 9073, 90730Q · © 2014 SPIE CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050157*, 2014.

During the *SpeCSI Solutions* project, other additional experiments with explosives were also conducted as laboratory tests with the assistance and supervision of the explosives manufacturer Forcit Ltd. and the Central Finland Police Department in July 2014. In these tests, nearly 100 individual samples were prepared with different explosives and mixtures on clear glass and several other materials. In the tests, secondary traces were also prepared on various surfaces with fingerprints after having touched the explosive materials. Samples were imaged with two hyperspectral cameras with VNIR and NIR wavelengths. The purpose of these tests was to obtain more knowledge on the detection and identification of a large variety of explosives and explosive mixtures as pure substances on various surfaces and setups to serve forensic and industrial purposes. The results are not included in this thesis.

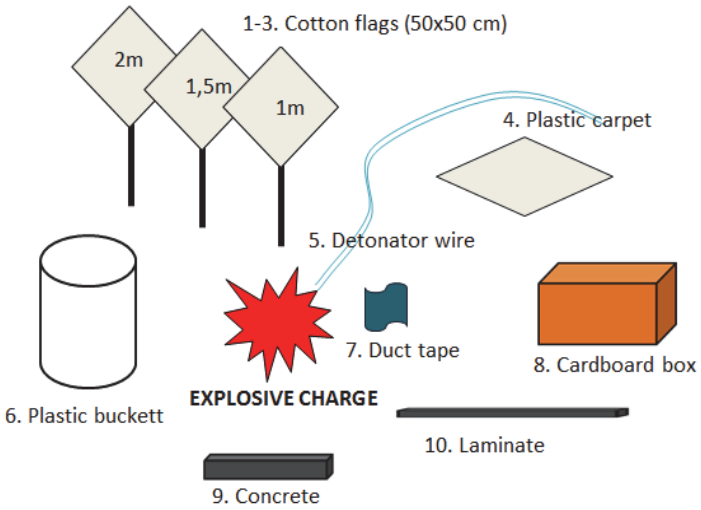


FIGURE 8 Research design for producing explosives' residue for detection tests

3.1.2 Hyperspectral detection and identification of CWAs and simulants

In May 2014 in the *SpeCSI Solutions* project, hyperspectral detection and identification tests were performed with CWAs. The tests were conducted in the laboratory of Verifin, which works closely with OPCW and applies their working methods in this field. Tests were performed with around 10 samples of pure chemical agents and their simulants, precursors and degradation products. Samples were measured with distinct safety measures in a fume cupboard as pure substances in a glass bowl, and some samples were on fabric on a piece of cotton. The chemicals tested included mainly organophosphorus and vesicant agents.

All samples were measured with three different hyperspectral cameras of the types SWIR, MWIR and LWIR. The purpose of the experiment was to test whether the spectra of the selected chemicals can be assessed with the hyperspectral cameras and whether the chemicals can be detected on fabric. The detection results varied depending on the chemical agent and camera. Strongly vaporizing chemicals could not be detected in a liquid form. The results are not included in this thesis except those for chloropicrin and capsaicin, whose hyperspectral detection results are published in the article Drone Based Hyperspectral Detection of CBRNE Threats, presented in the next section.

3.1.3 Airborne hyperspectral detection of explosives and biological spots

In July 2014, outdoor field tests were conducted in the *SpeCSI Solutions* project for the direct airborne hyperspectral detection of explosives and biological spots on the ground. The tests provide an example of the reconnaissance, surveying and verifying of the CBRNE hazard prediction area with hyperspectral technol-

ogy, and they were carried out with the assistance and supervision of the Central Finland Police Department and Forcit Ltd.

At the beginning of the tests, identical samples of 11 explosives were prepared on the ground on sand, asphalt and grass. Blood samples were also produced in the same way and are discussed in another section. The research design for the airborne detection test is shown in Figure 9. After preparing the samples, the explosives were imaged from the air with a small Fabry-Perot type of VNIR hyperspectral camera. The wavelength area of the camera is 500–900 nm and its weight is approximately 500 g. During the tests, the camera was mounted in a lightweight unmanned drone, which flew at the height of treetops and lower.

The experiment had two purposes. On one hand, it was organized to test in practice the operation of short distance detection with a small lightweight hyperspectral camera and drone without entering the site by ground or touching anything on the site. On the other hand, the experiment was expected to give additional information about the imaging performance of the small camera in the short distance airborne detection of a simulated crime scene and CBRNE site. It was known beforehand from earlier information and tests that the camera was able to detect blood in the laboratory environment but that its capability of detecting explosives was not very likely. However, tests were performed with this particular camera, because empirical information was needed about the behavior of small hyperspectral cameras and drones in the short range detection of a crime scene and CBRNE site, and because other camera types were not available in such a small size.

The experiment clearly demonstrates how dependent unmanned airborne operations and hyperspectral imaging are on environmental conditions. Environmental circumstances have a direct effect on the success of imaging and also on the operation of the airborne platform, which in turn also has an effect on the operation of the hyperspectral camera. To meet with success, outdoor hyperspectral imaging with an unmanned airborne platform requires clear daylight and dry, still weather. In this case, weather forecasts were followed carefully for several days before and during the day of the experiment to perform the tests in a good weather. However, in the middle of the tests the weather suddenly changed, and a thunderstorm, wind, rain and clouds disturbed the tests. There was just enough time to image all samples quickly but not to experiment with additional flying routes and alternative imaging positions. As a result, the tests gave experience of using different parameters in close-range airborne hyperspectral detection with a drone, and of the behavior of researched chemical and biological samples that were applied on three different types of soil. It is thus clear that lightweight devices are in this kind of use more dependent on environmental conditions than hyperspectral imaging in principal. It is also evident that even if samples can be detected with a hyperspectral camera in small volumes in the laboratory, it is not granted or very likely that they can also be detected in field conditions outdoors with the same volumes and with the same hyperspectral devices due to the imaging conditions and the behavior of sam-

ples on different types of ground. The experiment of airborne hyperspectral detection of explosives is described in included article PII:

Jaana Kuula. Drone Based Hyperspectral Detection of CBRNE Threats. *Jussi Paatero & Nils Meinander (Eds.). Proceedings of the NBC-2015 Symposium – How does the landscape evolve? - Helsinki, Finland, May, 2015. ISBN 978-952-93-5586-0*, 2015.

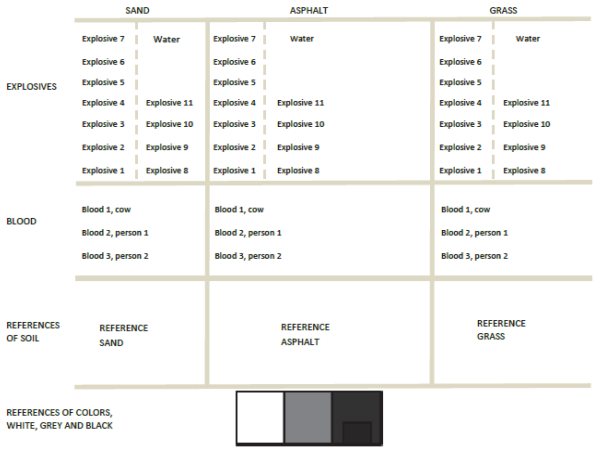


FIGURE 9 Research design of airborne hyperspectral detection tests

3.1.4 Hyperspectral detection of blood, other biofluids and biological markers

When an emergency site is entered for the first time, the CBRNE incident has to be identified by various indicators and signs. In explosions these are, for example, structural damage and the wounds and broken bodies of casualties. In other types of CBRNE incidents, the numbers of casualties are possibly higher and the casualties may have typical agent-specific external signs. Depending on the affecting toxin, they may be found on exposed people's skin, eyes, vomit, breath, saliva, urine, blood or other biological spots. Experienced medical personnel can usually notice typical signs, and diagnosis can be confirmed with clinical methods.

In this study, direct research on the biological markers of exposure to CBRNE substances was not undertaken. However, in the study several hyperspectral laboratory tests were performed with various biological samples, which entails the preliminary basic research in the recognition of signs and indicators of CBRNE incidents on humans and their remains. At the same time, such tests represent crime scene investigation and forensics, which are also part of the detection and investigation of CBRNE sites.

The first hyperspectral tests on biological samples were conducted with blood in the *SpeCSI* project in spring 2012. The experiments were performed with human and animal blood, and special interest was paid to distinguishing the different blood traces found at a crime scene. In the first of this kind of experiment, a sample of three persons' and one animal's blood was prepared on denim fabric to find out whether the different donors' blood could be distinguished with a hyperspectral camera. The sample contained a drop each of two males', one female's and a cow's blood, and it was imaged with a 500–900 nm Fabry Perot and 400–1000 nm push broom types of VNIR hyperspectral cameras and with a 1000–2500 nm SWIR camera. The tests began as blinded tests, where the constitution and origin of the samples on the fabric were not told to the researchers who analyzed the samples. Instead, their task was to find out with hyperspectral imaging, software analysis and mathematical algorithm development how many different substances there were on the fabric and what the substances were. The researchers also had to determine the best hyperspectral camera for the analysis of the particular kind of samples in the test.

As a result of the first experiment, the blood samples were not distinguished from each other using the VNIR cameras, but according to the imaging results of the SWIR camera, the four samples identified as different. A photograph and a hyperspectral image of the sample produced by the SWIR camera are presented in Figure 10. As the figure shows, all four blood stains look different in the SWIR image, which means, on the condition that other factors are eliminated, that the samples are of different origin. This experiment does not reveal the reason why or due to which factors the four blood stains are by the hyperspectral analysis shown to be different, and the reasons for that can be many. If the analysis result is correct, the hyperspectral camera has been able to detect the microscopic structural differences in the constitution of the four blood samples. However, there is also a chance that the four blood samples had absorbed into the fabric in a different way, which then produced different imaging results. Different absorption may have been caused by the different constitution of the blood samples or by structural differences in the background material. In this case the way the denim fabric had been woven and colored may have affected the imaging result.

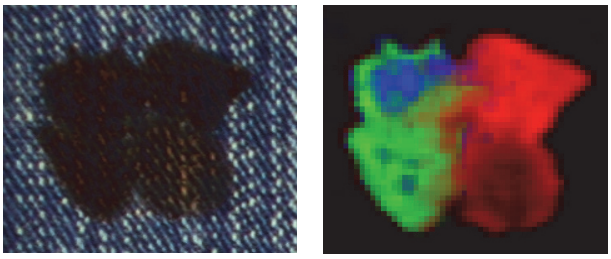


FIGURE 10 A photograph and a SWIR type of hyperspectral image of four blood stains

To verify the test result, a new experiment with blood was designed in the *SpeCSI Solutions* project in October 2013. In this experiment, special interest was

paid to finding the critical structural factor in the internal constitution of blood, which enables the discrimination of different donors' blood with a hyperspectral camera. A new sample was carefully prepared with four persons' blood on a natural cotton fabric, which was expected to eliminate the possible effect of the background material on the imaging results. This time the sample contained only human blood from two males and two female donors. The donation process was standardized by obtaining tested blood from all donors within an hour in a private medical laboratory and by storing it in identical tubes that were treated similarly until the samples were prepared for the imaging by the hyperspectral camera. The samples were prepared on the fabric with standard methods by measuring with an automated pipette exactly the same volume of blood in each stain. In addition, a blood count was taken from each donor's blood as a control and comparative measure for the constitution and structure of the tested blood.

After the samples were dried, they were imaged with a SWIR type of hyperspectral camera and, as a control and verification measure, also with an ATR NIR spectrometer. As is shown in Figure 11, different donors' blood samples were again distinguished with the SWIR type of hyperspectral camera. This result, after diminishing the influence of the background, supports the results of the earlier experiment concerning the hypothesis that the hyperspectral discrimination of blood on cotton is based on the internal factors of the blood.

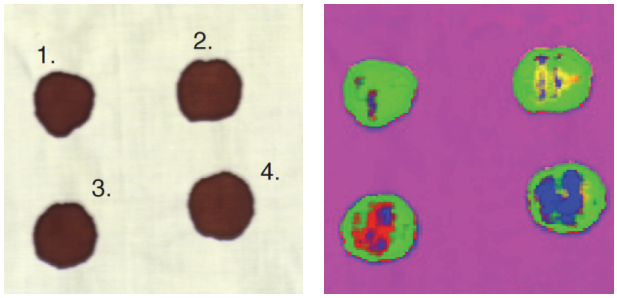


FIGURE 11 Distinguishing different donors' blood samples

To find the discriminating factors for the hyperspectral imaging in the constitution of blood, at this stage of the research a correlation analysis with standard mathematical and statistical methods was conducted between the hyperspectral imaging results and the blood count of the samples. According to the analysis, the number of erythrocytes in blood correlates with the distinguishing results of the hyperspectral camera by proposing that erythrocytes are what allow the discrimination between different persons' blood with a hyperspectral camera. This result, however, was not verified statistically due to the small number of tested materials. It should also be noted for forensic and juridical purposes that, even if erythrocytes are the physical factor enabling the discrimination between different people's blood with the hyperspectral technology, the physical features of blood may not stay the same for the whole life span of a

person. In addition, various changes in blood take place, depending on the conditions in which the blood is being kept after the donation until the analysis.

The hyperspectral tests with blood in this context represent experiments for the recognition of signs and indicators of CBRNE incidents and for the recognition of relevant signs for the forensic investigation, even though blood alone does not necessarily indicate a CBRNE event. These experiments, however, demonstrate how blood and, for the human eye, imperceptible smaller particles in blood can be detected and distinguished with hyperspectral technology. This in turn may also imply that other human-based biological traces and direct signs of CBRNE exposure on humans can possibly be recognized with the same technology. This result is also supported by other experiments performed with additional human-based samples in the same research. In addition to blood, in the *SpeCSI Solutions* project in 2013–2014, small-scale hyperspectral detection tests were also conducted with urine, saliva, sperm, hair, bruises and skin, of which some can possibly indicate CBRNE exposure and intoxication in the body. Except for those with blood, reports of the experiments with other biological samples are not included herein.

The first experiment for the hyperspectral detection and distinguishing of different donors' blood is documented in included article PIII:

Jaana Kuula, Ilkka Pölönen, Hannu-Heikki Puupponen, Tuomas Selander, Tapani Reinikainen and Tapani Kalenius. Using VIS/NIR and IR Spectral Cameras for Detecting and Separating Crime Scene Details. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI, edited by Edward M. Carapezza, Proc. of SPIE Vol. 8359, 83590P © 2012 SPIE · CCC code: 0277-786X/12/$18 · doi: 10.1117/12.918555*, 2012.

The second hyperspectral experiment with blood for examining the constitution of different donors' blood is documented in included article PIV:

Jaana Kuula, Heikki Rinta, Ilkka Pölönen and Hannu-Heikki Puupponen. The Challenges of Analysing Blood Stains with Hyperspectral Imaging. *Sensing Technologies for Global Health, Military Medicine, and Environmental Monitoring IV, edited by Šárka O. Southern, Mark A. Mentzer, Isaac Rodriguez-Chavez, Virginia E. Wotring, Proc. of SPIE Vol. 9112, 91120W · © 2014 SPIE · CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050180*, 2014.

3.1.5 Hyperspectral forensic investigation of a crime scene

In the spring of 2012 in the *SpeCSI* project and in the summer and fall of 2013 and in the summer of 2014 in the *SpeCSI Solutions* project, many other hyperspectral technology experiments were also performed with other kinds of samples representing examples of crime scene details for violence and organized crime. All of these may not be relevant for the immediate rescue and defence operations of a CBRNE incident, but they can have significance for the forensic investigation of CBRNE crimes in the same way as they are relevant for the investigation of other

kinds of crimes. It is also known that terrorism and other types of organized crime disregard the law and international borders and that other forms of criminality are often mixed in the operations of these illicit groups. For example, same criminal groups may conduct armed attacks and carry out illegal trade and business for gaining economic profits. This may include armed robberies; the growing, smuggling and selling of drugs; the selling of stolen artifacts; trafficking, illegal sex services and industry; art forgeries; burglaries; arson and fraud and other kinds of economic crime. Criminality for gaining economic profit may also be used for funding CBRNE terrorism and war and vice versa. In addition, due to international connections and internationally networked criminality, crimes in underdeveloped and Western countries may be linked, and minor crimes in one place may be carried out to support more severe crimes in another place.

In this research, hyperspectral technology tests with crime scene details include, in addition to above discussed blood, biofluids and other human-based marks, tests for the hyperspectral detection and distinguishing of contaminated soil; drugs, such as amphetamine, methamphetamine, cannabis and Subutex; traces of fires and arson; fingerprints; counterfeit documents and signatures; burglaries; art forgeries; traces of gunshots, tear gas, fibers, paint etc. Tests were carried in the laboratory with VNIR, SWIR and MWIR types of hyperspectral cameras and also partially outdoors as airborne hyperspectral monitoring, as presented above in section 3.1.3. Most of the tests for forensic investigation were carried out with the Central Finland Police Department and partially with the National Bureau of Investigation and some other units of the Police of Finland. Experiments with contaminated soil and traces of fires and arson were carried out with the Rescue Department of Central Finland. All tests with the police and fire and rescue service were performed in spring 2012, summer and fall 2013 and in summer 2014. The tests produced successful detection results except for the detection of primer residues, deeply absorbed material in soil and materials that were mixed with many minerals and dirt.

As a reminder when using hyperspectral technology in forensic investigations, one should note that even if the technology is capable of finding forensic marks, the device alone cannot determine the forensic relevance of the found items, unless they are originally illicit, for example, restricted CBRNE materials or drugs. The real knowledge of the relevance of forensic marks is determined by the investigator, who needs to know and decide, case by case, what to look for and what to present as evidence.

Some of the results of these experiments are published in included article PIII:

Jaana Kuula, Ilkka Pölönen, Hannu-Heikki Puupponen, Tuomas Selander, Tapani Reinikainen and Tapani Kalenius. Using VIS/NIR and IR Spectral Cameras for Detecting and Separating Crime Scene Details. *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI, edited by Edward M. Carapezza, Proc. of SPIE Vol. 8359, 83590P © 2012 SPIE · CCC code: 0277-786X/12/$18 · doi: 10.1117/12.918555*, 2012.

Some results are also reported in two other presentations, which are not included herein:

Jaana Kuula, Ilkka Pölönen, Hannu-Heikki Puupponen and Tapani Reinikainen. The Challenge of Using Hyperspectral Imaging in Crime Scene Investigation. *The European Academy of Forensic Science EAFS2012 - Towards Forensic Science 2.0 Conference, The Hague, The Netherlands, conference presentation, 20-24. August*, 2012

Jaana Kuula. The Hyperspectral Investigation of Fires and Explosions. *The 22nd International Symposium on the Forensic Sciences, Adelaide, Australia, conference presentation, 31. August - 4. September*, 2014.

3.1.6 Smartphone-based alerting and command and control of the special forces of the police

In November 2012 in the *Sapporo* project, technical tests were carried out for the alerting, warning, situational awareness and command and control capabilities of smartphones with representatives of the Central Finland Police Department, the Police Board and members of the special forces and crisis communication preparedness group of eight police departments of the Police of Finland around the country. The tests represent an example of the warning and updating, coordination, command and control, reporting, debriefing, counseling and monitoring of operative forces and of the creation of situational awareness for operation management for CBRNE incidents and other crises with smartphones.

In the experiment, the tested operative functions were created together with a tailored crisis communication and crisis management software, with the technical features and operability of mobile networks and with the technical features and operability of smartphone handsets. The core of the tailored crisis communication software was initiated as a part of the wider multi-objective *Scientific innovation product concept, Scope* project in 2009–2011, from which it was developed into to its full form as a mobile crisis management system in the *Sapporo* project in 2011–2013. The created software system consists of server-end and mobile-end functionalities and features that are dependent on the selected mobile data transmission method. Major commands are given with the server-end software and other critical functionalities, such as alerts and warnings with the mobile-end client application. Some of the most essential capabilities for crises management operations were, however, created with the smartphone's mobile data transmission method, which enables the usage of mobile push notifications on mobile handsets.

The technical tests of the smartphone system with the police covered the experimentation with the key functionalities, such as localization, profiling, prioritized alerting and warning, multi-sense alerting, mass communication, two-way communication, command and control, situational awareness and log of operations. With the localization functionality of the system, the geographical locations and areas of alerting zones can be defined freely, and all smartphone users inside the alerting zone will receive the alert on the basis of their precise

geographical position. When necessary, the area for giving alerts and warnings can be defined again each time messages need to be sent. The alerting area can vary, for example, from the size of one building or block up to the whole country or wider international area around the globe. In addition to the position-based messaging, the system also contains a profiling feature, which enables communication groups profiled beforehand. With this feature profiled alerts can be given to selected groups independent of the recipients' geographical location.

The prioritized alerting and warning feature that was tested with the police in the developed smartphone system is based on the commanding authority's official classification of threats and risks or on some other reason for classifying and prioritizing the messages given to users in selected areas or in selected groups. Priorities for alerts and warnings are created in the system with the different alerting tones and volume levels of the handset. These should be chosen and harmonized carefully by the authorities to ensure that users recognize and understand the voice signals instantly and to avoid confusion with other sounds in the environment. Priorities for the alerts and warnings can also be created through vibration, images and the textual features of the handset. Less urgent notifications can be given, for example, as a written text without the sound, vibration or images. Silent alerts, however, may also be needed by authorities for the most urgent of purposes, such as for communication in hostage situations.

Situational awareness in the tested system is created by the commanding authority in different more or less active ways. The least active form of creating situational awareness is based on all ad-hoc information that comes to the commanding authority irregularly from other parties without the authority specifically asking for it. Authorities can also receive emergency information within the system from other systems and sensors, which have been placed in various locations for a specific purpose. Sensors can be set, for example, for monitoring unauthorized motion, toxic gases or other unwanted changes at critical targets. Situational awareness can also be created in the system actively for a selected geographically defined area by sending interactive notifications on the smartphone devices in the area and by assessing the reception data from the devices at one location. The reception data can be processed and presented by the commanding authority in various ways, for example, by placing it automatically on a digital map and by creating in that way a situation picture of the emergency on the basis of direct response from the area. In the authorities' internal use, this technical feature of the smartphone system can be used during the mission by operation management for the command and control of operative forces, for assessing situational information from the operative forces, for making inquiries about reinforcement and for informing or making inquiries for the joint forces regarding some other issues.

Also, the log functionality of the system was tested with the police. With this technical feature, the system automatically creates a log of operations for each smartphone device involved with operative forces in the reported emer-

gency. Through this method, all essential events related to the handset and its user are recorded in the log, which enables the formation of an operational view of the operative forces during the mission. This information may be needed in debriefing or in making reports of completed tasks.

In the experiment, the performance of the smartphone system and user experiences of the police were measured with several indicators. Most attention was paid to response times, which were measured both at the system level and at the behavioral level of each test user in different situations by altering the technical parameters in the system and situations where alerts were given. At the system level, the lead times of alerts and commands were measured by assessing from the system's log all steps from the moment of giving the command from the server to the time when the signatures of the received commands were returned back to the server. For the whole lead time, the time of sending the command from the server, the time of receiving the command by the smartphone handset, the time of signing the command to have been received by the user and the time of receiving the signature by the server were all recorded. As a lead time for a partial process, the performance of the telecommunication network's part in the system was measured by sending, for comparison, the same commands through three different commercial mobile communication operators' networks at the same time. Outside the mobile networks, the more critical part in the response and lead times, however, was the police officers' ability to notice and respond to the given notifications in the test. This was tested by altering the alerting techniques on the smartphone handsets and the situations and environments in which commands were received. The alerting techniques were varied, for example, by changing the alerting tone, volume and vibration on the handsets and the images and texts in the notifications that were sent on the phones. The situations and environments in which the notifications were received were altered by changing the place where and point in time when commands were received. These were, for example, a normal day at the office, outside in the city or at home in the evening or at night.

As a result of the experiment, the tested smartphone system operated in the police force's use as it was designed and expected to. All main parts of the system, such as the server end and mobile end functionalities as well as the mobile networks and other telecommunications parts of the system, operated normally. Also, the main features of the system, such as giving, receiving and signing commands and alerts; localizing and defining alerting zones; creating a situation picture of the alerting zone and/or of officers who were called for duty and creating and reading the log worked as they were designed to. Moreover, some recommendations for improving the system were given, such as concerning the readability of the log and situation map and some icons that were used as visual content of some of the messages during the test.

For the response times, voice signals and vibration helped, in general, the awareness of alerts and commands. In an optimal situation, when alerts were noticed immediately, response times were measured in seconds. In the normal everyday operation of the police, however, there were also situations where

alerts were not noticed at once despite of giving them with the loudest possible tone that the smartphone handset was able to play. The main reasons for the delay in noticing alerts were the noisy urban everyday environment and the places where the test participants kept their handsets during the day. Concerning the awareness of alerts at different times of the day, at the planning stage of the experiment, the police wanted to know whether the operative forces could be alerted and called for duty with the system at night when they were asleep. Surprisingly, alerts were on average better noticed and responded to faster at night than during the daytime. The main reasons for this were that, as there was no other noise around and no other activities going on for the test participants at night, the alerts were heard well, and the participants woke up at once.

In conclusion, the experiment with the police supports the proposition that smartphones can be used for the warning and updating, coordination, command and control, reporting, debriefing, counseling and monitoring of operative forces and for the creation of situational awareness for operation management in general, including and as a part of CBRNE countermeasures and defence. The experiment is reported in the included article PV:

Jaana Kuula, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen and Tuomo Korhonen. Smartphones as an Alerting, Command and Control System for the Preparedness Groups and Civilians: Results of Preliminary Tests with the Finnish Police. *Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013, T. Comes, F. Fiedrich, S. Fortier, J. Geldermann and T. Müller, eds.,* 2013.

3.1.7 Smartphone-based public warning of civilians by the police

In December 2012 in the *Sapporo* project, another smartphone experiment was carried out with the police, this time directed to private citizens. The purpose of the experiment was to test how the same technical features that were tested in the internal use by the police would apply in public warning and crisis management with ordinary private citizens. In the experiment, the contents and risk level of the warning messages were also researched to find out which kind of warnings people would be ready to accept to receive on their personal mobile phones and which ones not. This experiment constitutes an example of giving warnings, updates and advice for private citizens and of crisis management and impact assessment among civilians with smartphones as a part of CBRNE countermeasures. The emphasis of the experiment is for the most part on the general warning techniques and procedures, which are also valid for CBRNE countermeasures, even if in the experiment the textual content of the warnings deals with content other than CBRNE threats.

At the time of the experiment in December 2012, there was no direct public warning system in use in Finland with which authorities would have been able to issue warnings to private citizens' personal communication devices. Instead, all public warnings were given through public radio and television broadcasting. As there was also no localization method in use for public warnings, local emergen-

cy notifications that concerned only a small share of the whole population were heard and seen nationwide in all other parts of the country.

In the experiment, public warnings, updates and advice were given to civilians by the police with the same smartphone system and with the same technical features that were tested a month earlier within the police's internal use in November 2012. The civilian test users' backgrounds varied from young to middle aged and senior persons, whose living conditions and interests varied accordingly.

Although the communication technology and system were the same in the two experiments, the target groups for the communication made the experiments substantially different. In the first experiment, the target group was the police, who represent rescuers in threat situations such as CBRNE. In this role, the police force is a trained, experienced, professional and homogeneous group of people, who are involved in a dangerous situation. Due to this homogeneity, communicating using the tested system with the involved police force during an emergency will evidently produce relatively similar responses, irrespectively of police officers as individual persons. When, however, the same system is applied during an emergency in communication with the civilian population, civilians are in the opposite position and role. Compared with rescue professionals, civilians are casualties, rescuees and endangered people. Additionally, concerning emergencies and threats, they are also an untrained, unexperienced, non-professional and extremely heterogeneous group of people, likely to exhibit unpredictable behavior in the face of the threat. Similarly, in a dangerous situation private citizens may react and respond to public warnings and other crisis communication unexpectedly and in many different ways. Also, private citizens' physical and mental ability to receive and perceive emergency communications with different technologies varies, and the same warnings may be understood, perceived and responded to differently by different people.

Concerning the technical features that create the alerting techniques and priorities for the given messages in the tested smartphone system, the relevance of the same features is different for the professional rescuers and civilians. When the different alerting tones, volumes and vibration are used to help get the alert to be noticed quickly and for prioritizing the content of the message, they can be used basically in the same way with both operative forces and the majority of the civilians. However, for persons with disabilities, the same technical features form a multi-sense warning and messaging system, with which the inability to communicate with one sense can be replaced by receiving messages with another sense. For example, persons who cannot hear voice signals may be able to notice and perceive emergency notifications by utilizing the sense of touch and the vibration functionality of the handset or the sense of sight and emphasized visual images in addition to written text. Visual images may also be utilized in emergency communication with persons who cannot read or understand the local language. However, images may have cultural connotations, but when their usage is prepared carefully, they support the other type of messaging that is given.

Concerning the technical capability of localizing and personalizing the warnings with smartphone technology, these features were tested in the experiment with the police force and civilians to find out whether it would be useful to give different emergency alerts for different geographical areas and for different groups of people. The reasoning for this was that, compared with national radio and television broadcasting, with the localized smartphone system it may be possible to improve the emergency service and safety by giving more detailed warnings and by warning people of smaller threats than with the nationwide public warnings. Although the test groups were small, the experiment indicates that this assumption may not be quite right. As during the experiment people were given localized warnings for minor threats, test users were satisfied with the geographical profiling of warnings, and no people outside the alerting zone were disturbed by unnecessary warnings. However, within the localized alerting zones, there were smaller citizen groups who became irritated by alerts that did not concern them. For example, elderly people did not like warnings that were directed to young people, and people who do not drive a car disliked warnings addressed to car drivers. This indicates that the localized public warnings with small audiences should possibly follow the same principles as the national warnings with wider audiences. The profiling of emergency messages should, however, be researched more, as, for example, persons with disabilities, elderly people and people with different nationalities and languages may need additional support to be able to perceive and understand public warnings. It is possible that smartphone technology is useful in offering this kind of focused public service.

The experiment with the civilians supports the proposition of using smartphone technology for the warning, updating, advising, crisis management and impact assessment of civilians during emergencies. During the tests, private citizens, for example, were given direct warnings by the police, updates on long-term threats and inquiries concerning the threat to which they were capable and willing to respond to interactively with the tested smartphone system. Although during the experiment private citizens were warned with the smartphone system other kinds of emergencies instead of CBRNE threats, there is a reason to believe that a public warning and crisis management system built on smartphone technology would also apply technically for the information management activities of CBRNE countermeasures and defense.

The experiment also implies that, as smartphone technology is more capable than any other communication media for delivering more focused, profiled, detailed, rich, networked and shareable information than any other public warning technology before, authorities need to carefully consider the content of emergency messaging with civilians with such a powerful communication method. Additionally, as shown in the experiments, during the emergency some information can be received by the recipient's device even if the person is not actively responding to the inquiry. There is therefore reason to believe that smartphone technology can also be used, in addition to the follow-up on casualties, for the monitoring of other kinds of protected targets. These are, for exam-

ple, critical infrastructures of which essential information can be assessed with smartphone technology for protection purposes, even if there is no person at the other end to respond to the inquiries concerning that issue.

The experiment with the police and civilians is reported in the included article PVI:

Jaana Kuula, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen and Tuomo Korhonen. Alerting Security Authorities and Civilians with Smartphones in Acute Situations. *Proceedings of the 12th European Conference on Information Warfare and Security ECIW-2013, Jyväskylä, Finland, 11-12. July*, 2013.

The usage of smartphones in the crisis management of civilians in long-term emergencies is also discussed in the following presentation, which is not included herein:

Jaana Kuula. Enriched Crisis Communication with Smartphones in Escalated Emergencies. *The 5th International Disaster and Risk Conference IDRC, Davos, Switzerland, conference presentation, 24-28. August*, 2014.

3.1.8 Smartphone-based alerting and warning within civilian organizations

In the *Sapporo* project, a smartphone-based emergency alerting experiment was also carried out within a civilian organization in one of the 500-student public schools of the City of Jyväskylä in from January to March 2013. The plan of the experiment was discussed with the city police and the designated school police before and during its implementation, but the police did not participate in the actual execution of the experiment. The experiment constitutes an example of operating procedures in large organizations and buildings that are being attacked or that end up in the middle of a severe emergency for some other reason. The rescue plan and operating procedures for these kinds of civilian organizations are not described in the operating concepts of CBRNE countermeasures discussed in the thesis; however, they are essential for survival during serious threats in large premises full of people.

According to the threat scenario of the experiment, a serious situation with hundreds of people in immediate danger begins within the school and has the potential to escalate before rescuers reach the location. The hypothetical situation is especially critical, because the people in the building are children. The main operating procedure in the experiment is that, to save time, the school immediately starts the rescue operation alone with the assistance of the smartphone system before the police and rescue service come to the location. As in this experiment and scenario the school is already in danger before the authorities know about it, the smartphone system needs to be implemented and used in this kind of situation in a different way compared with the two other experiments, where the police operate the system and issue the first warning to the people who are in danger. In this case, the whole system needs to be implemented and operated by

the school, although that cannot replace the public warnings or warning systems provided by the police or other authorities responsible for public safety.

According to the law, the government and municipalities are responsible for public safety and for giving public warnings. However, many organizations and building owners also have responsibilities for the safety of people on their premises. These responsibilities include both beforehand preparedness as well as immediate actions during the emergency. Preparedness includes, for example, maintaining up-to-date rescue plans and installing and maintaining alerting and first response technologies as well as arranging regular evacuation rehearsals. Immediate actions during the emergency obligate, for example, alerting security authorities, warning people in the building and, depending on the type of the emergency, evacuating people out of the building or shutting all windows and doors and keeping people inside the building.

Premises where special rescue plans are required include, for example, schools, elderly people's retirement homes, hospitals, restaurants and hotels, department stores, and office buildings. Many of these have speaker systems in most spaces. Speakers, however, work only in one direction and cannot be adjusted for specialized purposes, such as to give discrete security instructions for selected persons in cases where some people in the building should hear the instructions and others not. When the rescue authorities are not at the location, the personnel working in these buildings are responsible for leading the safety procedures to rescue other people. The responsibility is even greater if the people in the building are minors, elderly, disabled or sick.

The experiment with the school was organized in a building of 500 pupils aged 13–16 years to test how alerts and warnings can be issued with smartphones in a large organization and building full of people and how people can be kept safe without causing panic and chaos among the children. For the experiment, access to the emergency management system was given to a few designated persons for issuing alerts discretely to the teachers' and other personnel's mobile phones and to the electronic bulletin board placed in the teachers' common room. Alerts were not issued to the pupils' phones, because they were underage and under the supervision of the teachers. After receiving the alerts, the teachers and other personnel undertook the safety procedures that were designated for that kind of emergency in the school's rescue plan. The rescue plan was available for the personnel in a printed version at school. To improve its availability, it was digitalized for the experiment and loaded in a shortened version into the tested emergency alerting system to enable quick access with mobile phones.

The shortened version of the rescue plan included practical instructions for the safety measures that should be taken in cases of fire, chemical leak, hostage situation, assault, intrusion, etc. Compared with the experiments with the police and ordinary citizens, the experiment at the school also required other technical modifications to the smartphone system. Firstly, a new kind of emergency call buttons were taken into use at the school. Secondly, a digital map was created for the school building and integrated into the emergency alerting system. Altogether, three types of the emergency call buttons were taken into

use: 1) fixed buttons were implemented for the personnel's use in hidden locations in classrooms and other rooms that have higher safety risks than ordinary classrooms; 2) teachers and other personnel whose personal working environment contains a higher risk were given mobile emergency call buttons, which operate everywhere in the school area and, 3) a software-based digital emergency call button was implemented in the personnel's mobile phones so that they were able to issue a rapid alert everywhere in the school area.

The digital map of the school building was implemented to indicate the location of the emergency, of which warning had been sent with the emergency call buttons. Depending on the severity of the situation, the emergency button calls were programmed to give alerts to the doorman of the school and teachers in the next room, the manager of the school or to the private security company that hired to provide security services for the school. If the police or fire and rescue service was needed, a phone call was always placed to 112. In addition, when the security risk was announced and located with the emergency call button and digital map, a wider emergency alert and instructions for rescuing the children were given to the personnel with the smartphone system. If not all people in the school were in danger, personnel were only notified quietly of the incident without evacuating the children. In the case of greater threats originating from outside of the school, the implemented alerting system was designed to be used in the same way as in the case of the school's internal risks: an alert would be issued to the personnel's mobile phones, and the personnel would start making the pupils safe.

The experiment dealt with two kinds of hypothetic threats: those that take place in the school area and those that happen outside the school yet causing a risk for the people at the school. According to the experiment, there are also in reality minor security risks in the school once in a while, which the school is able to handle without the help of a security company or police. The personnel did, however, report of some kind of insecurity before the experiment and hoped for some support for the situation. According to the survey given to the personnel before and after the experiment, the new emergency alerting system with smartphones and emergency call buttons improved personnel's everyday sense of safety.

The experiment also revealed other issues that need to be taken into consideration in other organizations before a new emergency alerting system is taken into use. First, the rescue plan of the school was originally produced a long time before the existence of digital systems as well as when the potential threats were somewhat different. Although the rescue plan is updated regularly, its structure and content did not fully correspond with the current situation. It was also not possible to integrate and embed the rescue plan into the electronic emergency alerting system in its original form; however, this may not always be necessary if only the most relevant guidance is available in an understandable form at the time and place where it is needed immediately. There was also no digital map of the school, and that needed to be created and integrated into the smartphone system before starting the experiment. In addition, as the school was a heavy structures built in the early 1960s. long before mobile technologies were in use, the

mobile phone signal inside the building was weak, and the local area wireless network was also missing. The situation was improved by implementing an additional amplifier for the mobile phone network and a new wireless local area network inside the building.

In the end, the emergency alerting experiment at the school implied that digital emergency management systems and the rescue plans of large organizations and buildings may need to be improved and integrated better with the security authorities' systems. Regarding CBRNE threats in selected locations, more knowledge may also be needed about the safety procedures in these types of emergencies, and stand-off sensors may be needed in areas and buildings considered to have a certain type of risk. If severe incidents take place in large and crowded buildings such as schools, appropriate rescue plans and high quality detection and warning systems together with the organization's own actions may help to save lives if the rescue service is not immediately at the location.

The results of the experiment are partly reported in the included article PVI:

Jaana Kuula, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen and Tuomo Korhonen. Alerting Security Authorities and Civilians with Smartphones in Acute Situations. *Proceedings of the 12th European Conference on Information Warfare and Security ECIW-2013, Jyväskylä, Finland, 11-12. July*, 2013.

The experiment is also discussed in Finnish in the report "SAPPORO Smartphone Communication in Emergencies – A Case Study of a Rescue Rehearsal of a Chemical Accident," which is not included herein:

Jaana Kuula and Olli Kauppinen. SAPPORO Älypuhelinviestintä Vaaratilanteessa – Tapauskertomus Kemikaalionnettomuuden Pelastusharjoituksesta. *ISSN 2323-4997, ISBN 978-951-39-5573-1, Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisuja 6/2014, 78 s., January,* 2014.

3.1.9 Integrated sensor-based alerting with smartphone technology and a chemical detector

In April 2013, an experiment for a chemical accident was carried out in the *Sapporo* project together with the University of Jyväskylä and the Rescue Department of Central Finland. In the experiment, an ammonia release was staged at the Department of Chemistry and a simulation of automated gas detection followed by an authentic mobile emergency alerting and rescue rehearsal were carried out, including the evacuation and cleaning of the building. The experiment constitutes an example of automated CBRNE threat assessment and integrated alerting with smartphone technology as well as of the joint operation of rescue authorities with a civilian organization.

The experiment began by staging a chemical accident with a small volume of ammonia. As a part of the simulation, the chemical release was noticed by an

automated stand-off chemical detector, which was integrated with the observation system of the public emergency alerting center (112) and with the communications unit of the university. After the release of the chemical, the automatic detector launched an alert to 112 and from there to the fire and rescue department. Simultaneously, the detector also gave an automatic alert to the communications unit of the university, where the first warning of a chemical release was given on the mobile phones of the university personnel working in the building of the department of chemistry. The warning was given as an interactive forced emergency message with the smartphone push notification method and, for comparison, also as an SMS message with a commercial telecommunication operator's system. Later on when more details of the chemical release were received from the security manager at the emergency site, and when the rescuers were also working on the accident, more information was given about the incident with the same two systems to the people in the area.

During the experiment the warning, the messages that were given with the smartphone got through faster than the SMS messages. The first smartphone warnings were received and signed in less than 30 seconds, whereas the SMS messages reached the same persons at their best in 8-10 minutes. At that time, people had already been evacuated out of the emergency building and collected in the evacuation area in fresh air. The clear difference in the delivery times between the two messaging techniques is possibly caused by the different data transfer techniques of the systems, as the smartphone-based warnings are delivered as direct data transmission, whereas SMS messages are delivered through another channel, where they are mixed with the speech of ordinary phone calls. There may also be other reasons for the difference in delivery times between the two techniques, and, to obtain statistical confirmation for the lead times, a separate speed test should be conducted in a wireless data communication laboratory or in a wider living lab. In this experiment, however, the lead times for the smartphone-based warnings were explicitly faster.

In the experiment, a visual situation picture was also formed on the map in regard to the condition of the people in the risk area. According to the feedback information received from the people's smartphones in the emergency area, all people received the first warning of the gas release very quickly, and most of them managed to get to safety quickly. One person, however, had gotten stuck in a closed area behind the gas and was not able to get out. With the smartphone system, her situation was identified, her position was located quickly and fire fighters were able to carry her out with a gas mask on her face.

The experiment implies also that the alerting, warning and rescue processes are not synchronized and that all these processes need to be adjusted before interactive mobile alerting and warning systems are taken into use. When a mobile warning system is in use, critical questions include, for example, at which point exactly should people in the emergency building and surrounding zone be warned and by whom? Concerning large organizations, should the warnings to the environment be sent immediately from the exact point where the emergency is taking place, such as in this experiment from the chemical de-

partment where the gas release was first noticed? Or, should all warnings be delivered according to the organization's communication policy from one place only, such as in the experiment from the communications unit of the university? Or, should warnings be issued only by the authorities, in this case by the emergency alerting center 112?

Another critical question during the experiment was, where exactly should the smartphone responses from the people in the emergency area should be directed? Should they be addressed to the management of the organization's own crisis communication system, in this case to the communications center of the university, or should they be directed like all ordinary emergency phone calls to the public emergency alerting center at 112? Or instead, should the emergency response from the smartphones at the emergency site be directed to the field manager of the rescue operation, who already knows the situation and is in charge of the rescue operation at that particular site? During the experiment, there was no direct link for connecting the endangered person's phone from the contaminated building with the field manager of the rescue operation, and the only alternatives were to send the response to the communications unit of the emergency organization, or to make a phone call to 112. As this was an experiment, the smartphone system was not implemented fully with the operating protocols of the university and rescue service.

The experiment shows that the threat and risk assessment for CBRNE hazards can be performed in large organizations and buildings with smartphone technology in two ways. First, various stand-off detectors can be installed in the building and integrated with the smartphone system. In this way the two technologies, the CBRNE sensors and smartphone system together, comprise an automated detection and alert system for CBRNE threats. Stand-off detectors can also be commanded from the distance, for example, for activating them to operate and carry out desired actions when necessary. In this experiment they were demonstrated only as an example of autonomous devices, which give an alerts when the sensor detects anomalies in the environment. The threat and risk assessment can also be conducted with smartphone technology by sending interactive notifications to the hazard zone and by automatically collecting the position and feedback information on a virtual real-time situation map. This technical feature was demonstrated in the experiment with the person who was not able to come out of the building because of the toxic cloud.

The experiment also shows that these kinds of warning systems cannot be implemented in large organizations for warning and emergency management use just by installing them on servers and end-user devices. Instead, implementation needs to be designed carefully by re-evaluating and redesigning the crisis management, warning and rescue processes in the organization. In addition, the same re-evaluation of emergency management and rescue processes needs to be done for the joint operation of the emergency organization and rescue authorities so that each party's responsibilities are clear for all, both for the physical rescue operations and for the information processes during the operation.

The experiment is described and reported in Finnish in "SAPPORO Smartphone Communication in Emergencies – A Case Study of a Rescue Rehearsal of a Chemical Accident," which is not included herein:

Jaana Kuula and Olli Kauppinen. SAPPORO Älypuhelinviestintä Vaaratilanteessa – Tapauskertomus Kemikaalionnettomuuden Pelastusharjoituksesta. *ISSN 2323-4997, ISBN 978-951-39-5573-1, Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisuja 6/2014*, 78 s., January, 2014.

3.1.10 Tabletop rehearsal of the hyperspectral threat assessment and smartphone-based public warning in a real life explosion threat situation

In July 2013 there was a serious explosion threat situation at the explosives manufacturing plant near the City of Jyväskylä, and Finland's largest evacuation of civilian people during peacetime was carried out around the plant. Concerning this incident, a mental rehearsal was carried out for reviewing step by step in which ways the hyperspectral technology and smartphone technology could have been utilized in the CBRNE countermeasures of this emergency.

The rehearsal here constitutes a tabletop experiment of the hyperspectral threat assessment, prediction and monitoring of a CBRNE threat and of the smartphone-based public warning, informing, reachback and resource requirements assessment of the reinforcement, joint forces, authorities and hospitals, the establishment of a casualty office, multiagency support, notifying, giving situation reports and providing specialists notifications, the long-term health monitoring of people involved and of the joint operation with authority and civilian organizations.

The threat was caused by an overheated container of chemical waste, which presented a detonation risk for stored explosives equating 150 tons of TNT. The situation started late on a Tuesday evening, and the first risk assessment and evaluation of the situation was made during the night by the local rescue authority, the Rescue Department of Central Finland, who were in charge of the rescue operation. Also, the Central Finland Police Department and the Finnish Defence Forces were informed and alerted of the situation, and operative actions were carried out jointly by the three authorities. In addition, the local central hospital was alerted to be prepared for possible patients, and the volunteer civilian aid organization the Red Cross was asked for help with the evacuation. Close discussions were also held with the management of the plant and the local municipality of Laukaa, and additional support was received from the local church.

When the problem with the container was noticed, the precise constitution of the chemical was not known, because the waste was not produced at the plant. However, overheating was believed to have been caused by impurities in the mixture, and it was considered unsafe to remove the container or to go near it. All people within the risk area were therefore evacuated into an evacuation center at a public school. The evacuation was organized and secured by the po-

lice and defence forces, and the entry to the evacuated area was restricted. The Red Cross assisted the evacuation particularly by offering support for elderly and disabled people and for mothers with small babies.

Changes in the condition of the container were monitored from the air with a video camera mounted in a drone. Otherwise, all air traffic above the site was forbidden. At the same time, the container was cooled down with water with the assistance of a remotely controlled ground-operated robot provided by the defence forces. Evacuation was begun early the next morning on Wednesday, and the container was cooled down over the course of the whole day. By late in the evening, the container had been removed out of the area, and people were transported back to their homes. On the following morning on Thursday, the rescue organization was taken down, and the operation was declared ended.

In the aftermath of the incident, the fire and rescue department and other authorities were appreciated for the successful operation and for countering the severe threat. The detailed content and reason for the abnormal behavior of the unstable tank were, however, sorted out only later in a laboratory analysis and through a thorough inspection of the logistics trail of the chemical waste made by the Finnish Safety and Chemicals Agency Tukes. The crisis communication during the three days of the incident was considered by the public media to have failed. For example, it was criticized that the evacuated individuals did not receive the necessary information at any stage of the incident and that people in other parts of the country became disturbed by the emergency notifications given repeatedly on national radio and television broadcasts during the incident. Two months later, on September 9, 2013, the Rescue Department of Central Finland organized a "lessons learned" type of discussion and debriefing event about the incident for the rescuers and other stakeholders around the country. The event began with prepared statements given by all the authority organizations involved in the rescue operation as well as by the local municipality, the explosives plant, the Red Cross and Tukes. Prepared presentations were followed by open discussion, which was held actively. In general, people considered the debriefing event and experience received from the incident useful.

In the investigation report by Tukes (2016), the origin of the steaming tank was located at an external mining site outside the plant, and its contents were defined as sensitized emulsion explosives, rock material, two detonators and other impurities. As a result, the report gave further recommendations for improving safety with explosives. Also, the legislation was ordered to be improved, especially concerning the handling of emulsion explosives.

After the explosion threat situation, a mental rehearsal was carried out at the university to evaluate stage by stage how hyperspectral detection technology and smartphone technology may have been used for countering the situation. The rehearsal indicated that at the beginning of the threat situation, it may have been possible to use hyperspectral technology from a distance to determine, without touching and sampling, something about the chemical contents of the container had it been brought with an unmanned airborne or ground-based vehicle in direct visual contact with the tank or with the leaking steam. Even if

the full constitution of the chemical mixture could not have been determined immediately, indications may still have been received about the toxicity of the chemical or about its tendency to explode. It may also have been possible to trace with the hyperspectral camera the potentially toxic and invisible chemical cloud that had been created by the released steam. In addition, it may have been possible to detect and follow the logistics trail of the harmful container during the inspection after the incident. This tracing of the logistics trail would have been needed particularly if there was disagreement about the origin, handling and contents of the container or if it was not possible to trace such issues with any other method. However, during the incident it may not have been possible to discover possible objects at the bottom of the tank with the hyperspectral technology unless some identifying particles would have come out with the leaking steam. According to the inspection report, there were, for instance, emulsion explosives and two detonators in the tank.

With the smartphone system, the rescue department would have been able to give the first notification and alert about the threat to their own staff; other authorities, such as the police and defence forces; government officials, such as the responsible persons at the ministry of interior; hospitals and municipality officials and civilian aid organizations such as the Red Cross quickly, efficiently and at a low cost. After making the decision on the evacuation of the approximately 2,000 people, it would also have been possible to give the first warning with the smartphone system directly to the inhabitants in the risk area. This would have been possible to do before the evacuation buses with the support of the police and defence forces were at the people's doors, waking them up early in the morning. In the actual situation, people had practically no time to prepare before the evacuation, for which reason they were not able to take their daily medicine or any other essential matter with them or to take care of their livestock or other urgent issues at their homes.

During the day, in the evacuation center, people followed public news on the radio. That information was, however, directed to the broad audience of the whole country, and it was not confirmed by the authorities for all parts. The public news did not much serve the evacuated people, who needed practical information of how the situation was developing, what was happening to their property and when they would be able to return to their homes. It would have been possible to easily give this kind of information directly to the evacuated people's mobile phones. With the same system, people would also have been able to ask the authorities about many other issues that were bothering their minds. In the actual case, they received only a little information about the situation and were not able to be in contact with the authorities or ask any questions. Also, the civilian aid organization the Red Cross was in the same position and did not receive much more information over the course of events. Their role in the evacuation center was to comfort and support the evacuated people, and, as they were not fully aware of what was happening with the threat, they were not able to support the people as much as may have been needed. With the smartphone system, the Red Cross would have been better informed. With the

system, the Red Cross would also have been able to quickly assess the availability of volunteers to come help and to invite available persons to work. After the first warning, it would have been easy with the smartphone system to give updates about the situation to all the involved persons over the three days. It would also have been possible to give additional crisis support to the persons who needed it during and after the incident. Overall, with the support of the smartphone system, much of the communication and information needs of the local people and other relevant stakeholders would have been improved. At the same time, the public media would have been able to focus on doing other work, and the rest of the population, 5.5 million people, would not have been disturbed about the updates and repeated notifications on the national radio and television channels, which were not primarily directed to them.

The tabletop experiment indicates that there is a chance that hyperspectral technology can be used for the remotely controlled unmanned assessment and monitoring of CBRNE threats and for the assessment and monitoring of the spread of toxic clouds of imperceptible particles originating from a CBRNE source. The experiment also implies that hyperspectral technology can be used for tracing the logistics trail of transporting and handling a suspicious CBRNE source. The experiment also suggests that smartphone technology can be used for assessing the availability of operative forces and resources and for alerting, notifying and informing other authorities and joint forces about the CBRNE threat. Accordingly, the experiment suggests that smartphone technology can be used for alerting and notifying civilian joint and aid organizations, such as hospitals and Red Cross. According to the experiment, smartphone technology can also be used for the early warning of civilians in the case of a CBRNE threat, for giving them time to be prepared with any necessary medication and other essentials for the evacuation. Additionally, the smartphone system can be used for updates to keep the evacuated people informed about the development of the CBRNE threat. The emerged experiences and needs in the evacuation center also indicate that the same technology could be used by the evacuated people and their closest relatives to make inquiries about the condition of their homes and of individuals who have been involved with the threat inside the risk or evacuated area. In this form, the smartphone system would also be useful for the operation of the casualty office. Based on this real-world CBRNE incident, smartphone technology can also be used for the prolonged crisis support and long-term health monitoring of the involved operative forces and civilian population during the recovery phase of the emergency.

The tabletop rehearsal of the usage of the smartphone system in the 2013 explosion threat situation is discussed in the following publications, which are not included herein:

Jaana Kuula and Olli Kauppinen. SAPPORO Älypuhelinviestintä Vaaratilanteessa – Tapauskertomus Kemikaalionnettomuuden Pelastusharjoituksesta. *ISSN 2323-4997, ISBN 978-951-39-5573-1, Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisuja 6/2014, 78 s., January,* 2014.

Jaana Kuula, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen and Tuomo Korhonen. Alerting Security Authorities and Civilians with Smartphones in Acute Situations. *Proceedings of the 12th European Conference on Information Warfare and Security ECIW-2013, Jyväskylä, Finland, 11-12. July*, 2013.

Jaana Kuula. Enriched Crisis Communication with Smartphones in Escalated Emergencies. *The 5th International Disaster and Risk Conference IDRC, Davos, Switzerland. Conference presentation, 24-28. August,* 2014.

3.2 Results

The main research question in the study is

Can hyperspectral technology and smartphone technology be used for CBRNE countermeasures and defence?

In the following, this question is viewed and evaluated through sub-questions to find out whether the two technologies can, according to the experiments described in section 3.1, sufficiently fulfill the capability requirements of the military and civilian operating concepts for CBRNE countermeasures and defence (EDA, 2014; CF, 2012; NATO, 2008; Lefebvre, 2015) presented in sections 2.2.3–2.5.2. A satisfactory result is received if either one of the technologies is capable of fulfilling a reasonable share of detailed requirements defined in the described operating concepts.

Evaluation is carried out separately for hyperspectral technology and for smartphone technology. For hyperspectral technology, the evaluation is based on its capability for detecting, identifying and monitoring (DIM) CBRNE substances and threats and for smartphone technology on its ability to carry out the information management (IM) tasks of a CBRNE incident, including alerting and warning of CBRNE emergencies.

The evaluation of the main research question is carried out with sub-questions HQ1–HQ3 for hyperspectral technology and with questions SQ1–SQ8 for smartphone technology. Each sub-question is evaluated with the same procedure by first analyzing which of the individual capability requirements in the operating concepts relate with that particular research question. The selected capability requirements are then compared with the empirical experiments to determine which of the experiments relate with the particular capability requirements and whether the experiment results indicate that those requirements can be fulfilled with hyperspectral or smartphone technology. This evaluation process is visualized in Figure 12.

When all the sub-questions are evaluated through this procedure, the overall result of the study is generated as a summary of the evaluation results of all individual questions. In the evaluation, the following abbreviations are used:

- HQn: research question number (n) for hyperspectral technology
- DIM Mn: capability requirement number (n) for the detection, identification and monitoring of the threat in the military operating concepts for CBRNE defence, taken from Table 7
- DIM Cn: capability requirement number (n) for the Detection, Identification and Monitoring of the threat in the Civilian operating concepts for CBRNE countermeasures, taken from Table 8
- HEn: empirical experiment number (n) for hyperspectral technology, presented in section 3.1

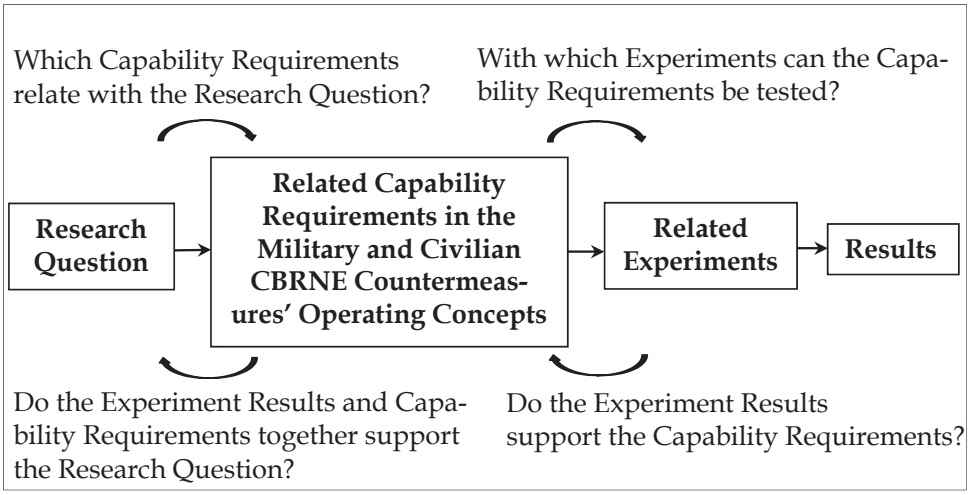


FIGURE 12 The evaluation process of the research questions

- SQn: research question number (n) for smartphone technology
- IM Mn: capability requirement number (n) for information management in the military operating concepts for CBRNE defence, taken from Table 9
- IM Cn: capability requirement number (n) for information management in the civilian operating concepts for CBRNE countermeasures, taken from Table 10
- SEn: empirical experiment number (n) for smartphone technology, presented in section 3.1

3.2.1 Hyperspectral technology in the detection, identification and monitoring of CBRNE threats

The research question

HQ1: Can CBRNE substances be detected with hyperspectral technology in indoor conditions?

is evaluated with the military and civilian capability requirements and empirical experiments, which are presented in Table 11. In the table, the military capability requirements DIM M4 and DIM M7 and civilian requirements DIM C1–C5 and DIM C26 of the operating concepts for CBRNE countermeasures and defence demonstrate how the detection of CBRNE substances is required in various situations during the CBRNE incident. Although not mentioned specifically, these situations also include detection in indoor environments, as CBRNE incidents may take place in such conditions.

TABLE 11 Capability requirements and experiments related to question HQ1

HQ1: Can CBRNE substances be detected with hyperspectral technology in indoor conditions?
Related capability requirements:
• DIM M4: Identifying CBRNE agents • DIM M7: Providing spectral data
• DIM C1: Carry out scene assessment • DIM C2: Recognize signs and indicators of CBRN incidents • DIM C3: Determine whether CBRN or hazardous material incident • DIM C4: Carry out risk assessment • DIM C5: Undertake hazard identification
• DIM C26: Decontaminate hospitals (i.e., confirm the cleaning result)
Related experiments:
HE1: Hyperspectral detection and identification of explosives and explosives' residues
HE2: Hyperspectral detection and identification of CWAs and simulants

The discussed capability requirements confirm, for their part, that research question HQ1 for hyperspectral technology's capability of detecting CBRNE substances in indoor environments is relevant for CBRNE countermeasures and defence. The requirements also specify in more detail what kinds of detection tasks hyperspectral technology (like other detection technologies) are required to perform in indoor conditions.

Table 11 also indicates that the discussed capability requirements are tested in the study with experiments HE1 and HE2. According to experiment HE1, explosives and, on the basis of experiment HE2, CWAs and TICs can be detected with hyperspectral technology in indoor environments. Thereby the two experiments confirm that hyperspectral technology is capable of fulfilling the capability requirements of CBRNE countermeasures and defence related to research question HQ1. For example, hyperspectral technology is capable of fulfilling the military capability requirements DIM M4: Identifying CBRNE agents

and DIM M7: Providing spectral data, and the civilian requirement DIM C5: Undertake hazard identification. At the same time, these experiments confirm a positive result for the question HQ1 of hyperspectral technology's capability of detecting CBRNE substances in indoor conditions. Concerning capability requirement DIM C26for confirming the cleaning result as a part of decontaminating hospitals in Table 11, this requirement indicates that the research question is relevant in this context. This particular requirement was however not directly tested in the referred experiments, and the most alike examples were the experiments that were carried out with the Forensic Laboratory of NBI for confirming with hyperspectral technology the cleaning result of materials covered with blood. Washing methods for CWAs and blood are however different, so the research results are not fully comparable.

Table 12 presents the capability requirements and experiments in CBRNE countermeasures and defence that correspond to the research question

HQ2: Can CBRNE substances be detected with hyperspectral technology in outdoor field conditions?

Requirements DIM M1, M3, M4, M7 and M8 of the military and DIM C1–C5 of the civilian countermeasures represent examples of various situations where detection needs to be carried out in outdoor conditions. On the basis of these requirements, the research question HQ2 is relevant for CBRNE countermeasures and defence.

Table 12 also shows that in the study, the related capability requirements for question HQ2 are tested with experiments HE1, HE2 and HE3. The results of experiments HE1 and HE2 show that explosives, explosives' residues, CWAs and TICs can be detected with hyperspectral technology in indoor environments. This evidence supports, but does not necessarily confirm, that such substances can also be detected directly on the target with the same technology in outdoor environments. Indoor conditions can, however, be built into field by bringing a mobile laboratory to the CBRNE site.

In experiment HE3, explosives are imaged in outdoor field conditions on soil, asphalt and grass with hyperspectral technology from an airborne drone. Although the imaging result is not ideal due to the limited properties of the available camera, the experiment demonstrates how the on-site hyperspectral detection of CBRNE substances can be carried out directly on the ground with an airborne hyperspectral camera mounted in a drone. In addition, experiment HE3 demonstrates how the airborne hyperspectral detection is carried out at a short distance compared with the widely used remote sensing, where targets are detected from tens of kilometers' distance or further.

As a conclusion, experiments HE1, HE2 and HE3 together support the proposition that CBRNE substances can be detected with hyperspectral technology in outdoor field conditions. This conclusion also supports the positive result for research question HQ2.

TABLE 12 Capability requirements and experiments related to question HQ2

HQ2: Can CBRNE substances be detected with hyperspectral technology in outdoor field conditions?
Related capability requirements:
• DIM M1: Verifying the hazard prediction area • DIM M3: Operating in built-up areas • DIM M4: Identifying CBRNE agents • DIM M7: Providing spectral data • DIM M8: Monitoring contaminated areas
• DIM C1: Carry out scene assessment • DIM C2: Recognize signs and indicators of CBRN incidents • DIM C3: Determine whether CBRN or hazardous material incident • DIM C4: Carry out risk assessment • DIM C5: Undertake hazard identification
Related experiments:
HE1: Hyperspectral detection and identification of explosives and explosives' residues
HE2: Hyperspectral detection and identification of CWAs and simulants
HE3: Airborne hyperspectral detection of explosives and biological spots

Table 13 presents the capability requirements and experiments that are related to the question

HQ3: Can hyperspectral detection technology be utilized at the different stages of the timeline of a CBRNE incident?

In the table, the qualifications DIM M1, M4, M7 and M8 represent examples of military requirements and DIM C1, C10, C15, C16, C25 and C26 examples of civilian capability requirements of CBRNE countermeasures and defence that correspond with research question HQ3. The requirements demonstrate how CBRNE detection is needed at the different stages of the timeline of a CBRNE incident and also how research question HQ3 is relevant for CBRNE countermeasures. For example, the scene must first be assessed, the hazard area confirmed and CBRNE agents identified. After that, hot, warm and cold zones need to be defined and cordoned. In its own time, evidence for criminal investigation also needs to be identified, maintained and collected, possibly including CBRNE detection. Later on, responder vehicles, equipment, hospitals and other possible targets need to be decontaminated, potentially by confirming the decontamination result by repeating the detection. The presented examples focus on the immediate CBRNE incident, but in the reality the full timeline of the incident may be longer and include more stages, for example, for revealing the preparation of a CBRNE attack or for investigating the cause of the incident.

Table 13 also indicates that the capability requirements related to research question HQ3 are tested in the study with experiments HE1, HE2, HE3, HE4 and HE5. As discussed above related to questions HQ1 and HQ2, experiments HE1, HE2 and HE3 demonstrate how explosives, explosives' residues, CWAs and TIMs can be detected with hyperspectral technology in indoor and outdoor conditions and from the air with a drone. Related to research question HQ3, the same experiments demonstrate how hyperspectral detection can be utilized at the early stages of a CBRNE incident, for example, for verifying the hazard area and for indicating the presence of and identifying CBRNE agents. The demonstration of the airborne hyperspectral detection in experiment HE3 also shows how the technology can be used at the early and later stages of the timeline for surveying the area and for monitoring the spread of contamination. Experiment HE1 also clearly shows how hyperspectral technology can be used for both pre- and post-blast detection of CBRNE substances, as in the experiment both unexploded explosives and explosives' residues are detected with this technology. In addition, in the laboratory tests of experiment HE3, fingerprints containing traces of explosives were detected on various surfaces, which demonstrates the forensic investigation being carried out as a part of security authorities' work due to a serious CBRNE incident.

TABLE 13 Capability requirements and experiments related to question HQ3

HQ3: Can hyperspectral detection technology be utilized at the different stages of the timeline of a CBRNE incident?
Related capability requirements:
• DIM M1: Verifying the hazard prediction area • DIM M4: Identifying CBRNE agents • DIM M7: Providing spectral data • DIM M8: Monitoring contaminated areas
• DIM C1: Carry out scene assessment • DIM C10: Establish inner and outer cordon (hot/warm/cold zone) • DIM C15: Preserve scene and maintain evidence to the extent possible (criminal investigation) • DIM C16: Carry out coordinated evidence collection • DIM C25: Decontaminate responder vehicles/equipment • DIM C26: Decontaminate hospitals
Related experiments:
HE1: Hyperspectral detection and identification of explosives and explosives' residues
HE2: Hyperspectral detection and identification of CWAs and simulants
HE3: Airborne hyperspectral detection of explosives and biological spots
HE4: Hyperspectral detection of blood, other biofluids and biological markers
HE5: Hyperspectral forensic investigation of a crime scene

Experiments HE4 and HE5 demonstrate the hyperspectral detection of blood, biofluids and other biological markers as well as other forensic details,

such as contaminated soil, drugs, traces of fires and arson, traces of gunshots, counterfeit documents etc. Of these, the human-based traces may possibly be connected with CBRNE triage, but also with forensic investigation, such as all materials tested in experiment HE5. As a conclusion, all these examples of experiments HE1–HE5 demonstrate how hyperspectral technology can be utilized at all stages of the timeline of a CBRNE incident, which also confirms a positive result for research question HQ3. Concerning capability requirement DIM C25 and C26 for confirming the cleaning result as a part of decontaminating responder vehicles/equipment and hospitals in Table 13, these requirements indicate that the research question is relevant in this context. The two requirements were however not tested in the referred experiments, and the only reference of this kind of requirement was gained with the experiments that were carried out with the Forensic Laboratory of NBI for confirming with hyperspectral technology the cleaning result of materials covered with blood. Washing methods for CWAs and blood are however different, so the research results are not fully comparable.

3.2.2 Smartphone technology in the information management of a CBRNE incident

The related capability requirements and empirical experiments of the sub-research question

SQ1: Can mass alerts, warnings and command and control activities be issued with smartphone technology?

are presented in Table 14. The question SQ1 specifies on one part the wider issue, which is discussed with the main research question about the usability of smartphone technology in CBRNE countermeasures and defence. Table 14 presents examples of military and civilian capability requirements that relate with this subject. They also indicate that question SQ1 is relevant and valid for CBRNE countermeasures and defence. For example, requirements IM M1, M13, M22 and M23 demonstrate how the mass deliveries of digital messages, such as warning messages and other notifications, need to be given in the military context to the troops and to the management of the defence organization. In the civilian operating model, requirements IM C4 and C6 stand for carrying out similar tasks for the first responders and for the management of their own organization. The civilian operating concept notifications need to also be given to large numbers of private citizens, as is defined by capability requirement IM C8.

The capability requirements in the civilian operating concept also show how the commanding authority needs to notify during a CBRNE emergency, in addition to their own organization, many other related organizations. Requirements IM C9, C10 and C21 indicate that particularly authorities at the local, regional and national levels, CBRNE specialists in various locations and hospitals need to be notified in such a situation.

TABLE 14 Capability requirements and experiments related to question SQ1

SQ1: Can mass alerts, warnings and command and control activities be issued with smartphone technology?
Related capability requirements:
• IM M1: Warning troops endangered by CBRN hazard in near real time • IM M13: CBRNe warning, reporting and CBRNe reachback • IM M22: Warning & reporting • IM M23: Warning messages • IM C4: Provide and obtain regular updates to and from first responders • IM C6: Provide situation report to emergency control rooms etc. and request assistance if necessary • IM C8: Provide timely warnings and advice to the public (immediate vicinity and beyond as necessary) • IM C9: Notify appropriate authorities at local, regional and national levels (governmental and responder agencies) • IM C10: Notify specialists (chemical, biological, radiological/nuclear, medical) • IM C21: Provide information to hospitals
Related experiments:
SE1: Smartphone-based alerting, command and control of the special forces of the police SE2: Smartphone-based public warning of the civilians by the police

As is indicted in Table 14, the capability requirements related to question SQ1 are tested with experiments SE1 and SE2. In experiment SE1, a smartphone-based alerting, warning and command and control system is tested within the police force's internal use by experimenting with all possible functionalities of the system with the representatives of different units of the police force around the country. In experiment SE2 public warnings are given with the same smartphone system by the police to the test group of private citizens.

As a result, in experiments SE1 and SE2 mass alerts, warnings and command and control messages are given successfully by the police. In experiment SE1 the given notifications are also received and responded to successfully by the police. In experiment SE2 notifications are also received and responded to successfully by the civilian people. In all, the results of experiments SE1 and SE2 confirm that the related capability requirements of CBRNE countermeasures and defence can be fulfilled with smartphone technology. The results of the two experiments also confirm a positive result for research question SQ1.

The research question

SQ2: Can the intensity of alerting be adjusted with smartphone technology?

discusses the capability of and need for giving notifications with a different volume of sound during a CBRNE incident. In this question, the concept of alerting

refers to the giving of emergency alerts or to the notifying for a received emergency message. This issue and the need for altering the alerting mode or tone are not discussed directly in the discussed capability requirements of the military and civilian CBRNE countermeasures and defence. However, the examples of capability requirements included in Table 15 represent different situations of giving CBRNE emergency notifications, from which can be concluded that some

TABLE 15 Capability requirements and experiments related to question SQ2

SQ2: Can the intensity of alerting be adjusted with smartphone technology?
Related capability requirements:
• IM M1: Warning troops endangered by CBRN hazard in near real time • IM M12: CBRNe advice and assessment including CBRNe intelligence • IM M13: CBRNe warning, reporting and CBRNe reachback • IM M22: Warning & reporting • IM M23: Warning messages • IM C4: Provide and obtain regular updates to and from first responders • IM C6: Provide situation report to emergency control rooms etc. and request assistance if necessary • IM C8: Provide timely warnings and advice to the public (immediate vicinity and beyond as necessary) • IM C9: Notify appropriate authorities at local, regional and national levels (governmental and responder agencies) • IM C10: Notify specialists (chemical, biological, radiological/nuclear, medical) • IM C21: Provide information to hospitals • IM C26: Provide timely warnings or advice to public
Related experiments:
SE1: Smartphone-based alerting, command and control of the special forces of the police
SE2: Smartphone-based public warning of civilians by the police

situations and notifications are more urgent than others. In addition, the situations potentially also contain other properties, for which reasons alerting should be made in a different way. For example, military requirements IM M1 and M12 deal with the warning of troops and with carrying out CBRNe intelligence, whereas the civilian requirement IM C4 defines the giving of similar warnings to first responders and IM C8 to the public. The first requirement for the high priority emergency alerts for all audiences is that they should be noticed and understood immediately. Often the recipients' attention is evoked with a standardized and strong voice signal, either mechanically or digitally. Different voice signals can also have different information content.

When the situations of troops and first responders are compared, it is possible that the troops (or the police) are required to operate as quietly as possible. This can be a situation such as during a terrorist attack, where the intruder can

still be around and capable of causing additional damage. Silent operation may also be needed in various situations in carrying out CBRNe intelligence. Due to these reasons, a strong voice signal may not be ideal for alerting in regard to all kinds of issues, and there may therefore be a practical need to alter the alerting tone or mode. The different alerting mode instead of sound could be, for example, the utilization of the sense of touch in the vibration function of a smartphone. Specialized alerting tones and modes may also be needed for private citizens for differentiating the emergency alert from other sounds and signals in the environment.

Table 15 also indicates that research question SQ2 is tested with the police and civilians in experiments SE1 and SE2. In experiment SE2, the alerting mode, tone and intensity of the alert are altered in the tests with the police inside the police organization, for example, when the alerts and notifications are given at different times of the day and in the middle of the night. It is clearly shown that alerts given with a different intensity and tone, or in a different mode, are recognized differently and that also the response times to different alerts vary. The

recognition of alerts is, however, not dependent on the type of alerts only, as also the situation, environment and time of the day have an effect on whether and how quickly alerts are noticed.

To summarize, the discussed capability requirements IM M1, M12, M13, M22, M23 and IM C4, C6, C8–10, C21 and C26 indicate that emergency warnings and notifications need to be given during a CBRNE incident in many different situations and for many different audiences and purposes. It is therefore possible that in these situations different alerting methods are also useful or needed. Research question SQ2 is thereby relevant and valid for CBRNE countermeasures and defence. The test results of recognizing and responding to alerts given in a different mode and with a different intensity and tone by the police and civilians in experiments SE1 and SE2 confirm that the intensity of alerting can be adjusted with smartphone technology. With these conclusions, a positive result is also confirmed for research question SQ2.

The research question

SQ3: Can mass alerts, warnings, command and control and other notifications be focused and scaled geographically and according to different recipient groups with smartphone technology?

addresses the question of the capability of and need for giving emergency notifications to smaller and more focused groups of people instead of the entire personnel of rescuers or troops or of the whole population of private citizens. The related capability requirements and experiments of question SQ3 are represented in Table 16. The discussed operating concepts do not specifically define that the geographically or by the recipient groups focused and scaled notifications are required in CBRNE countermeasures and defence. The included capability requirements IM M1, M7, M12 and M15 and IM C4, C8, C9, C10, C19 and

C21, however, indicate that during a CBRNE incident, various notifications must be given to different audiences, who are either a) located in a certain geographical area or b) representatives of a particular group. For example, the requirements IM M1 for providing warnings to troops, IM C4 for providing updates to first responders and IM C8 for providing warnings and advice to the public describe situations where notifications must be given to various audiences

TABLE 16 Capability requirements and experiments related to question SQ3

SQ3: Can mass alerts, warnings, command and control and other notifications be focused and scaled geographically and according to different recipient groups with smartphone technology?
Related capability requirements:
• IM M1: Warning troops endangered by CBRN hazard in near real time • IM M7: Providing CBRN situational awareness applicable at strategic, operational and tactical levels • IM M12: CBRNe advice and assessment including CBRNe intelligence • IM M15: Provide CBRN-related technical and scientific reachback • IM C4: Provide and obtain regular updates to and from first responders • IM C8: Provide timely warnings and advice to the public (immediate vicinity and beyond as necessary) • IM C9: Notify appropriate authorities at local, regional and national levels (governmental and responder agencies) • IM C10: Notify specialists (chemical, biological, radiological/nuclear, medical) • IM C19: Assess resource requirements (short, medium and long term) • IM C21: Provide information to hospitals
Related experiments:
SE1: Smartphone-based alerting, command and control of the special forces of the police SE2: Smartphone-based public warning of civilians by the police

within a certain geographical area. Accordingly, the requirements IM M12 for CBRNE advice, assessment and intelligence and IM C10 for notifying chemical, biological, radiological/nuclear or medical specialists define communication tasks that are carried out with a certain group of persons only, either within a certain geographical area or independently from their physical location. With these specifications, research question SQ3 can be considered relevant and valid for CBRNE countermeasures and defence.

As is indicated in Table 16, research question SQ3 is tested with experiments SE1 and SE2. Within these experiments various emergency notifications are given with the smartphone system by the police to police officers and to private citizens selectively on the basis of their geographical location or by the personal group or profile that they present. During the tests, notifications are given successfully based on the recipients' geographical location by changing the center point and range of the alerting area several times, which demon-

strates that the giving of focused and scaled notifications for varying numbers of people is possible with smartphone technology. The results of experiments SE1 and SE2 thereby also confirm a positive result for research question SQ3.

Research question

SQ4: Can mass alerts, warnings and command and control notifications be given interactively with smartphone technology?

addresses the question of the capability of and need for giving interactive notifications during a CBRNE incident. The discussed CBRNE operating concepts do not specifically indicate that these functions should be carried out with two-way communication. It can, however, be concluded that, for example, the communication tasks within the capability requirements presented in Table 17 can or should be interactive. For example, requirements IM M1 for providing warnings to troops or IM C8 for providing warnings to the public can in principle include an interactive feature with which the command of the operation or the reachback center can have direct and prioritized information from those who are believed to be in danger. The military capability requirements IM M12 and civilian requirements IM C2, C4 and C19 indicate the need for two-way communication and interactivity more clearly by defining the requirements for the CBRNE assessment, for the assessment of all available information to first responders, for obtaining regular updates from first responders and for the assessment of resource requirements. The requirement IM C23 also defines the need for providing health surveillance, which can refer to physical health inspections or possibly also to technically supported interactive communication with people whose state of health needs to be followed.

In experiments SE1 and SE2, interactive notifications are given with the smartphone system by the police to the police officers inside the police organization and to private citizens outside the police force. Interactive features and functions are defined in the notification system in advance, and with that the recipients are able to reply quickly and in a standard form to the given question. Interactive questions, given linked with the emergency notifications, are used within the police organization, for example, inquiries about the alerted police officer's availability for coming to duty during that particular emergency. Accordingly, when the interactive questions are given together with an emergency warning to the public, the questions are, for example, inquiries of whether the people are well or if they need help. In experiment SE4, interactive warnings are given within a rescue rehearsal of a chemical accident with the fire and rescue service when the building is evacuated because of a toxic cloud. During the rehearsal, two persons respond to the interactive warning and evacuation message that they need help. The two persons are stuck in the building and are not able to come out through the toxic cloud. One of the persons is rescued when the rescue service is checking all rooms, and the other is located and rescued on the basis of the response to the interactive warning and evacuation message.

TABLE 17 Capability requirements and experiments related to question SQ4

SQ4: Can mass alerts, warnings and command and control notifications be given interactively with smartphone technology?
Related capability requirements:
• IM M1: Warning troops endangered by CBRN hazard in near real time • IM M7: Providing CBRN situational awareness applicable at strategic, operational and tactical levels • IM M11: Providing the means to manage the CBRN defence resources • IM M12: CBRNe advice and assessment including CBRNe intelligence • IM M15: Provide CBRN-related technical and scientific reachback • IM C2: Gather, assess and disseminate all available information to first responders • IM C4: Provide and obtain regular updates to and from first responders • IM C6: Provide situation report to emergency control rooms etc. and request assistance if necessary • IM C8: Provide timely warnings and advice to the public (immediate vicinity and beyond as necessary) • IM C9: Notify appropriate authorities at local, regional and national levels (governmental and responder agencies) • IM C10: Notify specialists (chemical, biological, radiological/nuclear, medical) • IM C19: Assess resource requirements (short, medium and long term) • IM C21: Provide information to hospitals • IM C23: Provide health surveillance (short–medium term) • IM C26: Provide timely warnings or advice to public
Related experiments:
SE1: Smartphone-based alerting, command and control of the special forces of the police SE2: Smartphone-based public warning of civilians by the police SE4: Integrated sensor-based alerting with a smartphone and fire alarm

The capability requirements in Table 17 indicate that research question SQ4 in regard to the interactivity of alerts, warnings and command and control notifications is relevant and valid for CBRNE countermeasures and defence. The results of experiments SE1, SE2 and SE4 also show that alerts, warnings and command and control notifications can be given interactively with smartphone technology. With these results, a positive result is confirmed for research question SQ4.

The research question

SQ5: Can situational awareness and a common operating picture be supported or created with smartphone technology?

discusses the capability of and need for producing situational awareness during a CBRNE incident. In Table 18, the capability requirements IM M7, IM C3 and IM

C6 represent examples of requirements in which specifically the provision and creation of situational awareness, an overview or a situation report is needed. The examples speak to situational awareness in general and do not specify any particular aspect of the emergency upon which the overview or report should be created. Evidently, however, there are several different issues and aspects that need to be followed during a CBRNE emergency, and the changing of the CBRNE threat per se is only one of them. Along with the source of contamination defined by the capability requirement IM M4, different aspects to be followed are, for example, the situation of the troops/first responders/rescuers, CBRN defense resources, public, hospitals and, in the long run, also the rescuers' and other involved people's health, referred to by the military capability requirements IM M1 and M11 and by the civilian requirements IM C4, C8, C19, C21 and C23. The discussed requirements do not specifically define the need for the creation of situation reports on these issues, but it is obvious that situational information on these

TABLE 18 Capability requirements and experiments related to question SQ5

SQ5: Can situational awareness and a common operating picture be supported or created with smartphone technology?
Related capability requirements:
• IM M1: Warning troops endangered by CBRN hazard in near real time • IM M4: Determining the source of contamination • IM M7: Providing CBRN situational awareness applicable at strategic, operational and tactical levels • IM M11: Providing the means to manage the CBRN defence resources • IM C3: Establish an overview of the affected area • IM C4: Provide and obtain regular updates to and from first responders • IM C6: Provide situation report to emergency control rooms etc. and request assistance if necessary • IM C8: Provide timely warnings and advice to the public (immediate vicinity and beyond as necessary) • IM C19: Assess resource requirements (short, medium and long term) • IM C21: Provide information to hospitals • IM C23: Provide health surveillance (short–medium term)
Related experiments:
SE1: Smartphone-based alerting, command and control of the special forces of the police SE2: Smartphone-based public warning of civilians by the police SE4: Integrated sensor-based alerting with a smartphone and fire alarm

issues is needed and that for having that information, data need to be accessed from these sources with appropriate means. Such data can, for example, be obtained with the interactive features of smartphone technology, as is demonstrated earlier in research question SQ4.

In the examples, situational awareness can be created on the basis of information and data accessed from the people or from the devices that the people use. Data can also be retrieved from stand-alone devices, which are not operated by people all the time. In Table 18, for example, the capability requirement IM M4 for determining the source of contamination refers to a situation where the source of contamination can be defined and monitored in addition to other detector devices also with unattended stand-alone sensors. These can also be commanded and controlled through smartphone technology, and a real-time situation picture can be created on the basis of that information.

In experiments SE1 and SE2, situational awareness and the operating picture are created with smartphone technology by the police of the different aspects of the operation of the police and of the situation of the public. In these experiments, situational awareness is created on the basis of information received from the people as a response to interactive emergency notifications and on the basis of data received automatically from the people's personal smartphone devices. In experiment SE4, data are also received from a chemical sensor.

To conclude, the capability requirements in Table 18, especially the military requirement IM M7 and the civilian requirements IM C3 and C6, prove that research question SQ5 regarding situational awareness is relevant and valid for CBRNE countermeasures and defence. In addition, experiments SE1, SE2 and SE3 confirm that situational awareness and an operating picture can be created with smartphone technology. Together these results also confirm a positive result for research question SQ5.

The research question

SQ6: **Can the course of the operation be recorded and traced with smartphone technology?**

addresses the question of tracing and recording the operation during a CBRNE incident. In Table 19, particularly the capability requirement IM M11 and civilian requirements IM C4 and IM C 29 define situations in CBRNE countermeasures and defence, where information about the operation is required from troops and first responders for managing the resources, for reporting on the operation or for participating in the debriefing after the operation. Such information can be given by the involved persons by memory and by possible notes made during the operation. Also, other manually or automatically recorded information can be used if available.

The other capability requirements in Table 19 define tasks such as notifying the authorities and providing information to hospitals. These counterparts are not directly operating in the on-site mission, but their actions are still relevant and possibly critical for the execution of the operation. For the debriefing and further analysis of the operation, it is therefore important that such counterparts' operation is recorded in addition to operative forces.

In experiment SE1, various alerts, warnings and command and control notifications are given with a smartphone to a test group of police officers within a police organization. All transactions are recorded automatically by the system for each officer and for the command of the operation both on the individual officers' phones and on the server of the software system. In the debriefing after the operation, all officers are able to trace the course of the operation from their own point of view from the log on their phones, and additional information is available for the management of the operation is also on the server. This information indicates, for example, the exact times of giving notifications, commands

TABLE 19 Capability requirements and experiments related to question SQ6

SQ6: **Can the course of the operation be recorded and traced with smartphone technology?**
Related capability requirements:
• IM M1: Warning troops endangered by CBRN hazard in near real time • IM M8: Providing CBRN-related decision support to commanders and staff at each level of command • IM M11: Providing the means to manage the CBRN defence resources • IM M22: Warning & reporting • IM M23: Warning messages • IM C4: Provide and obtain regular updates to and from first responders • IM C6: Provide situation report to emergency control rooms etc. and request assistance if necessary • IM C9: Notify appropriate authorities at local, regional and national levels (governmental and responder agencies) • IM C19: Assess resource requirements (short, medium and long term) • IM C21: Provide information to hospitals • IM C29: Provide multi-agency debriefings for all responders (i)
Related experiments:
SE1: Smartphone-based alerting, command and control of the special forces of the police

and alerts and the times when they reach each person's device. In addition, the data indicate the times when the notifications are noticed and responded to as well as the response times for all notifications and commands by each officer. The data also tell if some of the officers are not reached at all, in which case that information is shown on the situation map by the command of the operation.

According to the discussed capability requirements, research question SQ5 is relevant and valid for CBRNE countermeasures and defence. Based on the results of experiment SE1, it is also possible to record and trace the course of the operation with smartphone technology. With this information, the overall result for research question SQ6 is positive.

The research question

SQ7: Can mass alerts, warnings and command and control functions be integrated with other technologies and systems, such as detectors/sensors and digital maps, with smartphone technology?

examines the capability of and need for integrating the alerting, warning and command system with other devices, such as sensors and digital maps. Table 20 presents some examples of capability requirements related to this question. Military requirements IM M1-5, M12 and M13 as well as civilian requirements IM C1, C2, C17 and C18 define the specifications for recognizing the signs of a CBRN incident, warning troops, CBRNE assessment and determining the source of contamination, distinguishing between an instantaneous and continuous hazard release and making an estimate of the CBRN hazard area as well as for hazard prediction and dispersion modeling. All these activities can be done only if there is available adequate information and/or data about the CBRNE hazard. These kinds of data can be produced with various CBRNE detectors and sensors, which may be operated in many forms. Unattended stand-alone sensors are usually mounted in fixed locations for monitoring critical targets, whereas others are used manually or remotely by humans or by autonomous mobile systems.

TABLE 20 Capability requirements and experiments related to question SQ7

SQ7: Can mass alerts, warnings and command and control functions be integrated with other technologies and systems, such as detectors/sensors and digital maps, with smartphone technology?
Related capability requirements:
• IM M1: Warning troops endangered by CBRN hazard in near real time • IM M2: Making a rough estimate of CBRN hazard area in near real time • IM M4: Determining the source of contamination • IM M5: Distinguishing between an instantaneous hazard release and a continuous hazard release • IM M12: CBRNe advice and assessment including CBRNe intelligence • IM M13: CBRNe warning, reporting and CBRNe reachback
• IM C1: Recognize that a CBRN incident has or may occur • IM C2: Gather, assess and disseminate all available information to first responders • IM C17: Hazard prediction • IM C18: Dispersion modeling
• DIM M3: Operating in built-up areas
Related experiments:
SE3: Smartphone-based alerting and warning within civilian organizations
SE4: Integrated sensor-based alerting with a smartphone and fire alarm

These are used, for example, in cases where an airborne platform is carrying out a pre-programmed task with a CBRNE sensor as a payload on it. The CBRNE detection data can be retrieved from the sensor and delivered for further use with various methods, for example, with smartphone technology.

In Table 20, the capability requirement DIM M3 for operating in built-up areas defines that the CBRNE countermeasures and defence should be capable of operating in built-up areas, possibly also inside the buildings. This entails that there be maps available in the operation management's use of the affected area and/or buildings. These are even more urgent if there are endangered rescuers, casualties, hostages and/or intruders in the building or in other specified areas. When, in addition, the maps are in a digital form, they may be integrated with other systems to facilitate the defence and rescue operation. For example, devices equipped with smartphone technology can be located with the digital maps even without visual contact, and the rest of the rescue operation can be planned on the basis of that information.

In experiment SE3, rehearsals are organized for various scenarios of school violence. The experiment is organized in an old labyrinthine school building, where more than 500 students, teachers and other staff work on a daily basis. In the rehearsals, many different warnings and notifications are given to the teachers and other personnel with the smartphone system. In the experiment, a digital map and mobile emergency call buttons are also integrated with the smartphone system. Due to the digital map of the building, it is possible to locate precisely the origin of the emergency and to give further warnings and notifications accordingly. In experiment SE4, a rescue rehearsal is organized for a chemical accident at the department of chemistry, and a chemical alarm is integrated with the smartphone system. When the toxic chemical is released, the alarm gives an immediate signal to the smartphone system, and focused warning and evacuation commands are given in the area.

Referring to the included capability requirements, such as DIM M3 for operating in built-up areas, it is evident that various sensors and maps are necessary for the CBRNE countermeasures and defence. Evidently it is also useful or essential to integrate them with the alerting, warning and command and control systems. Research question SQ7 is therefore relevant and valid for CBRNE countermeasures and defence. In addition, on grounds of the empirical test results in experiments SE3 and SE4, chemical detectors/sensors and digital maps can be integrated with smartphone-based alerting, warning and command and control systems. Referring to all this information, the result for research question SQ7 is positive.

The research question

SQ8: Can long-term health monitoring and other crisis follow-up be conducted with smartphone technology?

discusses the health monitoring and follow-up of rescuers and other involved people during and after the emergency. Examples of related capability require-

ments and experiments for the question are presented in Table 21. Particularly capability requirements IM C23 for providing health surveillance, IM C28 for providing health advice to the public, IM C30 for providing psychological counseling for victims and responders and IM C31 for providing long-term health monitoring (victims and responders) in the civilian countermeasures operating concept define that health surveillance and other follow-up are needed as a part of CBRNE countermeasures and defence. Health surveillance is typically carried out after the emergency, but it can also be started before the emergency is over. Health surveillance and counseling can be given to the victims and responders. When necessary, it can be carried out for years after the crisis. The other requirements in Table 21 define activities that possibly utilize the information that is received from the health monitoring and crisis follow-up. Such activities are, for example, the military capability requirement IM M9 for providing guidance for the planning and execution of CBRN defence in all phases of operations at each level of command and the civilian requirements IM C3 for establishing an overview of the affected area and IM C14 for establishing the effect on the population.

Health monitoring types of activities are tested in experiments SE4 and SE5. In experiment SE4, a rescue rehearsal is organized with the fire and rescue service for a chemical accident at the department of chemistry, and people are evacuated out of the building. Warnings and requests to be evacuated out of the building are given to the employees with a smartphone. Within these notifications, people are asked if they are all right or if they need help. After a while, they are also asked if they need crisis support, and advice for getting such support is given with the message. During the evacuation, there are two persons who need help, and after the situation, no one needs crisis support.

TABLE 21 Capability requirements and experiments related to question SQ8

SQ8: Can long-term health monitoring and other crisis follow-up be conducted with smartphone technology?
Related capability requirements:
• IM M7: Providing CBRN situational awareness applicable at strategic, operational and tactical levels
• IM M9: Providing guidance for planning and execution of CBRN defence in all phases of operations at each level of command
• IM C3: Establish an overview of the affected area
• IM C14: Establish effect on population
• IM C23: Provide health surveillance (short–medium term)
• IM C28: Provide health advice to public
• IM C30: Provide psychological counseling for victims and responders
• IM C31: Provide long-term health monitoring (victims and responders)
Related experiments:
SE4: Integrated sensor-based alerting with a smartphone and fire alarm
SE5: Hyperspectral threat assessment and smartphone-based public warning in an explosion threat situation

In experiment SE5, a tabletop rehearsal is carried out in connection with a real-life explosion threat situation and evacuation of approximately 2,000 people. The emergency lasted almost three days. According to the tabletop rehearsal, during the emergency it is evident that the evacuated people needed a lot of information about the course of the events and about their own situation, including the possibility of returning back home, family members, livestock, medication and property. In the evacuation center, people were taken care of physically, and they were also provided discussion and mental support by the Red Cross and the local church. They did however not get enough practical information about the course of events and about the length of the evacuation and the like, which made them worried. The tabletop rehearsal shows that it would have been possible to support the people easily and conveniently with the smartphone system right from the beginning of the emergency and by carrying out the support during the whole incident as well as after it as long as the help would have been needed.

The discussed capability requirements show clearly that research question SQ8 is relevant and valid for CBRNE countermeasures and defence. Experiments SE4 and SE5 also indicate that health monitoring and crisis follow-up can be done with smartphone technology. This should, however, not be left to only after the emergency, as support may be needed at the time when the CBRNE incident is still going on. The results confirm a positive result for research question SQ8.

3.2.3 Hyperspectral technology and smartphone technology in CBRNE countermeasures and defence

Above sections 3.2.1 and 3.2.2 present the evaluation and testing results for the sub-questions of the main research question of the study:

Can hyperspectral technology and smartphone technology be used for CBRNE countermeasures and defence?

A summary of these results is presented for the detection of CBRNE threats with hyperspectral technology below in Table 22 and for the usage of smartphone technology in the information management of a CBRNE incident in Table 23. As can be noted in Table 22, all sub-questions for the usability of hyperspectral technology in the detection of CBRNE threats are supported both by the military and civilian capability requirements for CBRNE countermeasures and defence, which are taken from the CBRNE countermeasure operating concepts of the EDA (EDA, 2014), NATO (Lefebvre, 2015), the Canadian Armed Forces (CF, 2012) and NATO's guidelines for civilian CBRNE protection (NATO, 2008). All sub-questions for the usability of hyperspectral technology in the detection of CBRNE threats are also supported by the empirical experiments carried out as a part of this study for the forensic investigation and detection of CBRNE materials. These are conducted particularly with explosives, CWAs, TICs and other forensic details with the Central Finland Police Department, the

National Bureau of Investigation, the Finnish Defence Forces, Verifin and the explosives manufacturer Forcit Ltd. As a conclusion of these results, *the usability of hyperspectral technology in CBRNE countermeasures and defence is confirmed for using the technology in indoor and outdoor conditions and at all stages of the timeline of a CBRNE incident*.

It can also be seen in Table 23 that all sub-questions for smartphone technology's usability in the information management of a CBRNE incident are supported both by the military and civilian capability requirements for CBRNE countermeasures and defence, which are taken from the operating concepts for CBRNE countermeasures of the EDA (EDA, 2014), NATO (Lefebvre, 2015), the Canadian Armed Forces (CF, 2012) and NATO's guidelines for civilian CBRNE protection (NATO, 2008). All sub-questions for smartphone technology's usability are also supported by the empirical experiments carried out as a part of this study for testing smartphone-based alerting, command and control of operative forces and related authorities, public warning of civilians and alerting and warning within civilian organizations as well alerting that is integrated with various sensors. These experiments are carried out with the Central Finland Police Department in Jyväskylä; the Police Board and the Police Departments of Helsinki, Espoo, Tampere, Joensuu, Kuopio, Vaasa and Oulu; the Rescue Department of Central Finland and Kilpinen School of the City of Jyväskylä as well as with the Department of Chemistry and the Communications unit of the University of Jyväskylä. Also, a tabletop rehearsal is organized for smartphone technology's potential role during a real-life explosion threat situation and the evacuation of approximately 2,000 people. As a conclusion, these capability requirements and the results of the experiments *confirm the usability of smartphone technology for CBRNE countermeasures and defence for 1) carrying out mass alerts, warnings and command and control; 2) adjusting the intensity of alerting; 3) focusing and scaling geographically and according to different recipient groups mass alerts, warnings, command and control and other notifications; 4) giving mass alerts, warnings and command and control notifications interactively; 5) creating situational awareness and a common operating picture; 6) recording and tracing the course of the operation and 7) integrating mass alerts, warnings and command and control functions with detectors/sensors and digital maps as well as 8) carrying out long-term health monitoring and other crisis follow-up with smartphone technology.*

With these results for the sub-questions for the two discussed technologies, *the overall research question of the study for the usability of hyperspectral technology and smartphone technology for CBRNE countermeasures and defence is confirmed concerning the usability of hyperspectral technology for the detection, identification and monitoring of CBRNE threats and the usability of smartphone technology for the information management of a CBRNE incident*.

TABLE 22 Summary of the results for the detection, identification and monitoring of CBRNE threats

Main research question: **Can hyperspectral technology and smartphone technology be used for CBRNE countermeasures and defence?** **Sub-questions for CBRNE detection:**			
RESEARCH QUESTIONS	**RELATED CAPABILITY REQUIREMENTS**	**EXPERIMENTS**	**RESULT**
HQ1. Can CBRNE substances be detected with hyperspectral technology in indoor conditions?	DIM M4, DIM M7 DIM C1, DIM C2, DIM C3, DIM C4, DIM C5, DIM C26	HE1, HE2	SUPPORTED
HQ2. Can CBRNE substances be detected with hyperspectral technology in outdoor field conditions?	DIM M1, DIM M3, DIM M4, DIM M7, DIM M8 DIM C1, DIM C2, DIM C3, DIM C4, DIM C5	HE1, HE2, HE3	SUPPORTED
HQ3. Can hyperspectral detection technology be utilized at the different stages of the timeline of a CBRNE incident?	DIM M1, DIM M4, DIM M7, DIM M8 DIM C1, DIM C10, DIM C15, DIM C16, DIM C25, DIM C26	HE1, HE2, HE3, HE4, HE5	SUPPORTED

TABLE 23 Summary of the results for the information management of a CBRNE incident

Sub-questions for the information management of a CBRNE incident:			
RESEARCH QUESTIONS	**RELATED CAPABILITY REQUIREMENTS**	**EXPERIMENTS**	**RESULT**
SQ1: Can mass alerts, warnings and command and control activities be issued with smartphone technology?	IM M1, IM M13, IM M22, IM M23 IM C4, IM C6, IM C8, IM C9, IM C10, IM C21	SE1, SE2	SUPPORTED
SQ2: Can the intensity of alerting be adjusted with smartphone technology?	IM M1, IM M12, IM M13, IM M22, IM M23 IM C4, IM C6, IM C8, IM C9, IM C10, IM C21, IM C26	SE1, SE2	SUPPORTED
SQ3: Can mass alerts, warnings, command and control and other notifications be focused and scaled geographically and according to different recipient groups with smartphone technology?	IM M1, IM M7, IM M12, IM M15 IM C4, IM C8, IM C9, IM C10, IM C19, IM C21	SE1, SE2	SUPPORTED
SQ4: Can mass alerts, warnings and command and control functions be carried out interactively with smartphone technology?	IM M1, IM M7, IM M11, IM M12, IM M15 IM C2, IM C4, IM C6, IM C8, IM C9, IM C10, IM C19, IM C21, IM C23, IM C26	SE1, SE2, SE4	SUPPORTED
SQ5: Can situational awareness and a common operating picture be supported or created with smartphone technology?	IM M1, IM M4, IM M7, IM M11 IM C3, IM C4, IM C6, IM C8, IM C19, IM C21, IM C23	SE1, SE2, SE4	SUPPORTED
SQ6: Can the course of the operation be recorded and traced with smartphone technology?	IM M1, IM M8, IM M11, IM M22, IM M23 IM C4, IM C6,IM C9, IM C19, IM C21, IM C29	SE1	SUPPORTED
SQ7: Can mass alerts, warnings and command and control functions be integrated with other technologies and systems such as detectors, sensors and digital maps with smartphone technology?	IM M1, IM M2, IM M4, IM M5, IM M12, IM M13 IM C1, IM C2, IM C17, IM C18 DIM M3	SE3, SE4	SUPPORTED
SQ8: Can long-term health monitoring and other crisis follow-up be conducted with smartphone technology?	IM M7, IM M9 IM C3, IM C14, IM C23, IM C28, IM C30, IM C31	SE4, SE5	SUPPORTED

4 DISCUSSION AND CONCLUSION

4.1 The overall contribution and impact of the study

The overall contribution and impact of the present study is created by developing, in separate research and development projects, a new hyperspectral detection method and a new smartphone-based alerting and warning method by experimenting and testing these methods empirically in various research designs for crime scene investigation and the detection of CBRNE threats with the police, defence forces and fire and rescue service. After this, the usability of the two technologies and the newly developed detection and alerting methods are explored by evaluating via the experiment results whether hyperspectral technology and smartphone technology can fulfill the capability requirements of the generic forms of NATO's, the EDA's and the Canadian Armed Force's operating concepts for CBRNE countermeasures and defence. The examined operating concepts include both military and civilian operating procedures.

The evaluation of the research questions through the experiments conducted with the police, defence forces and fire and rescue service shows that all related capability requirements in the discussed operating concepts can be carried out or supported with hyperspectral technology and with smartphone technology. These technologies are currently not being used by the authorities in CBRNE countermeasures and defence in such a form, volume or at all, as discussed in the study, and the utilization of the research results in practice would possibly bring improvement to the current methods. During the evaluation it also became apparent that the experiments reveal other functionalities that are not mentioned in the described CBRNE countermeasures and defence operating concepts but that would still be useful in carrying out those tasks. Such capabilities are related to both the immediate management of an actualized CBRNE incident and with the long-term measures in countering CBRNE threats, especially in the authorities' interactions with civilian organizations and the civilian population.

According to the study, the two technologies are usable (where applicable) 1) for the authorities' internal use, 2) for joint operations between authorities, 3) for the authorities' operations with the civilian organizations and 4) for the authorities' operations with the civilian population. They can also be used for improving safety within and by civilian organizations, although in this study the discussion is focused primarily on the authorities' perspective of using these technologies.

These technologies are available, with some limitations, for the authorities' use as COTS products. Regarding the smartphones, the technology and technical requirements are available in several commercial brands. All smartphones, however, need additional software to perform the referred capability requirements. Such a system has been commercialized as a result of this study and is commercially available on the market. There are also various commercially available hyperspectral technologies in different brands, which are in principle capable of detecting the tested substances and targets. However, to carry out all the discussed CBRNE detection tasks outside the laboratory in the changing field environment, one needs several different hyperspectral devices in different wavelengths, sizes and weights operated with several different manned and unmanned operating platforms. Not all of these may be directly available on the market, and particularly the availability of small lightweight devices is limited. Moreover, appropriate software for all of these technical solutions may not be directly available.

As mentioned, as a result of this study, the smartphone-based alerting software has been commercialized and is available on the market and a hyperspectral analysis software has been commercialized for industrial purposes. In addition, after the study the research and development on hyperspectral CBRNE detection is being carried on in a four-year-long project of eight countries, coordinated by the UK and with the funding of the European Commission from 2015 to 2019.

In the following sections 4.1.1–4.1.5, the contribution and impact of the study are presented in a greater detail according to contribution, which is the result of the following:

1) the research topic and research methods;
2) the concept design and technological development work on the hyperspectral detection and investigation method and on the smartphone-based alerting, warning and situational awareness method;
3) the experiments and empirical testing of the developed hyperspectral and smartphone-based methods in CBRNE-related research designs with the police, defense forces and fire and rescue service and with other civilian organizations and the civilian population;
4) a comparison of the experiences and knowledge produced via the technology development and empirical testing with the capability requirements of

the authority-based CBRNE countermeasures and defence operating concepts and by the

5) dissemination of the research results by 1) commercializing the results of the technical development work on hyperspectral and smartphone-based detection, alerting and warning methods within two private enterprises, 2) publishing numerous articles internationally and by giving presentations in scientific forums, professional conferences and public media as well as by being awarded four years of funding, 11,9 million euros, for further work on the hyperspectral detection of CBRNE threats as a part of a UK-led CBRNE countermeasures development project of eight European countries, funded by the European Commission, from 2015 to 2019.

4.1.1 The specialty and essence of the applied research methods

First, the research topic of exploring and testing the usability of two novel information technologies in CBRNE countermeasures is highly relevant and important in current times, as terrorism is spreading, becoming more radical and taking new forms even in the most democratic and peaceful areas of Europe. There are also ever-present many other kinds of CBRNE risks that require improvement in CBRNE countermeasures and in the development of new CBRNE detection methods all over the world. These risks are related particularly to industrial accidents and transportation on the roads, railways and in the sea and air as well as to natural disasters and extremities of weather, which trigger catastrophes such as the nuclear disaster in Fukushima in 2011.

In the information technology field, hyperspectral technology as such is not a particularly new commercial technology, and the embedded software products have already been on the market for some 20 years. However, in recent years there has been a fast-growing interest and demand, especially in the areas of forensics, homeland security and defense, for small imaging devices and rapid field investigation methods, which appear to be promising and also very challenging in terms of production with hyperspectral technology. The key problem is how to produce very small, efficient and preferably multi-purpose hyperspectral imaging devices at a low cost. The devices should be capable of simultaneously detecting relevant CBRNE targets in varying environmental conditions, both indoors and outdoors and of being operable with many different operating platforms. These include manually operated devices and various unmanned platforms in ground-based, airborne and other forms. In addition, it is also challenging to develop appropriate software and analysis methods for the required detection technologies and tasks. One reason for this is that the field environments are in general “messy” and uncontrolled, whereas the creation of accurate and high-quality measuring results through optical methods optimally requires standardized and controlled measuring conditions. Additional challenges in the CBRNE detection and forensics are that they deal with illicit and prohibited substances and are carried out in extremely dangerous and

toxic environments, which creates even more stringent technical requirements for the hyperspectral devices.

This kind of research topic is also challenging because it is mostly focused in regulated military research institutes, designated research laboratories and commercial enterprises producing specialized protection and defence technologies. Research input on this kind of topic from the open university sector is therefore relatively rare and difficult to obtain. It may still bring fresh and new insights into the research field if the study has access to the needed materials and can thus be carried out successfully. For these reasons, one valuable contribution of this research is in the specialized study of and experiments with the close-range hyperspectral detection and investigation of CBRNE incidents, for which there has previously lacked sufficient and cost-effective detection and investigation methods on the market.

Thus far, a hyperspectral detection method also appears to have been missing from the authorities' field investigation guides for CBRNE, such as that of the OPCW. This indicates in part that the new information produced by this research and the associated experiments may help in evaluating whether this technology should be added into the field operations toolboxes of CBRNE specialists.

Moreover, smartphone technology, which is the other developed and tested information technology investigated in this research, is relatively new and underexplored technology in the CBRNE field. The development of the tested smartphone-based alerting and warning system was started at the University of Jyväskylä in another practical research and development project in 2009. At that time, touchscreen technology had not yet made its global breakthrough, as Apple introduced its iPhone only in 2007 and as the very first commercial touchscreen phone with the Android platform was established by HTC in October 2008, just before the beginning of the development of the smartphone-based alerting system in Jyväskylä in 2009. The University of Jyväskylä's mobile system, originally built on an HTC device, is therefore possibly the first smartphone-based alerting and warning system in the world running on the Android operating platform, and particularly on HTC, and the very first touchscreen type of mobile phone ever operating with the Android platform. The University of Jyväskylä's mobile system is now available on other platforms as well, but it is possible that in 2009 there were no other similar systems in the world built on Android or iOS platforms, which were the only commercial touchscreen-based operating platforms at that time.

In this study, smartphone technology emerges as emergency and crisis management technologies, which are applicable on a daily basis also outside the CBRNE field for many other kinds of small- and large-scale emergencies. The same technology can also be used in the management of broad- scale catastrophes and disasters all over the world, even if there are no CBRNE elements involved.

In addition to the research topic, the research approach is also ambitious, as it aims at contributing in two fields, in the information technology and secu-

rity sectors at the same time, and at producing new knowledge at the intersection of the two fields. The research framework is therefore constructed of two research lines, those of the CBRNE threat and information technology, and the whole research and discussion in the study is built upon merging these two very different research fields.

Due to the two research fields, the research methods are also varied, with an attempt to exploit the research methodologies applicable and representative in each field. At the main level of the work, the study discusses issues that are common to the two fields, and the main research question of the usability of hyperspectral and smartphone technology in CBRNE countermeasures deals with the same concepts. At this level, however, it is not easy to find any particular research method that is typical in both fields, as both disciplines are very broad and constructed of several other fields of science. The study also deals with two separate types of information technologies, which are usually studied with different research methods. This complicates the selection of the main research method of the study.

For these reasons the CD&E method from the military research sector was chosen as the primary research method at the top level of the study. It is used widely in the international military sector for developing and experimenting with future technologies to achieve the required capabilities needed in the security field. And, as has been discussed in earlier chapters, it suits the pondering over and examination of the main research question of the study perfectly. In addition to CD&E, many other research methods are used in the study that specifically fit research on the hyperspectral and smartphone technology. The value of the research methods thereby results from all these methods.

4.1.2 The contribution of the technological development work

The main contribution of the technological concept design and development work is created through the following three technology development projects funded by Tekes and the University of Jyväskylä:

- *Crime Scene Investigation by Spectral Imaging, SpeCSI* (2011–2012),
- *Hyperspectral Solutions for Crime Scene Investigation, SpeCSI Solutions* (2013–2014) and
- *Situational awareness through proactive risks and opportunities, Sapporo* (2011–2013).

Of these, the *Sapporo* project was not started from scratch, as the core of the software was originally created in the *Scientific innovation product concept, Scope* project (2009–2011), from which it was developed further and tested in the *Sapporo* project.

The author participated in all four projects by working as a project manager and concept, test and commercialization designer in the *SpeCSI Solutions* and *Sapporo* projects and as a concept and commercialization designer in the

SpeCSI project. In the preceding *Scope* project, the author's work was focused on planning and funding for the further development of the smartphone system.

The technological contribution of the hyperspectral technology development projects *SpeCSI* and *SpeCSI Solutions* is formed by the concept development and the creation of a specialized hyperspectral analysis software and analysis algorithms for hyperspectral imaging devices dedicated to the analysis of various crime scene investigation samples in different research designs. The software was created on the basis of particular use cases, which were designed and tested in the experiment parts of the projects. The created software is capable of, for example,

- the detection (in regard to recognizing and finding) of various dedicated and unknown forensic samples that are visible or invisible to the human eye,
- distinguishing various dedicated and unknown samples and the
- identification of dedicated samples.

The analysis software is also capable of detecting applicable substances in a pure form as well as those absorbed in selected matrices. For example, explosives can be detected with the software in their pre- and post-blast form as pure substances and in particulate form as explosives' residues. With the software, detailed analysis can also be performed on biological samples, such as blood, where the analysis result is based on the separate components of blood.

The software is designed to be independent from any manufacturer or brand, and it is expected to be compatible and integrable with many kinds of hyperspectral cameras. The detection tasks discussed in this study can, however, be carried out with the software only via dedicated hyperspectral cameras, depending on the target and environmental conditions. If an inappropriate camera is used, the software cannot give a reliable detection result, either.

The technological contribution of the smartphone technology project *Sapporo* is the result of the concept design and the creation of the server-end and mobile-end software for the mobile alerting, warning, C2, situational awareness, log and tracing system. The first version of the software core was created in an earlier project, *Scope,* in 2009–2011, and in the *Sapporo* project in 2011–2013 the software was in some aspects reproduced and developed further. The system was created on the first commercial version of the Android operating platform with which it was capable of also having access to other kinds of mobile phones and other smart devices, such as tablet computers. With all its features it was at that time technically ahead of its time. Touchscreen smartphone devices were brought to the market just shortly before, and all the newest technical features of the touchscreen technology, together with the push notification feature and global positioning service, were embedded within the scalable and interactive mobile warning system.

The early technology selection at the University of Jyväskylä proved to be accurate, as the Android platform quickly started spreading globally by becom-

ing the world's leading touchscreen operating system for mobile phones in 2012. During the *Sapporo* project in 2011–2013, the warning system was developed further on the basis of the special needs of the authorities and civilians, which came up when the system was tested with the police and fire and rescue service and with civilian organizations, such as the public school and the department of chemistry at the university. Along with these experiments, for example, the command and control facilities of the system, application interface with other systems and integration with external sensors, digital maps and other alerting technologies were generated and improved. Also, a new emergency call button was created on the smartphone handsets to enable quick reaction time in a sudden emergency situation.

The research distinctly shows smartphone technology's superior performance in alerting and warning applications, which are not limited to the private citizens' or authorities' internal use only but rather apply to both. In this context the technology is also not limited to only direct alerting and warning functions, as the given notifications can also be interactive and thus enable many other useful functions. The technology can also utilize the global positioning service, be adjustable according to geographical location and be integrated with other technologies and systems, which all make it very usable and superior compared with all other alerting and warning technologies.

4.1.3 The contribution of the hyperspectral experiments and testing

Most of the practical contribution and a part of the technological and scientific contribution to hyperspectral technology were the result particularly of the *SpeCSI Solutions* project with the design and execution of hyperspectral technology experiments with the police, defence forces and fire and rescue service. The variety of these experiments is vast, taking into account all the tested use cases, environments, technical devices, substances and matrices. The experiments give empirical information specifically on

- which kinds of forensic and CBRNE samples can be found, distinguished and identified and
- in which forms,
- in which kinds of environments,
- in which kinds of circumstances,
- on which kinds of matrices,
- with which kinds of hyperspectral cameras and
- with which kinds of operating platforms.

The experiments were carried out with seven different hyperspectral imaging devices of VIS, VNIR/NIR, SWIR, MWIR and LWIR types, with wavelengths varying between 450 and 12,000 nm. Some of the experiments were carried out as laboratory tests indoors and some as field experiments outdoors. In some of the experiments, such as those involving explosions, tests were carried

out in the defence force's specialized testing field outdoors, after which samples were collected and analyzed with the hyperspectral cameras and analysis software indoors. During the experiments on the airborne hyperspectral detection of explosives and blood, the tests were carried out as an authentic field experiment outdoors by imaging prepared samples on the ground with a hyperspectral camera mounted on a drone. The specialized technological, practical and scientific knowledge resulting from these experiments includes empirical knowledge specifically on

- carrying out forensic crime scene investigation with hyperspectral cameras, specializing in biological samples, drugs, the use of firearms, the use of tear gas, fires and other forensic details;
- detecting military and civilian explosives and explosives' residues with hyperspectral cameras and
- detecting TICs and CWAs with hyperspectral cameras as well as
- carrying out hyperspectral imaging in different environments and in varying weather conditions with different hyperspectral cameras and operating platforms, such as imaging with fixed cameras in the laboratory, working in arctic winter conditions outdoors and imaging prepared samples with a hyperspectral camera outdoors with a drone in dry summer weather.

A great part of the value of these experiments is based on their novelty, as hyperspectral technology is not yet applied very widely in the on-site inspection of crime scenes, especially in the on-site detection and investigation of CBRNE sites. The long distance hyperspectral remote sensing of, for example, gas, the transportation of armament, camouflaged warehouses and illicit production facilities of prohibited materials is, however, used quite widely internationally, but the hyperspectral precision analysis of crime scenes and CBRNE sites is not well developed yet. One of the main reasons for this is that small, efficient, flexible and cost-effective hyperspectral technologies capable of precise detection and the rapid analysis of forensic and CBRNE details in the field environment are missing. As the usage of hyperspectral technology is also dependent on environmental conditions, and as the regulated authority and CBRNE sectors are a very challenging market for private enterprises, most commercial technology developers would rather provide new innovations for the industrial sector on the open market than invest in the development of new products with strict requirements by the regulating authorities. In this study, however, most of the research and development interest is paid to the hyperspectral close-range precision detection and investigation of crime scenes and CBRNE sites, which also led to a large part of the scientific and practical contribution of the study.

A great deal of the value of the experiments is also created by the exceptional opportunity of being able to use genuine forensic and CBRNE samples provided by specific authorities, research laboratories and private companies. Without these partners, the most relevant parts of the study would not have

been possible due to the restricted access to and usage of such materials by unauthorized persons. The special materials and distinct organizations that enabled the production of the scientific and practical results with genuine samples of restricted materials include

- forensic samples, such as blood and other biological marks, gunshot materials, tear gas and drugs provided by the Central Finland Police Department, the National Bureau of Investigation and the Oulu Police Department;
- samples of fires, arsons and environmental crimes provided by the Rescue Department of Central Finland;
- explosion tests and other experiments with explosives carried out with the technical and material support of the Central Finland Police Department, the Finnish Defence Forces/Finnish Air Force and Oy Forcit Ab and
- samples of TICs and CWAs tested with the technical and material support of the Finnish Institute for Verification of the Chemical Weapons Convention Verifin.

In addition, the services of several technology providers were used to produce the research results for hyperspectral technology. These are for the hyperspectral cameras Specim Ltd. (most of the imaging devices), VTT and Rikola and for the unmanned airborne vehicles/drones VideoDrone Finland Ltd.

4.1.4 The contribution of the smartphone experiments and testing

The experimental and further scientific contribution of the smartphone system results from the experiments carried out during the *Sapporo* project in 2011–2013. The technological capabilities and the overall mobile crisis management knowledge produced via the practical experiments with the smartphone system together with the police, fire and rescue service, civilian organizations and civilian population are valuable and valid for managing almost any kind of crises, not only CBRNE incidents. The experiments show that there is a great need for mobile warning and mobile crisis management systems in today's society. The authorities, organizations and private citizens who enabled the practical experiments with real-life end-users have therefore contributed a great deal to the creation of future mobile security systems.

The project was originally planned to experiment and gain knowledge on the government issuance of nationwide, localized and scalable public warnings on people's personal mobile phones. The overall need for mobile public warnings was evident, as the current procedures of giving public warnings through the national radio and television broadcasting network were, in general, considered inflexible and in part also a nuisance by people unaffected by the emergency. With the national broadcasting system, all public warnings were given to the whole country, even if the emergency was local and the rest of the population had no need to be warned about it. From the workflow point of view, the

communication process of giving local warnings was also many staged and bureaucratic, causing delays in the warning process. The whole warning process was, for example, divided into two or more parts of the country, and the original warning message needed to be typed manually into electronic systems twice during the same warning process. It also needed to be brought manually between two floors to be read to the public on air in the broadcasting studio.

The research was also planned to study alternative maintenance models for the warning systems to minimize the costs of the public service. The experimentation with issuing government-based public warnings on mobile phones and the idea of financing public warning systems with government funding other than budget-based was, however, not supported by the two responsible ministries, so the empirical knowledge was created in the study by testing the smartphone system with

- the Central Finland Police Department, Police Board and eight police departments around the country;
- the Central Finland Police Department and a testing group of private citizens in the City of Jyväskylä and beyond;
- the City of Jyväskylä and Kilpinen school;
- the Department of Mathematical Information Technology, Communications Unit and Department of Chemistry of the University of Jyväskylä and the Rescue Department of Central Finland
- and with a tabletop experiment utilizing the smartphone system in public warning, crisis communication and crisis management during the explosion threat situation in the Vihtavuori explosives plant in July 2013.

The rejection of the originally planned national experimentations in the two ministries showed why it is so complicated to take into use a new public warning method on mobile phones as well as why it takes such a long time, for example, in the country of Finland. The same issues hold up taking into use other security and safety technologies and systems as well, including hyperspectral technology, and it is important to pay attention to the roadblocks in the public sector. In all, this issue is a broader question in the entire field of the innovation, development and funding of new technologies for the security sector and in commercializing and taking into use such innovations, especially by the security authorities in the public sector. In addition, selling security products within the international market is much more complicated and difficult than marketing products to the open industrial and consumer market. Evidently, for this reason, a large part of innovation and development capacity is also directed to fields other than security and safety. The common procedures of operating on the security products market may also foster the concentration of the security product suppliers as well as the high and, in some cases, overpriced security products.

At the end of 2011, the rejection of testing and taking into use a scalable public warning system on mobile phones as a part of the national warning system was reasoned in the ministries according to cost, equal service for people and the national policy of giving public warnings through the national radio and television broadcasting network only. Additionally, the price of other commercial systems not based on smartphone technology was considered too expensive. Still, even though the implementation and usage of the smartphone system was expected to be much cheaper, and the development and testing costs of the smartphone system were covered by the university project, this did not make a difference in the ministries. People in the ministries also referred to the democratic system of the country, which entails that all people should be served equally by public services. Concerning the proposed public warning on mobile phones, they then concluded that as "all people" cannot afford to buy mobile phones, it is technically not possible to give public warnings to "all people" with mobile phones. In addition, as all people cannot afford to buy mobile phones, public mobile warnings should not be given to those people who do have mobile phones, either. For comparison, however, the coverage of the national radio and television broadcasting network is technically not 100% of the area of the country, and not all people have an access to television broadcasts. Also, part of the population does not watch or accept the existence of the television device because of religious reasons. Moreover, in general, television and radio receivers are not any cheaper than mobile phones, and nowadays especially younger generations choose not to watch television or listen to the radio. Instead, most of them have access to mobile devices 24 hours per day.

As the university had already received government funding for the project from Tekes, and also as the software core had already been produced in the earlier project, the project was continued by excluding the experimentation and testing of national first priority public warnings by government authorities from the project. The two ministries were not expected to change their stance until the end of the project by the end of 2013, so the university was not able to wait for a more favorable time to accomplish that part of the project, especially due to its responsibilities toward the main financier, Tekes. The technical and user experiments were then structured as organization-based tests instead of testing how the government would give public warnings on private citizens' mobile phones to warn the whole population, certain parts of the country, immigrants and other temporary residents, tourists, visitors or other suddenly endangered groups of people by various threats.

The organization-based testing and experimenting program was then organized with the Central Finland Police Department; a large public school in the City of Jyväskylä; the department of chemistry at the university and a big department store, shopping mall and hotels and restaurants of a large commercial enterprise. After a while, however, of these the commercial enterprise reconsidered their decision and withdrew from the project, pointing out that they have a loudspeaker system in their department stores and other business premises and thus do not see digital warnings on mobile phones and on electronic

bulletin boards necessary in their buildings. They also noted that in hotels and restaurants, the personnel are responsible for the customers' safety and that direct warnings on customers' mobile phones are therefore not needed. One may still ask whether the loudspeakers are a sufficient alerting, warning and emergency management system in public buildings such as shopping malls, hotels and restaurants. Nevertheless, that kind of emergency scenario and testing was not carried out with a commercial enterprise, despite having it in the project plan, tentatively signed by a private company.

During the project it became clear that many other organizations are also highly sensitive about their security issues and would like to hide the whole topic from the public. Even if certain technology would improve the organizations' safety, the decision makers fear that the implementation of such systems might ruin their public image and reputation by implying that they have a security problem. According to various experiences during the project, public schools and cities, for example, do not want to tell the public details about how many, what kind of or whether at all they have security problems or if they have implemented some security technologies in their schools or cities.

After revising the project plan, the first empirical experimentations with the real end-users of the mobile alerting and warning system were begun with the Central Finland Police Department in November 2012 with the kind support of chief police officer Markku Luoma. The experiment was at first designed to be carried out as a rehearsal for the local police to give public warnings to private citizens in various locations in the area of Central Finland. Discussions with the police, however, led to new ideas regarding user needs, and the experiment was extended to cover basically the whole country of Finland, according to police officer Tuomo Korhonen's suggestion and support by the Police Board. It was also decided that before sending any messages with the system from the police to the civilian population, the operation and technical functions of the system would be tested inside the police organization. The testing was organized as a nationwide experiment, with participants from the Police Board, the communication preparedness group and special forces from eight different police departments around the country. This experiment produced extremely valuable contributions, as it tested not only the technical functionalities of the system but also showed the potential of and requirements for the use of the system as an alerting, command and control system inside authority organizations and also between authority and other organizations.

Even though most authorities already have their own standardized command and control systems, according to this experiment, the smartphone system can possibly be used for supporting and complementing other systems inside and between the authority organizations. The smartphone system can also be used as an efficient and affordable command and control system inside civilian aid organizations and for supporting joint operations between security authorities and civilian aid organizations. In Finland, widely and regularly used examples of such kinds of joint operations can be found especially in volunteer fire brigades in association with municipal fire and rescue service and the vol-

unteer rescue service offered by the Red Cross, which is often asked for help in supporting the work of the fire and rescue service and police. The system may also be helpful in organizing and commanding conscripts during their military service, as they are often asked for help, for example, in searching for people who are lost, fighting forest and ground fires and in cordoning areas in emergencies and large public events.

After testing the system within the internal organization of the police, a new experiment was arranged to give public warnings and create situational awareness with the system about the situation of private citizens by the police. Both the internal and external experiments with the police were the first of their kind in Finland, and they were also lauded in international evaluations, where the experiments were reported in scientific conferences and articles. As in the experiment with private citizens the police were for the first time capable of giving public warnings and delivering other information on the private citizens' personal mobile phones, and as the police were also able to localize and scale such communication to any geographical location with any measurable range, the tests produced extremely valuable information in regard to how the authorities' emergency communication should be issued to citizens' personal mobile devices in the first place as well as how the localized and scaled emergency messaging should be arranged.

The experiments and experience of working with the police were also useful for the preparation of the two experiments with civilian organizations, which were carried out shortly after the experiments with the police. These civilian organizations were the Kilpinen school, which is one of the biggest public schools in the City of Jyväskylä, and the Department of Chemistry of the University of Jyväskylä. In carrying out the experiment at the Department of Chemistry, the Rescue Department of Central Finland and the Communications Unit and the Department of Mathematical Information Technology of the University of Jyväskylä were also involved.

From a technical point of view, the two experiments with the civilian organizations demonstrated how a mobile alerting and warning system can be integrated as well as what kind of use there is in integrating the system with various automatic detectors and sensors, human-operated e-call devices and the digital ground plans of buildings. The experiments also gave indications as to how well public buildings in general are (or at the time of carrying out the experiments were) technically prepared for the implementation of digitalized security systems. At the time of designing these experiments, there was, for example, a very weak mobile phone signal inside the 500-student school due to the windows, architecture and wall structures of the old building. There were also some other heavy elements inside the school that formed a black spot for a mobile phone network in some critical locations inside the building. In addition, there was no digital ground plan of the building available, and it was created together with other technical improvements before starting the experiment. At the department of chemistry, the main technical problem was that at the time of

carrying out the project there was only a fire alarm device in the experiment area, and fire alarm devices cannot detect or warn of chemical accidents.

From a digital content perspective, the experiments also showed that even if the rescue plans of public buildings are reviewed regularly, they may still contain some unpractical content or may not completely fit with the changed threat scenarios of today. It is also very difficult to transform and import current manual rescue plans into a digital format, especially to be used as a quick emergency guide in the mobile emergency system of the building. If, however, mobile warning systems become official (in areas where they are not yet used as a part of official warning systems), there may also be a need for creating public guidelines for municipalities and building owners to provide the rescue plans of public buildings in a digital format, quickly assessable by mobile warning systems.

For the purpose of CBRNE protection and safety, the technical findings during these experiments in public buildings with civilian organizations also point to the need for implementing the right kinds of CBRNE detectors in all places where there is a possible risk for an accidental CBRNE release. In critical locations, such as international airports, government buildings and the like, certain types of CBRNE detectors integrated with mobile alarm systems are also needed in cases of other-than-accidental releases of CBRNE materials.

From an operational point of view, the experiments with civilian organizations showed that there certainly is a need for mobile warning systems in large organizations and buildings and that smartphone-based systems are more useful and flexible than others. The experiments also showed that many issues need to be discussed and decided upon before a mobile alerting and warning system can be taken into use in an organization. For example, does the employer provide all personnel with mobile phones, and are people willing or obligated to use their own phones for emergency communication at work? Or, are people allowed to carry their phone at work? This may be limited, for example, at schools and in dangerous working environments in certain industrial fields. Special arrangements are also needed in places where there are many children or many people with disabilities at the same time. For example, in school alerts issued with the organization's own mobile system can be directed to the personnel of the school only, and also silent alerts can be given to avoid unnecessary anxiety among the children. If, however, public alerts are given from outside of the school, there is the possibility that children will receive alerts on their personal devices during their day at school. As such systems are not currently in use, for example, in Finland, there is no policy on how mobile warnings should be given by the security authorities or inside organizations such as schools in relation to the children or their parents. Due to the rich technological features of smartphones, these kinds of issues can, however, be managed technically, as long as the emergency communication rules for children are agreed upon first.

The experiments with the civilian organizations also show that concerning mobile warning systems inside private and public organizations, there is cur-

rently no implementation guide or operation procedure available for integrating such systems with authorities' operating procedures and emergency management systems. In Finland, the basic procedure for organizations with emergencies is 1) to call 112, 2) perform, depending on the type of threat, the immediate necessary first aid, rescue, protection and/or evacuation tasks and 3) let the rescue service and police do everything else. If, however, mobile warning and situational awareness systems are taken into use in private or public organizations, the line between organizations' own and authorities' systems should be clarified. During the experiments, the operation between the organization's own emergency management system, the public emergency center's system and the rescue authority's system was unclear. The problem came up especially during the rescue rehearsal of the chemical accident, when the emergency alerts and instructions inside the building were given with the organization's own system, and simultaneously there were in use at least two different authorities' systems, which did not communicate with each other. In this case, the information about the status and location of the people in the building was in the organization's own mobile system and issued by the crisis management personnel of the building, but there was no technical means of transferring that information to the authorities. Also, a position or person designated by the authority to whom that information should be delivered was missing. In addition, unless coordinated, the authority could have in principle used a similar mobile warning and situational awareness system within the same emergency area and building, in which case there might have been confusion between the authority's system and emergency organization's own system. However, these are not technical problems of the mobile system per se but rather issues that need to be discussed and agreed upon before implementing such systems. There is also a chance that if private and public organizations have their own mobile warning systems, authorities can in principle utilize them in their own emergency communications and vice versa. In addition, if civilian aid organizations have mobile warning systems, they can basically be integrated with the authorities' emergency management and command and control systems for supporting joint operations in selected emergencies. Such situations are, for example CBRNE incidents.

The last experiment with the smartphone system during the *Sapporo* project was the tabletop rehearsal of utilizing the system in public warning, crisis communication and crisis management during the explosion threat situation in the Vihtavuori explosives plant in July 2013. The experiment demonstrated with a real-life threat situation, step by step, how the system could have been used for localized warning and evacuation to provide support right from the beginning of the emergency and as a prolonged crisis management system for the people during their evacuation. The system would also have offered a reliable and direct information and discussion channel between the evacuated people and authorities during the whole three-day-long emergency, which would have helped people to cope better with the situation and recovery after it ended. In the real situation, they received practically no information from the authorities

about the course of the emergency or the state of the homes and property, cattle and pets inside the emergency zone. It also became clear that the system would have been needed as an alert, information and command and control system between the authorities and volunteer rescue service of the Red Cross as well as in the use of the local organization of the Red Cross when volunteers were needed for help in organizing the evacuation.

4.1.5 The contribution of the comparison of the empirical experiments with the capability requirements of CBRNE countermeasures and defence

The comprehensive contribution of the study is created by comparing the experiences and knowledge produced through the technology development and empirical testing with the capability requirements defined in the operating concepts for the CBRNE countermeasures and defence as well as by evaluating in that way the overall usability of hyperspectral technology and smartphone technology in CBRNE countermeasures and defence. This knowledge is useful for authorities who participate in CBRNE countermeasures and defence at the strategic and operative levels. Such authorities are particularly the defence forces, fire and rescue service and police. The knowledge is also useful for the border guard and customs, because CBRNE materials are transported illegally across borders.

The comparison of the experiments with the CBRNE countermeasure operating concepts within the study also indicates the stages in the timeline of CBRNE incidents, in which the two technologies can be used and for what purpose. On grounds of the experiments and requirements of the operating concepts, the overall usability of both hyperspectral technology and smartphone technology is broad and covers the whole timeline of CBRNE incidents.

The study also discusses the requirements of the CBRNE countermeasure operating concepts from the military and civilian protection points of view. The analysis indicates that the military operating concepts do not provide much information about the immediate rescue of civilians or about joint operations with civilian organizations and civilian people as a part of CBRNE defence. Based on the experiments, the study suggests how the authorities' joint operations with the civilian organizations can be supported and also how the civilian population can be better protected with smartphone technology.

Much of the information and knowledge produced via this study is new in this context, and the implementation of this knowledge is expected to improve the efficiency of joint operations between the different authorities and between authorities and civilian organizations. Improved joint operations should at the same time increase the overall resources in the management of a crisis.

4.1.6 The importance and impact of the dissemination of the research results

Many of the research results of this study, both about hyperspectral technology and smartphone technology, have been published in international forums since 2012. The publications are scientific and practical articles and presentations

published in scientific forums, in professional conferences and seminars and in public media in Finland and other countries abroad. The publications have generated scientific, professional and public discussion particularly about the usage and potential of hyperspectral technology in crime scene investigation and counter-terrorism and about the role and technical forms of public warnings. Discussion on the forms of public warnings has been especially intense in Finland.

Other scientific, practical and societal impacts of the study can be measured, for example, as the knowledge exchange between the researchers and as the participation in many significant international conferences, exhibitions, excursions and other meetings in the key areas of CBRNE and other security fields during the research and writing process of this thesis. These include, among others, the Spie Defence and Security conferences in the US; the European Forensic Expo and Counter Terror Expo in the UK; a visit to DSTL, Porton Down, UK; research cooperation with Verifin that operates in Finland in cooperation with the international laboratory network of the OPCW; a visit to the CBRNE research facilities in the Tsech Republic, Swedish Defence Research Agency (FOI) and the European CBRNE Center in Sweden; the European Academy of Forensic Science Conference (EAFS) in The Netherlands; visits to the International Criminal Court and Europol in The Hague, Netherlands; a forensic science conference in Australia; the disaster and crisis management conferences of the Global Risk Forum in Switzerland; conferences on information warfare and crisis response and management systems in Germany and Finland; the European conference on critical communications in The Netherlands; conferences of the International Society of Military Sciences (ISMS) in Finland and Poland; international symposiums on CBRNE threats (NBC Symposium) in Finland, as well as a conference on technological innovations in emergency and crisis management as a part of Latvia's international meetings during their presidency of the European Union in 2015.

The research has also produced and contributed to nine to ten academic degrees, of which four are doctoral theses and the others candidate and master's theses. Two of the doctoral theses are produced solely and two others partially on the basis of the discussed research.

Both the hyperspectral analysis software and the smartphone-based public warning system have also been commercialized in two private companies during the research and thesis process. The smartphone-based warning system was commercialized first in 2013 and the hyperspectral software after that in 2015. After the commercialization, the smartphone system was at first implemented in a trial use in the Sochi Winter Olympics in Russia in 2014. Since then its commercial utilization has been growing, for example, by its use in the fire and rescue services and in private companies. In 2016 it is also being integrated with the Tetra networks, as was proposed in the University of Jyväskylä's presentation in the meeting of Critical Communications Europe in Amsterdam in 2014.

The commercial utilization of the hyperspectral solution is proceeding more slowly as it was commercialized two years later than the smartphone ap-

plication. During this time, more technical working effort has also been spent on the development of the smartphone system, which means that at the commercialization stage, the smartphone system has been technically more mature than the hyperspectral system. The hyperspectral research has, however, received remarkable recognition as the scientific and empirical knowledge that has been created in the hyperspectral research projects as a part of this study is being utilized in a European Commission funded CBRNE countermeasures research and development project from 2015 to 2019. In 2015 the project was awarded with a funding amount of 11.9 million euros by the Horizon 2020 program of the European Commission, and the hyperspectral research forms one part of the multi-technology and multinational project. The project is led by the UK, and the consortium consists of 19 partner organizations from eight different European countries. The author's participation in this European Commission funded project and becoming a part of the broad international network of research and development partners would not have been possible without the research that has been carried out as part of this thesis.

4.2 The validity and reliability of the research

4.2.1 The validity of the study

The validity of the present study is formed by the relevance of the research topic, problem and questions the information technology's applicability in the security field and practice of CBRNE protection and by the research approach and methods, through which the research problems are studied. This study represents cross-border research between the information technology and security sciences, and therefore the validity needs to be evaluated from both these two research fields' perspectives.

On the security sciences' side, there is currently a strong interest internationally in CBRNE issues, which indicates that the research theme is relevant and current. Currently CBRNE risks, threats and provocation occur quite often in various parts of the world, so there also is a need to improve CBRNE protection and, when possible, create new CBRNE protection methods. Strong demand exists especially for efficient and economic protection methods that indicate the risk immediately and are able to warn people efficiently and quickly at a low cost.

In the information technology field, both hyperspectral technology and smartphone technology are novel techniques at the moment. They are both still gaining great research interest, even though the main principles of hyperspectral technology and earlier generation mobile technology before the current smartphones were originally invented more than 20 years ago. The hyperspectral technology field is currently rapidly producing new innovations, technological solutions and applications all the time, and, for example, the European Union has defined photonics, of which hyperspectral technology is a part, as one

of the fastest growing key enabling technologies (KET) in Europe from 2014 to 2020. KET technologies are expected to spread rapidly into all areas of society and to create new growth faster than any other technologies. Also, the usage and applications of the new form of smartphone technology have been increasing rapidly since the introduction of the first commercial touchscreen platforms by Apple in 2007 (iOS) and HTC in 2008 (Android). Most smartphone applications are evidently created for the consumer sector, but as smartphone technology is very advanced, usable and affordable for all and has the potential for performing many useful tasks, it is reasonable to also utilize them in the security sector, such as in CBRNE protection, as is discussed in this study. The same also applies for hyperspectral technology, for which many new application areas have been found in recent years and which is also potentially feasible in the security sector, including in CBRNE protection.

The validity of the study is also results from the validity of the selected research approach and research methods. First, the study's bilateral nature is built by covering both the information technology and security sciences fields. This approach provides more content to the study and brings more challenge for the validity. If instead the research would have been focused solely on information technological issues, it would have been possible to build the two systems as ordinary information systems development work in the office and to test their technical abilities with technical tests in the laboratory. That would, however, lead to only the technical information of the systems without any practical information from the user environment in the field, where the systems are designed to be used. Technical tests in the laboratory are, however, the first step in this kind of systems design and testing, and it is the researcher's choice as to whether the technical tests of the study are focused only on laboratory tests or if field experiments are also included in the study.

However, there are also other reasons in the information technology field for why it is reasonable to proceed quickly into empirical testing in the system's development process instead of carrying out thorough systems development work and moving on to user experiments in the field only after first carrying out heavy and costly technical development work. In general, iterative systems designed with agile software development are often preferred to avoid unnecessary development work on features that are not needed or wanted by the users or that do not support carrying out the technical tasks required in the real user environments of the system. For example, it would have been possible in this study to first develop a technically brilliant hyperspectral detection system that operates perfectly with dummy materials in the office but not with real-world CBRNE threats, which cannot self-evidently be tested by average information technology faculties in civilian universities. It would also have been possible to build any kind of smartphone system on the basis of the programmers' ideas only, but there is a great risk that much of the time, work and money will be wasted if the system does not meet the end-user requirements and other conditions of the real user environment. In this case, both systems are directed to be used in life-threatening emergency situations by authorities and

civilians, so it is even more important to assess the user needs and environmental requirements as early as possible in the systems design process.

For the reasons above, the chosen research strategy to first identify the user needs for the hyperspectral field detection method and smartphone-based public warning method and then proceed through agile systems development work and laboratory tests into empirical field tests with end-users from the security field is an appropriate and valid method for conducting this research. Building up and testing information technology systems per se is, however, not academic research unless there are broader or more detailed research questions, which are studied with these information technology systems development processes. This study contains such research questions, which are then studied with the information technology systems development processes.

In the study, the whole research process initially started from first identifying the novelty and potential of smartphone technology and hyperspectral technology per se and also from realizing the new technological solutions' need in the security field, including the possibilities that the two technologies could offer for improving the public safety. At the same time, there have also been expectations by the financier of the practical projects that the developed systems should be commercialized to creating new businesses. In addition, the researcher's personal interest in and devotion to the research field has been a driving force for pushing the research forward. Owing to this, the individual research and development projects have not remained only practical information technology projects but have been included as a part of a wider and more holistic academic and practical research.

The academic research, scientific writing and publishing were therefore first carried out within the practical projects, conducted with smartphone technology in the disaster and crisis management field and with hyperspectral technology in the crime scene investigation and counter-terrorism field, including the detection of CBRNE substances. As the two research processes were managed and carried out by the same person, logical interconnections between the two research and development processes started coming up during the work. However, it was originally clear that both projects would be carried out in the security sector, but that alone does not directly indicate that the two processes would have something more in common, as they deal with two completely different technologies. The one is about smartphone technology and telecommunications and the other about optical detection and the chemical analysis of substances, which have in a technological sense practically nothing in common. However, when in the smartphone project a possible need emerged for integrating the smartphone-based alerting and warning system with other devices such as the fire alarm and other sensors, it became obvious that there might be a chance to also integrate the hyperspectral devices with the same system. It was, however, not at first clear how and for what particular reason the two technologies should be integrated, as one project was at that time focusing on public warning and the other on real-time crime scene investigation. Later on, when the hyperspectral detection tests were performed with CBRNE sub-

stances, the interconnections between the technologies became stronger, because the CBRNE materials create a significant security risk, which in certain situations requires the issuance of public warnings. It was also realized that the two development processes were in fact dealing with the same broader issue, managing emergencies and crises, which also connected the two research processes, and the two seemingly different technologies, as a part of the same research framework and of the same research question.

Concerning the academic research process, the common research framework, research question and methodologies then needed to be refined further, and also the question of working together with several different authorities needed to be resolved. The research work and empirical experiments were begun in both projects and with both technologies by working from the beginning with the police but later on also the fire and rescue service and the defense forces. Police work and forensic investigation or crime scene investigation as an application area did therefore not cover the whole research field, and some other approach from the authorities' view was needed as a framework for the study. Joint operation between the security authorities, including the police, fire and rescue service and the defence forces, was an essential issue in this respect, but that alone did not offer a satisfactory framework for the whole study, either. However, when the research was viewed from the CBRNE threats and emergencies perspective, the authorities appeared to have particular written operating concepts for CBRNE countermeasures and defence. That was then chosen as a starting point for defining the common framework for the research and for the empirical experiments with the two technologies. The described operating concepts are usually written from one particular authority's viewpoint only, but when they are examined at a generic level, as in this study, the discussion can to some extent be generalized to apply for all, not, for example, for defence forces or police only.

After the common research framework was chosen and built up by starting from the generic CBRNE countermeasures and defence operating concepts, all empirical experiments conducted with the police, fire and rescue service and defence forces in separate projects were merged within the same study and under the same research question and approach. As a result, each experiment demonstrates on its own part how hyperspectral technology and smartphone technology can support the execution of CBRNE countermeasures and defence. In addition, the experience and knowledge produced by the study can basically be applied by all authorities, not only o

On the methodological side, the CD&E method is applied creatively as the empirical experiments were carried out first, with the holistic framework and common operating concept after that. The concept design, systems development, experimenting and testing have, however, followed an iterative process, and the iterative working method is an essential part of the CD&E method. The research and development process must, according to the CD&E method, start from identifying the research need or problem to be solved, and the process also needs to produce some kind of concept to be tested. Due to the iterative

working method – and also according to the agile systems development methods – there is, however, flexibility in the stage of the project in which the concept can be developed and at which stages it can be modified and updated. If the concept is sketched roughly and quickly at the beginning, light prototypes can be produced sooner, and with the help of the visualization created by the prototypes, the final concept can be improved and updated in the later stages of the project. It is also possible to apply the opposite working method, by first identifying a lot of environmental and user requirements and by creating with that information a very carefully planned concept to be built up with technical methods and to be tested with empirical methods later.

As can be noted, there is no exact procedure for how the discussed research and development process should be carried out, because each process is different and also the time and costs required for producing concepts and prototypes vary a great deal. In this study the research and development process began by first producing two different concepts for different problems in two separate projects. In both projects, the concepts were also tested separately with the police, defence forces, and the fire and rescue service. After the experimentations, the results of both projects were approved and moved forward by commercializing the software applications to take them into use in end-user organizations. At this stage, the research process was, however, not over as the CD&E processes were carried on and taken to a new level. A new and broader concept was created above the two earlier concepts, which were both more focused and based on one particular technology. The new model forms a wider operational plan for the hyperspectral and smartphone-based CBRNE countermeasures operation concept, which covers the knowledge and experiences from the earlier technologies and concepts and also new information produced at the upper level during the new stage of the research process. The new broader-level operating concept is more than just the earlier two concepts together, and it specializes particularly in CBRNE countermeasures and defence, which was not directly the primary focus of the two earlier projects. This concept also is tested with the same experiments as the earlier, more focused concepts, but at this stage testing is performed by retrospectively evaluating the newly created CBRNE countermeasures model through the experiments that had already been executed with the police, defence forces, and the fire and rescue service.

4.2.2 The reliability of the study

Reliability is usually evaluated for quantitative research. In this study, this method is not used much. A quantitative approach is used mainly in certain parts of the empirical experiments and hyperspectral analysis, which are reported in scientific articles that have been evaluated and published earlier as a part of this research.

In general, as hyperspectral measurements are done within the experiments of the study with qualified commercial hyperspectral imagers, the detection results are in principle reliable. The tested samples are either detected or not. As many of the experiments also are carried out in the laboratory as con-

trolled tests, this also improves the reliability of the results. In most experiments, same samples are also measured with many different hyperspectral cameras, and the measuring results of the different cameras are compared to confirm the results. Also, other kinds of methods are used for controlling and confirming the hyperspectral measuring and analysis results. For example, in the blood tests, the blood count is made for the same samples by health care professionals with their own standardized devices in another research institute. Accordingly, in the explosion experiments performed to test the detection of explosion residues, same samples were also measured with a high-quality spectrometer by another research unit in the department of chemistry to control and confirm the analysis results of the hyperspectral method.

In the study, some questionnaires and surveys are also used within the smartphone experiments, where the question of reliability is relevant. In the study, the size of the test groups is small, and the results of the questionnaires are not confirmed statistically. However, the experiments represent case studies, which, according to their nature, give mostly qualitative information about the studied issues. Such results can be generalized to wider populations only after further research.

The hyperspectral experiments and tests conducted in the study in the laboratory environment can be repeated. For the field experiments, however, it is difficult to produce identical weather conditions. Also, the smartphone experiments can be repeated for the technical parts. With the test groups of different people, each testing situation is nonetheless different, and each person will respond in the tests according to the situation.

4.2.3 Limitations and risks

As is demonstrated in the experiments above, hyperspectral and smartphone technologies have great technical potential to be used as a part of CBRNE countermeasures and defence. There are, however, also generic limitations and risks, which may affect the performance of these technologies in certain situations. For hyperspectral technology, for example the following features can be found:

1. The technology can distinguish various samples but identify only such substances whose reference is included or integrated in the detection system.
2. Not all substances can be detected or identified with the same wavelengths.
3. Detection is dependent on environmental conditions such as the illumination and in outdoor operation also on other weather conditions.
4. Detection is dependent on the measuring distance and optics as well as on the resolution of the hyperspectral camera.
5. Detection is dependent on the properties of the surfaces and matrices on which the detected substance is placed or in which it is absorbed.
6. Detection is dependent on the analysis software and algorithms.

7. Detection is dependent on the volume of the sample. However, no generic value for the minimum detectable volume, applicable for all substances, can be defined.
8. In principle, substances can be detected in a solid, liquid and gaseous phases. However, the detection of rapidly vaporizing and degrading substances may be challenging as they may change their physical form and turn into different substances during the measurement.
9. Measurement is possible in indoor and outdoor conditions, but the same airborne devices used for CBRNE detection at high altitudes may not be used for airborne detection inside the buildings.
10. In radiological and nuclear environments, the operation of electronic and mobile devices has a risk of failing.

For smartphone technology, the following limitations and risks may appear when the technology is being used for alerting, warning and other related purposes in crisis management:

1. There is an ongoing debate concerning the usability of COTS devices such as smartphone handsets as a part of authority-based security systems in contrast to dedicated tailor-made devices. In authorities' use only, tailored devices are often more expensive than COTS devices. However, in public warning and other emergency management, COTS technologies can be used as personal handsets for private citizens. For this reason, authorities' emergency management systems need to be adapted to work with a large variety of different brands, models and generations of mobile phones. In addition, authorities' systems need to be prepared to cope with market forces and fluctuations in the consumer market, which have an effect on the usage of different handsets by the public population.
2. Regarding the justification of giving public warnings on private citizens' personal mobile phones, there is also an ongoing discussion of the equality and democracy related to private citizens' ability to buy mobile phones. Irrespective of public policies and the equal service for people, in the end, individual persons make the choice as to whether or not they regard public warnings and warning systems.
3. In general, investments in public security systems are based on expectations of accidents and other crises, on costs of the new systems and on expected loss in cases of investing or not investing in the proposed system. The calculative gain of the system is created when an emerging threat can be turned down or mitigated. The studied smartphone system can, however, also be employed outside emergencies for other useful functions, which may create additional payback for the system.
4. Regional authorities can take into use mobile warning and emergency management systems. Public security procedures, processes and systems should,

however, be standardized, and new systems should be integrated with already existing systems. Public procurements also need to be tendered, which may lead to different systems in different regions, depending on the competition in the market.

5. In many areas, mobile communication infrastructures are built on a commercial basis, not according to the principles of public service or regional homogeneity. This may lead to an unbalanced network structure in different regions, which may also affect the availability and quality of service of mobile services in different areas.
6. In general, mobile networks with higher transmission capacity have a smaller service area and vice versa. For the current 2G, 3G and 4G networks, the service area has been decreased each time a newer generation technology has been taken into use. The quality of the service for mobile applications may change by taking into use different network technologies.
7. Complementary and back-up networks for mobile systems may be built, for example, with WLAN, p-to-p and satellite networks.
8. Mobile networks can become overloaded by too much traffic, which may affect the quality of service for mobile applications.
9. Telecommunication infrastructures are vulnerable to interruptions in the electricity supply, heavy storms and the destruction of cell towers. Failings in telecommunication infrastructures may also affect the operation of mobile systems.
10. CBRNE incidents, particularly radioactive and nuclear activity, can disturb the operation of electronic devices, including mobile phone handsets or the servers of mobile phone applications.
11. Cyber threats such as service denial attacks and hijacks can be directed to the servers, networks and handset devices of mobile services. Such attacks may affect also the operation of mobile warning systems.
12. The price of mobile data transfer varies in different countries. This may have an effect on people's willingness to use mobile services when they are abroad.

The vulnerability of mobile networks, international usage and the scalability of mobile emergency alerting systems as well as barriers to taking into use mobile emergency alerting and crisis management systems are discussed in the following articles and presentations, which are not included herein:

Jaana Kuula, Jonne Räsänen, Pauli Kettunen, Olli Kauppinen and Slava Panasenko. Mobile Emergency Messaging and the Vulnerability of Crisis Communication. *Proceedings of the 8th Symposium of CBRNE Threats, Turku, Finland, 11-14. June,* 2012.

Jaana Kuula, Markku Häkkinen and Jukka Jalasvuori. The Need for International Harmonization of Emergency Notification Systems: The Case of Finland. *Proceedings of the Global Risk Forum GRF, One Health Summit, Davos, Switzerland, 19-22. February,* 2012.

Jaana Kuula. Smartphone Based Multi-Channel Emergency Alerting. *Latvian Presidency of the Council of the European Union, Workshop on Civil Protection: Workshop on needs of persons with disability throughout disaster management cycle, Riga, Latvia, 12-13. January,* 2015.

4.3 Conclusions and recommendations for future work

4.3.1 Conclusions

The objective of this work was to study, whether the hyperspectral and smartphone technology can be used for CBRNE countermeasures and defence. This was examined with more detailed sub-questions that are compatible with the NATO's, EDA's and Canadian Armed Force's operating concepts and capability requirements for CBRNE countermeasures and defence. Sub-questions were also tested with empirical experiments that were carried out together with the police, defence forces and rescue service. Experiments were focused especially in the hyperspectral detection of explosives and explosive residues, CWAs, biofluids and forensic samples, and in the mobile alerting and warning, command and control and the creation of situational awareness during the whole timeline of a CBRNE incident.

The study shows, that the research questions are relevant for the capability requirements of the common military and civilian operating concepts for CBRNE countermeasures and defence, and that the hyperspectral and smartphone technology experiments support the research questions. This confirms, that there are several previously defined and approved user needs in the common operating concepts for CBRNE countermeasures and defence, that can potentially be fulfilled with hyperspectral and smartphone technology. However, for practical reasons the empirical experiments in the study are limited and especially the potential use area of the hyperspectral technology is in this context so challenging and wide, that each use case needs to be defined and tested more carefully before definite statements can be given of this technology's performance in mission critical CBRNE incidents. For example, one cannot suggest taking any of the commercial hyperspectral imaging devices and expecting that CWAs and TICs can be found with them in wherever environmental circumstances just like that. Instead, one must, for each agent or agent group separately, define and test in beforehand, what particular type of camera is potential to detect the wanted agent, and what kind of other peripherals, software and other necessities are needed for making the detection possible with that particular

device. In addition, one must be familiar with many other limitations and conditions, that define the practical requirements for the detection of that agent in unknown and uncontrolled field environments. It is therefore possible that, even if hyperspectral technology can find various agents in ideal conditions (which usually do not exist in everyday user environments), the detection will fail in real-world field conditions, where circumstances are unknown, uncontrolled and in many aspects different from the ideal measuring situation. In the identification of substances one can though utilize approximation, but in mission critical situations that may not be useful, as in those cases it is a question of life and death for plenty of people, and the threat should be identified as precisely as possible and as quickly as possible.

For improving the accuracy of the detection in time and mission critical, uncontrolled and "messy" environments in the field, one should, for example, try to develop detection technologies and mathematical and software based analyzing methods. One can also try to increase control in the detection situation and to standardize the measuring event. This may though lead into situation where the ideal competitive advantage of the hyperspectral detection needs to be compromised. For example, the target may need to be touched or treated, or one may need to take a physical sample. Hyperspectral method may however be competitive and useful even with these additional procedures, even if the primary idea of optical detection is to identify substances without touching or treating the target.

Compared with hyperspectral technology, the usage of smartphone technology is more widespread and common. Smartphone technology also is primarily a largely adopted consumer technology, and in addition to that a potential professional smart device. Even though this study demonstrates much of the potential of the smartphone technology in CBRNE emergencies' and other crises' use, it cannot be taken granted that it will be utilized systematically for the proposed purposes. Authorities can, for example be so committed to and stuck with their current technologies and systems, that the proposed tasks may not be designated to smartphones, even if the technology is applicable for that. It is also difficult to change authorities' emergency management and operation procedures, especially when changes should be applied to more than one regional operating areas or to different authorities' joint operation. Authorities may also be reluctant to increase or take in use digital connections with civilian aid organizations, that assist and carry out operative rescue and recovery work during the crisis, but do not hold an access to authorities' internal information and command and control systems. In the emergency management context, a critical question with the smartphone technology also is, whether the handset devices should be tailored for professional use only, or if ordinary consumer product type COTS devices can be used instead. Both options have their pros and cons, especially concerning the devices' security and overall costs.

There are also other issues that need to be noted, when private people's personal smartphones are utilized in emergency communication by authorities in a wide scale at a time. Direct instant messaging with masses of people re-

quires organizing and management in the first place, and if the communication requires additional work for designing the content, the whole process becomes more complicated. If, in addition, emergency communication is planned to be interactive, authorities need to be prepared for managing not only the giving of public warnings to the people, but also the other communication that possibly comes from the uncounted number of people to the authorities. The incoming communication also needs to be received and evaluated immediately, as some of the information may require instant operative actions, while at the same time some of it can be unnecessary or not urgent.

When direct emergency communication applications are built between the authorities and private people, there also is a chance, that people get overloaded by the authorities' messages, or by all digital messages that come constantly from various sources, among them from authorities. In this kind of situation critical emergency messages may not be noticed, or, if they do, some people may still ignore them. There also is a risk that authorities' direct communication channels and systems with masses of people become hijacked, which may have some serious consequences. Such systems are usually cyber secured, but all risks may not always be fully rejected. Authorities' direct communication systems with citizens are however better secured than average social media applications, that most people use in their everyday life. It is for example possible and common, that social media applications get filled up with unconfirmed and untrue information and even with deliberate hostile content that is created by trolls or other unwanted sources. This kind of things happen also during the most serious emergencies, and some of them can possibly be counted as information warfare. Authorities' encrypted and in other ways secured direct communication with citizens may therefore protect people in this kind of situations better than other communication that is built on ordinary social media. With these secured systems authorities can at first warn and inform people reliably for various threats, and also diminish the harm that is caused by disruptive information that is spread in other channels by trolls or other unwanted sources. As an example of recent events, this kind of disturbing troll attack with negative false information took place associated with the shooting event in Eastern Finland in Imatra in early December in 2016, and the false information needed to be corrected in public.

4.3.2 Recommendations for future work

Concerning the whole research area of the study, further research and discussion are needed on many topics. First, discussion is recommended about the coverage of current CBRNE countermeasure operating concepts and about the possible implications of taking into use new technologies. For example, the real operational potential of the suggested hyperspectral technology and smartphone technology needs to be evaluated through the already operationalized strategies and operating concepts for CBRNE countermeasures and defence. This, however, cannot be done through public research.

For hyperspectral technology, further research and development are needed on the CBRNE detection devices, operating platforms, software and analysis methods. Even though there are many commercial hyperspectral imaging and detecting devices on the market, user needs in CBRNE detection are varied and cannot be answered with any single hyperspectral device type only. The CBRNE user environment also sets additional requirements for the technological devices due to the toxic and in other ways dangerous working environment. Ideally, development is needed on such hyperspectral devices in different sizes, which are capable of performing many different CBRNE detection tasks and which are also resistant to various CBRNE environments.

For working in toxic and other dangerous environments, there also is always the question of which kinds of operating platforms should be used. Many CBRNE sites are too dangerous for humans to work there, even when wearing protective suits, and preferably automated devices are sent to the location instead. The requirements for such technical devices are many and possibly cannot be met with ordinary consumer electronics or other everyday technologies. The development of automated and remotely controlled special devices, however, is expensive, and operation in toxic environments may damage or destroy them as well. The usage of automated platform devices may in some cases also spread the contamination or destroy forensic evidence, and further research is needed to solve these problems.

Detection systems also require several kinds of other devices, software and analysis methods, which all need to fit together and operate extremely fast on CBRNE sites. The requirements, for example, for hyperspectral analysis are therefore different for mission critical use, such as CBRNE, compared with other civilian application areas. Unlike on CBRNE sites, in ordinary civilian targets hyperspectral measurements can be made in a safe and clean environment, and the measuring results can also be analyzed thoroughly in peace without immediate time pressures. Improvement is needed particularly in rapid detection in toxic environments and in rapid real-time analysis and wireless communication of detection results.

Concerning smartphone technology, or mobile technology in general, authorities are recommended to consider whether they are ready to extend mobile alerts and warnings outside their current inter-authority relations and systems. Especially authorities' mobile connections with various civilian organizations may need to be improved and increased. In addition, the implementation of similar systems for civilian organizations' internal use would possibly improve the efficiency of overall emergency management, including the management of CBRNE countermeasures and defence. It would also be useful to implement mobile warning and communication systems for private citizens' use, as has already been done in several countries.

Taking mobile alerting systems into use within or between organizations or with the public can be a broad multi-stage process involving many authorities, civilian partner organizations and civilians. The process can, however, be made easier by doing it in smaller steps. New operating procedures and warn-

ing methods can be first tested in smaller pilot areas, and experiences can be transferred to wider environments gradually, when the counterparts are satisfied with the usage.

It is also possible to conduct further academic research in the area of mobile emergency alerting, warning and management systems. For example, there are possibly needs to improve the encryption of the communication in some areas of this field and possibly to create new cybersecurity methods. Cyber protection needs are not limited to the usage of data processing and communication methods only, as they are also needed in the commanding and operation of various mobile, automated and remotely controlled devices. Such devices are particularly mobile phones and other communication devices, emergency detection devices, unmanned operating platforms and vehicles. Cyber protection is needed in these cases to ensure the secure operation of emergency systems in cases of malfunction caused by external disturbances or the hostile hijacking of critical systems and devices.

Emergency communication and management systems also need back-up systems, preferably with other technologies, such as satellite or peer-to-peer connections. Also, the data content, form of discussion and share of fixed and freeform messages as well as the criteria for giving public warnings are worth further research. However, as people's current digital environment is full of unreliable information, the key values of emergency communication are the quick delivery of true information, direct and clear instructions, people's trust in authorities and the ability take the required precautions when necessary. This kind of communication needs to be short and efficient, and citizens should have no doubt as to whether the information is coming from an authorized party or whether the information is true and urgent.

YHTEENVETO (FINNISH SUMMARY)

Hyperspektri- ja älypuhelinteknologian käytettävyys CBRNE-vastatoimissa ja -puolustuksessa

Kansainvälisistä kieltosopimuksista huolimatta joukkotuhoaseen ja luvanvaraisten CBRNE-aineiden käyttö ei ole maailmanlaajuisesti loppunut. Joukkotuhontaan soveltuvien aineiden teollinen, lääketieteellinen ja muu yhteiskunnan normaaliin toimintaan kuuluva käyttö on laajaa ja useilla valtioilla on myös varsinaisia joukkotuhoaseita. Teollisuuskäytössä CBRNE-aineista aiheutuu vakavia onnettomuuksia ja vaaratilanteita usein. Yleisimmin vaaratilanteita aiheuttavat inhimillisestä erehdyksestä, huolimattomuudesta, laiterikosta tai luonnonmullistuksista johtuvat kemikaali-, räjähdysaine- ja säteilyonnettomuudet kuljetuksen, varastoinnin tai valmistusprosessin aikana. Vakavimpia viimeaikaisia CBRNE-onnettomuuksia ovat olleet esimerkiksi maanjäristyksen ja tsunamin aiheuttama Fukushiman ydinvoimalaonnettomuus Japanissa vuonna 2011 ja väärällä tavalla sammutetusta räjähdysaineiden varastopalosta syntynyt räjähdys- ja myrkkykaasuonnettomuus Tianjinissa Kiinassa vuonna 2015. Laittomasti hankittuja teollisuus- ja puolustuskäyttöön tarkoitettuja aineita ja tarvikkeita käytetään myös tahallisesti vahingoittamaan ihmisiä ja aiheuttamaan aineellista tuhoa. Rauhan aikana varsinaisen sotilaallisen toiminnan ulkopuolella rikollisessa mielessä vahinkoa aiheuttavat yleensä yksittäiset häiriintyneet ihmiset, terroristit tai muut järjestäytyneet rikolliset.

Tässä työssä tavoitteena on löytää uusia teknologisia keinoja ja menetelmiä, joilla CBRNE-onnettomuuksia ja tuhotöitä voitaisiin estää ja joilla voitaisiin lisäksi vähentää CBRNE-tilanteiden aiheuttamia inhimillisiä ja materiaalisia vahinkoja. Tässä käyttötarkoituksessa työssä tutkitaan, kuinka kaksi modernia teknologiaa, hyperspektriteknologia ja älypuhelinteknologia, soveltuvat eri turvallisuusviranomaisten harjoittamien CBRNE-vastatoimien ja CBRNE-puolustuksen käyttöön. Näihin kuuluvat niin sanottuina detektointitoimenpiteinä muun muassa CBRNE-uhkien havaitsemiseksi tehtävä tiedustelu, havainnointi ja valvonta, monitorointi, aineiden läsnäolon ja pitoisuuksien mittaus, kontaminaation mittaus, dekontaminaation jälkeinen tarkastus sekä rikospaikka- ja forensinen tutkinta ja löydettyjen aineiden verifiointi. Vastatoimiin kuuluvia informaatiojohtamisen toimenpiteitä puolestaan ovat muun muassa viranomaistoiminnan sisällä suoritettavat operatiivisen toiminnan hälytykset ja komennot, viranomaisyhteistyössä tarvittava keskinäinen informointi ja muu yhteistoiminnan vaatima kommunikointi, CBRNE-uhkaan ja kriisinhallintaan liittyvä tiedonhankinta, tiedonsiirto, prosessointi ja kommunikointi, tilannekuvan luonti, väestön varoittaminen, päivitykset ja jälkihoito sekä yhteydenpito kriisialueella olevien uhrien ja altistuneiden henkilöiden kanssa. Tässä työssä tutkitaan, kuinka edellä mainittuja CBRNE-uhkiin liittyviä detektointitoimenpiteitä voidaan suorittaa hyperspektriteknologian avulla ja kuinka CBRNE-kriisin

hallintaan kuuluvia informaatiojohtamisen toimenpiteitä voitaisiin suorittaa älypuhelinteknologian avulla.

Tutkimus on suoritettu poimimalla aluksi Euroopan turvallisuusjärjestön EDA:n, Pohjois-Atlantin liiton NATO:n ja Kanadan puolustusvoimien yleisistä CBRNE-vastatoimi- ja puolustusmalleista yksittäiset detektointi- ja informaatiojohtamisen vaatimukset ja päättelemällä tämän jälkeen hyperspektri- ja älypuhelinteknologian teknisiin ja toiminallisiin ominaisuuksiin perustuen, mitkä näistä vaatimuksista mahdollisesti ovat toteutettavissa näiden kahden teknologian avulla. Löydetyt käyttötarkoitukset on lisäksi todennettu viranomaisten ja muiden erityisasiantuntijoiden kanssa hyperspektri- ja älypuhelinteknologian avulla suoritettujen empiiristen testausten avulla. Tärkeimmät testit ovat olleet poliisin kanssa suoritetut rikospaikkatutkimuksen kokeet, poliisin ja puolustusvoimien kanssa suoritetut räjäytyskokeet, poliisin ja Forcitin kanssa miehittämättömällä lennokilla ilmasta käsin suoritetut räjähdysaineiden havainnointikokeet, Verifinin kanssa suoritetut myrkyllisten teollisuuskemikaalien ja kemiallisten joukkotuhoaineiden havainnointikokeet, poliisin kanssa suoritetut valmiusryhmien hälytys- ja komentotoiminnan kokeet, poliisin ja siviilihenkilöistä koostuvan testiryhmän kanssa suoritetut väestönvaroituksen ja tilannekuvan muodostamisen kokeet, pelastuslaitoksen kanssa suoritettu kemikaalionnettomuuden pelastusharjoitus sekä Jyväskylän kaupungin ja Kilpisen koulun kanssa suoritetut koulualueen turvatoimia koskevat kokeet.

Tarkastellut CBRNE-vastatoimien ja puolustuksen viranomaismallit ja viranomaisten kanssa suoritetut käytännön kokeet osoittavat, että hyperspektri- ja älypuhelinteknologia soveltuvat hyvin laaja-alaisesti CBRNE-uhkien ja kriisien hallintaan ja hoitoon. Hyperspektriteknologia soveltuu erityisesti viranomaisten ja pelastustoimista vastaavien siviiliorganisaatioiden käyttöön ja älypuhelinteknologia näiden lisäksi myös yksityishenkilöiden ja koko väestön tai kohdennettujen väestönosien käyttöön.

Kumpikaan teknologia ei ole viranomaisilla tällä hetkellä riittävässä laajuudessa kriisinhallinnan ja väestönsuojelun käytössä. Hyperspektriteknologian osalta käyttöönoton edistämiseksi tarvitaan lisää teknologian ja menetelmien tutkimus- ja kehittämistyötä. Älypuhelinteknologia on kypsempää, mutta sitäkään ei nykyisellään hyödynnetä kriisinhallinnan käytössä siinä laajuudessa ja niillä tavoilla, jotka kyseinen teknologia mahdollistaa niin viranomaistoiminnan sisällä kuin viranomaisten ja siviiliorganisaatioiden sekä viranomaisten ja kansalaisten välillä.

REFERENCES

ACO, 2015. NATO Multinational Chemical, Biological, Radiological and Nuclear Defence Battalion. http://www.aco.nato.int/page136195217.aspx. Accessed: Nov 4, 2015.

Baum, S. 2015. Antinuclear Austria Should Lead the Way on Nuclear Power. Though constitutionally outlawed, atomic energy is ripe for development in the central European country. Guest Blog. Scientific American. http://blogs.scientificamerican.com/guest-blog/antinuclear-austria-should-lead-the-way-on-nuclear-power/. Accessed: Jan 14, 2014

BBC, 2015a. Madrid train attacks. http://news.bbc.co.uk/2/shared/spl/hi/guides/457000/457031/html/default.stm. Accessed: Nov 18, 2015.

BBC, 2015b. MH17 Malaysia plane crash: What we know. http://www.bbc.com/news/world-europe-28357880. Accessed: Nov 5, 2015.

BBC, 2015c. China explosions: What we know about what happened in Tianjin. http://www.bbc.com/news/world-asia-china-33844084. Accessed: Nov 5, 2015.

BBC 2015d. Islamic State 'using chlorine gas' in Iraq roadside bombs. http://www.bbc.com/news/world-middle-east-31847427. Accessed: Jan 2, 2016.

BBC 2015e. Alexander Litvinenko: Profile of murdered Russian spy. http://www.bbc.com/news/uk-19647226. Accessed: Jan 12, 2016.

BBC 2015f. Paris attacks: What happened on the night. http://www.bbc.com/news/world-europe-34818994. Accessed: June 6, 2016.

BBC 2016. Brussels explosions: What we know about airport and metro attacks. http://www.bbc.com/news/world-europe-35869985. Accessed: June 6, 2016.

Berenson 2015. Yasser Arafat Wasn't Poisoned, French Prosecutors Say. http://time.com/4021200/yasser-arafat-not-poisoned/. Accessed: Jan 12, 2016.

Bhopal, 2008. The Bhopal Memorial Hospital and Research Centre. Available in: http://www.bmhrc.org/Bhopal%20Gas%20Tragedy.htm. Accessed: Nov 5, 2015.

BIO 2016. Marie Curie Biography. http://www.biography.com/people/marie-curie-9263538. Accessed: Jan 12, 2016.

Boston marathon, 2015. Boston-marathon-bombings. http://www.history.com/topics/boston-marathon-bombings. Accessed: Nov 9, 2015.

Bennet, M. 2003. TICs, TIMs, and Terrorists. Commodity chemicals take on a sinister role as potential terrorist tools. Today's chemist at work. American Chemical Society. http://pubs.acs.org/subscribe/archive/tcaw/12/i04/pdf/403regulations.pdf. Accessed: Dec 10, 2015.

Borger, J. 2016. Nuclear weapons risk greater than in cold war, says ex-Pentagon chief. http://www.theguardian.com/world/2016/jan/07/nuclear-weapons-risk-greater-than-in-cold-war-says-ex-pentagon-chief. Accessed: Jan 13, 2016.

Bunn, G. 1969. Banning poison gas and germ warfare: Should United States agree? Wisconsin Law Review. Vol. 1969:375

BusinessDictionary 2015. Opt in. http://www.businessdictionary.com/definition/opt-in.html. Accessed: Nov 21, 2015.

CBRNeWORLD 2015. Global CBRNE threats and activity. CBRNe WORLD. August, 2015.

CBRNeWORLD 2016. Global CBRNE threats and activity. CBRNe WORLD. June, 2016.

Chang, C-I. 2003. Hyperspectral Imaging: Techniques for Spectral Detection and Classification. Kluwer Academic / Plenum Publishers. New York.

CDC 2012. Severe Acute Respiratory Syndrome (SARS). Centers for Disease Control and Prevention, U.S. Department of Health & Human Services. http://www.cdc.gov/sars/about/fs-sars.html. Accessed: Dec 14, 2015.

CDC 2015. Deaths and Mortality. Centers for Disease Control and Prevention. U.S. Department of Health & Human Services. http://www.cdc.gov/nchs/fastats/deaths.htm. Accessed: Jan 26, 2016.

Cellbroadcastforum 2009. What is cell broadcast. http://www.cellbroadcastforum.org/whatisCB/. Accessed: Nov 21, 2015.

CF 2012. Chemical, Biological, Radiological and Nuclear Defence Operating Concept. Chief of Force Development, Canada. NDID # A-FD-005-005/AF-003.

Charbonneau, L. & Nichols, M. 2013. U.N. confirms sarin used in Syria attack; U.S., UK, France blame Assad. http://www.reuters.com/article/2013/09/16/us-syria-crisis-un-idUSBRE98F0ED20130916. Accessed: Nov 9, 2015.

ChemImage 2016. http://www.chemimage.com/. Accessed: Feb 2, 2016.

Choi, D 2016. 'Unique, strange, and terrible' — ISIS may have created a new type of bomb. Business Insider Nordic. http://nordic.businessinsider.com/isis-created-a-new-type-of-bomb-2016-7. Accessed: July 30, 2016.

Chrisafis, A. and Sherwood, H. 2013. Yasser Arafat may have been poisoned with polonium, tests show. http://www.theguardian.com/world/2013/nov/06/yasser-arafat-poisoned-polonium-tests-scientists. Accessed: Jan 12, 2016.

CNN 2015. Hero rats sniff out landmines. CNN. http://edition.cnn.com/videos/intl_tv-shows/2015/07/17/hero-rats-sniff-out-landmines-orig.cnn. Accessed: Jan 16, 2016.

DAU 2016. Commercial Off-the-Shelf (COTS) Software Solutions. Defense Acquisition Guidebook. https://acc.dau.mil/CommunityBrowser.aspx?id=511641. Accessed: March 5, 2016.

De Nijs, H. 2010. Concept Development and Experimentation Policy and Process: How Analysis Provides Rigour. Nato HQ Supreme Allied Command Transformation, Norfolk, USA.

Dhillon, R. and Kelly, J. 2013. Encryption and the migration to COTS technologies. Military Embedded Systems. http://mil-embedded.com/articles/encryption-the-migration-cots-technologies/. Accessed: March 5, 2016.

Digital Marketing Glossary 2013. What is Push notification definition? The Digital Markeging Glossary. http://digitalmarketing-glossary.com/What-is-Push-notification-definition. Accessed: Feb 29, 2016.

DOD 2012. CBRNE. DOD Dictionary of Military Terms. http://www.dtic.mil/doctrine/dod_dictionary/index.html?zoom_query=cbrne&zoom_sort=0&zoom_per_page=10&zoom_and=1. Accessed: Dec 10, 2015.

DOE 2016. The Manhattan Project, interactive history. U.S. Department of Energy. https://www.osti.gov/opennet/manhattan-project-history/Events /events.htm. Accessed: Jan 12, 2016.

EC 2014. From the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on a new EU approach to the detection and mitigation of CBRN-E risks. European Commission. Brussels. COM(2014) 247 final.

EDA 2008. EDA CBRN Exercise "Firm Foundation 2008". European Defence Agency, Capabilities Directorate, Planning and Policy Unit.

EDA 2014. EDA – CBRNe Countermeasures Concept. https://www.ib-consultancy.com/project/eda-cbrne-countermeasures/. Accessed: Nov 4, 2015.

Encyclopaedia Britannica, 2014. Weapon of mass destruction (WMD). http://global.britannica.com/technology/weapon-of-mass-destruction. Accessed: Nov 4, 2015.

Encyclopaedia Britannica, 2015. Frédéric and Irène Joliot-Curie, French chemists. http://www.britannica.com/biography/Frederic-and-Irene-Joliot-Curie. Accessed: Jan 12, 2016.

ETSI 2016. Tetra. European Telecommunications Standards Institute ETSI. http://www.etsi.org/technologies-clusters/technologies/tetra. Accessed: Feb 24, 2016.

Farlex 2016. Electro-optics. The Free Dictionary by Farlex. http://www.thefreedictionary.com/electro-optical. Accessed: Jan 24, 2016.

EU 2009. EU Cbrne action plan. Council of the European Union. 15505/1/09 REV 1.

FBI 2015a. Amerithrax or Anthrax Investigation. https://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax. Accessed: Nov 9, 2015.

FBI 2015b. Weapons of Mass Destruction. https://www.fbi.gov/about-us/investigate/terrorism/wmd/wmd_faqs. Accessed: Dec 10, 2015.

FEMA 2010. The Federal Emergency Management Agency Publication 1. The Federal Emergency Management Agency. Fema, November, 2010.

Finnpanel 2015. TV-vastaanottimien lukumäärä kotitalouksissa, Vuosi 2014. http://www.finnpanel.fi/tulokset/tv/vuosi/tvtaloudet/2014/. Accessed: Nov 21, 2015.

Fisher, A. 2011. Calls to regulate fertilizer after bomb. http://www.newsinenglish.no/2011/07/25/calls-to-regulate-fertilizer-after-bomb/. Accessed: Nov 9, 2015.

Ganesan, K., Raza, S. K. and Vijayaraghavan, R. 2010. Chemical warfare agents. Journal of Pharmacy & BioAllied Sciences, 2010 Jul-Sep; 2(3): 166–178.

Garamone, J. 2014. Cape Ray teams begin neutralizing Syrian chemicals. www.army.mil. The official home page of the United States army. July 8, 2014. http://www.army.mil/article/129611/Cape_Ray_teams_begin_ neutralizing_ Syrian_chemicals/. Accessed: Dec 20, 2015.

GPS 2016. The Global Positioning System. http://www.gps.gov/systems/gps/. Accessed: March 4, 2016.

GTI 2015. Global Terrorism Index 2015. Measuring and understanding the impact of terrorism. The Institute for Economics and Peace, Sydney, New York, Mexico City, 2015.

Guardian 2013. Terror in Nairobi: the full story behind al-Shabaab's mall attack. http://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya. Accessed: June 6, 2016.

Guardian, 2015. Available in: http://www.theguardian.com/world/2015/sep/12/tianjin-explosion-china-sets-final-death-toll-at-173-ending-search-for-survivors. Accessed: Nov 5, 2015.

Guardian 2015b. Turkey terror attack: mourning after scores killed in Ankara blasts. http://www.theguardian.com/world/2015/oct/10/turkey-suicide-bomb-killed-in-ankara. Accessed: June 6, 2016.

Harris, M., L., Sapko, M. J. and Mainiero, R. J. 2003. Toxic Fume Comparison of a Few Explosives Used in Trench Blasting. National Institute for Occupational Safety and Health Pittsburgh Research Laboratory. Centers for Disease Control and Prevention, U.S. Department of Health & Human Services.

Hart, J. D. 2014. The Analysis of Competing Hypothesis (ACH) in the Assessment of Chemical Warfare Activities. National Defence University. Department of Strategic and Defence Studies. Series 1: Strategic Research No 34. Helsinki 2014.

HC, 2006. Report of the Official Account of the Bombings in London on 7th July 2005. Ordered by the House of Commons to be printed 11th May 2006.

http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/11_05_06_narrative.pdf. Accessed: Nov 9, 2015

Heiskanen, M. 2010. TEPO/ CBRNE yhteistyö eri viranomaisten kanssa and Yhteistyö kaupungissa sijaitsevien yritysten, laitosten, virastojen sekä lähetystöjen turvallisuushenkilöstön kanssa in Onnistumisen iloa - Turvallisuuden hyviä käytäntöjä. Sisäinen turvallisuus. Sisäasiainministeriön julkaisuja 34/2010. Ministry of Interior, Finland.

Hillebrand, F. (ed.) 2010. Short Message Service (SMS): The Creation of Personal Global Text Messaging. http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470688653.html. Accessed: Nov 18, 2015.

History, 2015a. Pan Am Flight 103 explodes over Lockerbie, Scotland. http://www.history.com/this-day-in-history/pan-am-flight-103-explodes-over-lockerbie-scotland. Accessed: Nov 18, 2015.

History, 2015b. 9/11 Attacks. http://www.history.com/topics/9-11-attacks. Accessed: Nov 18, 2015.

Hoft, J. 2015. Breaking: ISIS Smuggled Sarin Gas Through Turkey – Terrorists Captured With Poison Gas in Switzerland. http://www.thegatewaypundit.com/2015/12/breaking-isis-smuggled-sarin-gas-through-turkey-terrorists-captured-with-poison-gas-in-switzerland/. Accessed: Jan 2, 2016.

Hänninen, J. & Passi, M., 2014. Esitutkinta: Yliopistoisku peruuntui viime hetkellä tammikuussa. http://www.hs.fi/kaupunki/a1401069671937. Accessed: Nov 9, 2015.

IAEA 2011. Fukushima Nuclear Accident Update Log. International Atomic Energy Agency, IAEA. https://www.iaea.org/newscenter/news/fukushima-nuclear-accident-update-log-52. Accessed: Jan 12, 2016.

IAEA 2015. INES. The International Nuclear and Radiological Event Scale. http://www-ns.iaea.org/tech-areas/emergency/ines.asp. Accessed: Jan 15, 2016.

IAEA 2016a. International Atomic Energy Agency, IAEA. https://www.iaea.org/. Accessed: Jan 12, 2016.

IAEA 2016b. IAEA Publications on Accidents Response. http://www-pub.iaea.org/books/IAEABooks/Publications_on_Accident_Response. Accessed: Jan 12, 2016.

IAEA 2016c. IAEA Director General Yukiya Amano's Statement on the DPRK's Announcement of a Nuclear Test. https://www.iaea.org/newscenter/pressreleases/iaea-director-general-yukiya-amano%E2%80%99s-statement-dprk%E2%80%99s-announcement-nuclear-test. Accessed: Jan 13, 2016.

ICRP 2016. International Commission on Radiological Protection. http://www.icrp.org/index.asp. Accessed: Jan 12, 2016.

Intermin 2010. Kansallinen terrorismin torjunnan strategia. Ministry of the Interior, Finland.

Intermin 2014. Valtioneuvoston periaatepäätös Kansalliseksi terrorismin torjunnan strategiaksi 2014-2017. Ministry of the Interior, Finland.

ISMS 2015. ISMS Conference 2015. (R)Evolution Of War. 13-15 October, 2015. Helsinki, Finland. The International Society of Military Sciences and the Finnish National Defence University, Finnish Defence Forces. Conference notes.

Johnson, N. G 2015. Explosive. Chemical product. Encyclopaedia Britannica. http://www.britannica.com/technology/explosive. Accessed: Jan 7, 2016.

Justia 2015. 2010 Nevada Code. Title 15. Crimes and punishments. Chapter 202 Crimes Against Public Health and Safety. NRS 202.4437 "Radioactive agent" defined. http://law.justia.com/codes/nevada/2010/title15/chapter202/nrs202-4437.html. Accessed: Jan 12, 2016.

Karimi F. and Almasy S. 2016. Istanbul airport attack: Planner, 2 bombers identified, report says. CNN. http://edition.cnn.com/2016/07/01/europe/turkey-istanbul-ataturk-airport-attack/. Accessed: July 2, 2016.

Keller, J. 2013. The revenge of COTS: an ageing commercial technology base complicates military supply chain. Military & Aerospace Electronics. http://www.militaryaerospace.com/blogs/mil-aero-blog/2013/11/the-revenge-of-cots-an-ageing-commercial-technology-base-complicates-military-supply-chain.html. Accessed: March 5, 2016.

Kerkelä, L. 2015. Hovioikeus kumosi joukkosurmaa Helsingin yliopistoon valmistelleen naisen vankeustuomion. http://www.hs.fi/kotimaa/a1432085856028. Accessed: Nov 9, 2015.

KNO3 2015. Uses of potassium nitrate. http://www.kno3.org/about-potassium-nitrate/uses-of-potassium-nitrate. Accessed: Jan 5, 2016.

Kube, C 2015. ISIS Used Mustard Gas Against Kurdish Forces in Iraq, U.S. Believes. http://www.nbcnews.com/storyline/isis-terror/isis-used-mustard-gas-against-kurdish-forces-iraq-u-s-n409461. Accessed: Jan 2, 2016.

Kuula J, Emergency Alerting with Smartphones, Critical Communications Europe, Amsterdam, The Netherlands, conference presentation, 11-12. March, 2014

Kuula J, Enriched Crisis Communication with Smartphones in Escalated Emergencies, The 5th International Disaster and Risk Conference IDRC, Davos, Switzerland, conference presentation, 24-28. August, 2014.

Kuula J, Häkkinen M, Jalasvuori J, The Need for International Harmonization of Emergency Notification Systems: The Case of Finland, Proceedings of the Global Risk Forum GRF, One Health Summit, Davos, Switzerland, 19-22. February, 2012

Kuula, J, Kauppinen O, SAPPORO Älypuhelinviestintä vaaratilanteessa – Tapauskertomus kemikaalionnettomuuden pelastusharjoituksesta, ISSN 2323-4997, ISBN 978-951-39-5573-1, Jyväskylän yliopisto, Informaatioteknologian tiedekunnan julkaisuja 6/2014, 78 s., January, 2014

Kuula J, Kauppinen O, Auvinen V, Kettunen P, Viitanen S, Korhonen T, Smartphones as an Alerting, Command and Control System for the Preparedness Groups and Civilians: Results of Preliminary Tests with the Finnish Police, Proceedings of The 10th International Conference on Information Systems for Crisis Response and Management ISCRAM Conference – Baden-Baden, Germany, 12-15. May, 2013.

Kuula J, Kauppinen O, Auvinen V, Kettunen P, Viitanen S, Korhonen T, Alerting Security Authorities and Civilians with Smartphones in Acute Situations, 12th European Conference on Information Warfare and Security ECIW-2013, Jyväskylä, UK / Finland, 11-12. July, 2013.

Kuula, J., Kettunen, P., Räsänen, J., Kauppinen, O., Viitanen, S. and Auvinen, V. 2013. Practical experience in mobile software research, development and testing project Tilannekohtaista turvallisuutta parantavat kohdennetut palvelut / Situational awareness through proactive risks and opportunities, Sapporo in 2011-2013. University of Jyväskylä, Department of Mathematical Information Technology.

Kuula J, Räsänen J, Kettunen P, Kauppinen O, Panasenko S, Mobile Emergency Messaging and the Vulnerability of Crisis Communication, Proceedings of the 8th Symposium of CBRNE Threats, Turku, Finland, 11-14. June, 2012

Lallanilla, M. 2013. What Causes Fertilizer Explosions? http://www.scientificamerican.com/article/what-causes-fertilizer-explosions/. Accessed: Jan 7, 2016.

Lefebvre, X. 2015. Joint Chemical, Biological, Radiological and Nuclear Defence Centre of Excellence, A new NATO CBRN Reachback capability. Presentation given by Colonel Xavier Lefebvre, Director, Operations Support Department, Nato, in NBC 2015 Symposium in Helsinki, Finland on 20 May 2015.

Levy, A. 2015. India Is Building a Top-Secret Nuclear City to Produce Thermonuclear Weapons, Experts Say. http://foreignpolicy.com/2015/12/16/india_nuclear_city_top_secret_china_pakistan_barc/. Accessed: Jan 13, 2016.

Marcus, J. 2015. Japan's (self) defence forces. BBC News. http://www.bbc.com/news/world-asia-33549015. Accessed: Jan 15, 2016.

Medlibrary 2015. Cell Broadcast. http://medlibrary.org/medwiki/Cell_Broadcast. Accessed: Nov 21, 2015.

Merriam-Webster 2016. Optoelectronics. http://www.merriam-webster.com/dictionary/optoelectronics. Accessed: Jan 24, 2016.

Nato 2008. Guidelines for First Response to a CBRN Incident. NATO Civil Emergency Planning. Civil Protection Committee.

Naylor, H. 2015. Weapons inspectors say non-state fighters in Syria used mustard gas. https://www.washingtonpost.com/world/weapons-inspectors-determine-syrian-insurgents-used-mustard-gas/2015/11/06/7865d4e0-84b0-11e5-8bd2-680fff868306_story.html. Accessed: Nov 9, 2015.

NBC 2015. NBC 2015 9th Symposium on CBRNE threats. How does the landscape evolve? 18 – 21 May, 2015. Helsinki, Finland. Conference notes.

Nerg, P. 2015. Opening speech in the NBC 2015 9th Symposium on CBRNE threats on 19.5.2015 given by Permanent Secretary Päivi Nerg from the Ministry of the Interior. Helsinki, Finland.

NEW 2008. New World Encyclopedia. Sarin.

NOAS 2015. The 4th Nordic Military Analysis Seminar. 1. – 2. June, 2015. Helsinki, Finland.Finnish Defence Research Agency FDRA. Conference notes.

NRC 2013. Backgrounder on Chernobyl Nuclear Power Plant Accident. The U.S. Nuclear Regulatory Commission, NRC. http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/chernobyl-bg.html. Accessed: Jan 12, 2016.

NRC 2015. Nuclear Materials. The U.S. Nuclear Regulatory Commission, NRC. http://www.nrc.gov/materials.html . Accessed: Jan 12, 2016.

NTI 2016. The Nuclear Threat Initiative. http://www.nti.org/. Accessed: Jan 12, 2016.

One2many 2012. Cell broadcast explained. http://www.one2many.eu/en/cell-broadcast/how-it-works. Feb 29, 2016.

OPCW, 2015a. Genesis and Historical Development. https://www.opcw.org/chemical-weapons-convention/genesis-and-historical-development/. Accessed: Nov 9, 2015.

OPCW, 2015b. About OPCW. https://www.opcw.org/about-opcw/. Accessed: Dec 18, 2015.

Osaki, T. 2015. Deadly sarin attack on Tokyo subway system recalled 20 years on. http://www.japantimes.co.jp/news/2015/03/20/national/tokyo-marks-20th-anniversary-of-aums-deadly-sarin-attack-on-subway-system/#.Voj2U8LUidE. Accessed: Jan 3, 2016.

OSHA 2016. Biological agents. Occupational Safety & Health Administration. U.S. Department of Labor. https://www.osha.gov/SLTC/biologicalagents/. Accessed: Jan 12, 2016.

Phillips, C. T., Checkai, R., T., Kuperman, R. G., Simini, M., Kolakowski, J. E. and Kurnas, C. W. 2004. Environmental toxicity of the explosives RDX and TNT in soil to the soil inverterbrate Folsomia Candida. U.S. Army Edgewood Chemical Biological Center (ECBC) Aberdeen Proving Ground, MD 21010-5424 USA.

Pletcher, K., 2014. Tokyo subway attack of 1995. http://global.britannica.com/event/Tokyo-subway-attack-of-1995. Accessed: Nov 9, 2015.

Pubchem 2005. Ammonium Nitrate. Pubchem Open Chemistry Database. National Center for Biotechnology Information, _U.S. National Library of Medicine.

Ramseger, A., Kalinowski, M. B. & Weiß, L. 2009. CBRN Threats and the Economic Analysis of Terrorism .Network for the Economic Analysis of

Terrorism (NEAT) Economics of Security Working Paper Series, DIW Berlin.

Rapiscan 2016. http://www.rapiscansystems.com/. Accessed: Feb 4, 2016.

Reinl, J. 2015. Syrian medic takes chlorine gas evidence to Congress. http://www.middleeasteye.net/news/syrian-medic-takes-chlorine-gas-evidence-congress-1925178043. Accessed: Jan 2, 2016.

Rouse, M. & Steele, C 2014. Push notification definition. http://searchmobilecomputing.techtarget.com/definition/push-notification. Accessed: Nov 21, 2015.

Salminen, P., 2015. Opening speech at the 8th Military sciences days in Finland on 16.10.2015 given by major general (ret.) Pertti Salminen, chair of The Finnish Society of Military Sciences.

Schleifer, T., 2015. Kerry: Syrian regime 'absolutely' used chlorine in attacks. http://edition.cnn.com/2015/06/16/politics/john-kerry-syrian-chemical-weapons-chlorine. Accessed: Nov 9, 2015.

Schmitt, K. & Zacchia, N. A. 2012. Total Decontamination Cost of the Anthrax Letter Attacks. Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science 10(1)

SFOE 2015. Nuclear energy. Swiss Federal Office of Energy SFOE. http://www.bfe.admin.ch/themen/00511/?lang=en. Accessed: Jan 15, 2016.

Smith, C. 2008. Cell Phone Triangulation Accuracy Is All Over The Map. Third Door Media. http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790. Accessed: March 5, 2016.

Smith, R. 2012. Introduction to Hyperspectral Imaging. TNTmips. MicroImages Inc.

Smith-Spark, L. & Black, P., 2015. UK inquiry into Litvinenko's poisoning death wraps up. http://edition.cnn.com/2015/08/01/europe/uk-russia-litvinenko-inquiry/. Accessed: Nov 9, 2015.

Spirent 2012. Hybrid Positioning. Spirent Federal Systems. http://www.slideshare.net/spirentgnss/hybrid-positioning. Accessed: March 13, 2016.

STAT 2014. Causes of death in 2013. Statistics Finland. http://www.stat.fi/til/ksyyt/2013/ksyyt_2013_2014-12-30_kat_001_en.html. Accessed: Jan 26, 2016.

Steele, C. 2014. Push notification. http://searchmobilecomputing.techtarget.com/definition/push-notification. Accessed: Feb 29, 2016.

Strickler, S. 2001. The Fallacy of COTS Economics for Space Applications. Intersil. http://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0ahUKEwi0sKvY7anLAhWB2hoKHYRYA2QQFghVMAc&url=http%3A%2F%2Fnepp.nasa.gov%2Fnepag%2Finfo%2Fparts_costs%2FCMSE%2520 %2520The%2520Fallacy%2520Of%2520COTS%2520Economics3.ppt&usg=AFQjCNHf08PYMzZ9IO5CbiNls47knzzPaA. Accessed: March 5, 2016.

STUK 2016. Radiation and Nuclear Safety Authority. http://www.stuk.fi. Accessed: Jan 12, 2016.

STUK 2016b. Environmental radiation. Deposition. http://www.stuk.fi/web/en/topics/environmental-radiation/deposition. Accessed: Jan 15, 2016.

STUK 2016c. Tšernobyl-laskeuma Suomessa. http://www.stuk.fi/aiheet/sateily-ymparistossa/laskeuma/tsernobyl-laskeuma-suomessa. Accessed: Jan 15, 2016.

SVT 2015. Lankapuhelin ja matkapuhelin kotitalouksissa, elokuu 2015. Suomen virallinen tilasto (SVT): Väestön tieto- ja viestintätekniikan käyttö [verkkojulkaisu]. ISSN=2341-8699. Helsinki: Tilastokeskus. http://www.stat.fi/til/kbar/2015/09/kbar_2015_09_2015-09-28_kuv_016_fi.html. Accessed: Nov 21, 2015.

Taylor, A. 2016. Map: The countries believed to have tested hydrogen bombs. https://www.washingtonpost.com/news/worldviews/wp/2016/01/06/map-the-countries-believed-to-have-tested-hydrogen-bombs/. Accessed: Jan 13, 2016.

Tawfeeq, M. and Capelouto, S. 2016. Baghdad bombing kills at least 200; ISIS claims responsibility. CNN. http://edition.cnn.com/2016/07/02/middleeast/baghdad-car-bombs/. Accessed: July 4, 2016.

Telco 2016. Poor Mobile Network Coverage Explained - Weak Signal. Telco Antennas. https://www.telcoantennas.com.au/site/poor-mobile-network-coverage-explained-weak-signal. Accessed: Feb 27, 2016.

Telops 2016. Environment. http://www.telops.com/en/. Accessed: Feb 2, 2016.

Thavaselvam, D. and Vijayaraghavan, R. 2010. Biological warfare agents. Journal of Pharmacy & BioAllied Sciences, 2010 Jul-Sep; 2(3): 179–188.

Topham, G., Weaver, M. & Luhn, A, 2015. Egypt plane crash: Russia says jet was bombed in terror attack. http://www.theguardian.com/world/2015/

nov/17/egypt-plane-crash-bomb-jet-russia-security-service. Accessed: Nov 18, 2015.

Tracey, S. J. 2012. Qualitative Research Methods: Collecting Evidence, Crafting Analysis, Communicating Impact.

Tukes 2016. Tutkitut onnettomuudet 2013. http://www.tukes.fi/fi/Palvelut/asia-tieto-onnettomuustietoja/Tutkitut-onnettomuudet-2013/. Accessed: April 9, 2016.

UC Davis 2011. Comprehensive Emergency and Continuity Management Plan. University of California, Davis.

UN 1991. Resolution 687 (1991). United Nations. Security Council.

UN 2013. Resolution 2118 (2013). United Nations. Security Council.

UNISDR 2015. Sendai Framework for Disaster Risk Reduction 2015-2030. The United Nations Office for Disaster Risk Reduction. Geneva, Switzerland, 2015.

UNODA 2015. 1925 Geneva protocol. United Nations Office for Disarmament Affairs. http://www.un.org/disarmament/WMD/Bio/1925Geneva Protocol.shtml . Accessed: Dec 18, 2015.

UNODA 2016. Nuclear weapons. United Nations Office for Disarmament Affairs. http://www.un.org/disarmament/WMD/Nuclear/. Accessed: Jan 13, 2016.

UNOG 2016. The Biological Weapons Convention. http://www.unog.ch/80256EE600585943/(httpPages)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument. Accessed: Jan 11, 2016.

Urban Airship 2016. Push Notifications Explained. https://www.urbanairship.com/push-notifications-explained. Feb 29, 2016.

UW-Madison Police Department 2012. What is a tabletop exercise?. http://uwpd.wisc.edu/content/uploads/2014/01/What_is_a_tabletop_exercise.pdf. Accessed: Dec 2, 2015.

Valtonen, V. 2010. Turvallisuustoimijoiden yhteistyö operatiivis-taktisesta näkökulmasta. Doctoral thesis. Finnish National Defence University, Department of Tactics. Julkaisusarja 1, n:o 3. Helsinki, 2010.

Verge 2011. Android: A visual history. http://www.theverge.com/2011/12/7/2585779/android-history. Accessed: Nov 21, 2015.

Victim list, 2011. Detailed Oslo bombing and Utøya massacre victim list. https://sites.google.com/site/breivikreport/documents/detailed-oslo-bombing-and-utoya-massacre-victim-list. Accessed: Nov 9, 2015.

Violino, B. 2014. Tabletop exercises help security teams prepare for the worst. http://www.csoonline.com/article/2838365/emergency-preparedness/planning-for-a-security-emergency-from-the-tabletop-down.html. Accessed: Dec 2, 2015.

Virveverkko 2016. Suomen Virveverkko Oy. http://www.virveverkko.fi/. Accessed: Feb 24, 2016.

Welker, J. R. 2016. Explosions. Chemistry Explained, Foundations and Applications. Chemistry Encyclopedia. http://www.chemistryexplained.com/Di-Fa/Explosions.html. Accessed: Jan 6, 2016.

WHO 2015. Ebola virus disease. http://www.who.int/mediacentre/factsheets/fs103/en/. Accessed: Dec 14, 2015.

WHO 2016. Latest Ebola outbreak over in Liberia; West Africa is at zero, but new flare-ups are likely to occur. World Health Organization WHO. http://who.int/mediacentre/news/releases/2016/ebola-zero-liberia/en/. Accessed: Jan 14, 2016.

World Nuclear Association, 2015. Fukushima Accident. http://www.world-nuclear.org/info/safety-and-security/safety-of-plants/fukushima-accident/. Accessed: Nov 18, 2015.

Wyke, T. and Boyle, D. 2015. Have police foiled an ISIS chemical weapons plot in Europe? Two Syrian terror suspects are arrested in Geneva for 'making and transporting explosives and toxic gases'. http://www.dailymail.co.uk/news/article-3357320/Two-Syrian-men-arrested-Geneva-amid-fear-plotting-chemical-bomb-terror-attack-Swiss-city.html. Accessed: Jan 2, 2016.

ORIGINAL PAPERS

PI

DETECTING EXPLOSIVE SUBSTANCES BY THE IR SPECTROGRAPHY

by

Jaana Kuula, Heikki Rinta, Ilkka Pölönen, Hannu-Heikki Puupponen, Marko Haukkamäki & Tuomas Teräväinen, 2014

Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XV, edited by Augustus W. Fountain III, Proc. of SPIE Vol. 9073, 90730Q · © 2014 SPIE CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050157

Detecting explosive substances by the IR spectrography

Kuula J.[a], Rinta H.[b], Pölönen I.[a], Puupponen H-H.[a], Haukkamäki M.[c], Teräväinen T.[d],

[a]Department of Mathematical Information Technology, University of Jyväskylä, Mattilanniemi 2, 40100 Jyväskylä, Jyväskylä, Finland;
[b]Department of Chemistry, University of Jyväskylä
[c]Air Force Command Finland
[d]Central Finland Police Department

ABSTRACT

Fast and safe detection methods of explosive substances are needed both before and after actualized explosions. This article presents an experiment of the detection of three selected explosives by the ATR FTIR spectrometer and by three different IR hyperspectral imaging devices. The IR spectrometers give accurate analyzing results, whereas hyperspectral imagers can detect and analyze desired samples without touching the unidentified target at all. In the controlled explosion experiment TNT, dynamite and PENO were at first analyzed as pure substances with the ATR FTIR spectrometer and with VNIR, SWIR and MWIR cameras. After three controlled explosions also the residues of TNT, dynamite and PENO were analyzed with the same IR devices. The experiments were performed in arctic outdoor conditions and the residues were collected on ten different surfaces. In the measurements the spectra of all three explosives were received as pure substances with all four IR devices. Also the explosion residues of TNT were found on cotton with the IR spectrometer and with VNIR, SWIR and MWIR hyperspectral imagers. All measurements were made directly on the test materials which had been placed on the explosion site and were collected for the analysis after each blast. Measurements were made with the IR spectrometer also on diluted sample. Althogh further tests are suggested, the results indicate that the IR spectrography is a potential detection method for explosive subjects, both as pure substances and as post-blast residues.

Keywords: Hyperspectral detection and analysis, IR spectrography, explosives

1. INTRODUCTION

Fast and safe detection methods are needed for managing cbrne threats and their consequences during the state of war and other sudden disasters in more stable areas. This article represents an experiment were hyperspectral analysis and IR spectrography were used for identifying various explosives as pure substances and for detecting explosive residues after the blast. The motivation for the experiment was to find out whether the hyperspectral imaging technology could be used for detecting IEDs and HMEs or their carriers or builders prior to an explosion, and for detecting and identifying explosive residues after an accidental or intentional blast.

The experiment was designed and built jointly by the researchers of the Department of Mathematical Information Technology and Department of Chemistry of the University of Jyväskylä, and by the explosives specialists of the Central Finland Police Department, the bomb squad of the Finnish Police, and of the Finnish Air Force. The experiment was built to simulate a shopping mall attack, though carried out in controlled outdoor conditions. During the experiment four sequential explosions were carried out with a similar design with powder, TNT, dynamite and PENO, of which the results of TNT, dynamite and PENO are reported in this article. The residues of the explosions were caught on ten different surfaces and objects which were placed identically around the seat of the explosion in all four cases. The materials of these sample collectors were cotton fabric (in three distances), laminate, plastic carpet, detonator wire, duct tape, concrete, plastic bucket and cardboard box. Before the explosions, small samples of the pure substances were also preserved on a clean cotton cloth for the identification with the IR devices.

Further author information:
Jaana Kuula: E-mail: jaana.kuula@jyu.fi, Telephone: +358408053272

Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XV,
edited by Augustus W. Fountain III, Proc. of SPIE Vol. 9073, 90730Q · © 2014 SPIE
CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050157

After the explosion tests all samples were analysed with the ATR FTIR spectrometer and with VNIR, SWIR and MWIR hyperspectral cameras. The ATR FTIR spectrometer was used as a comparative technology for the hyperspectral analysis and for crosschecking which samples have residues and which possibly not. Samples of pure explosives were analysed at first for recording their spectra. After that explosive residues were searched from the ten collectors which were set on the explosion scene in advance for that purpose. Samples were at first analysed with the IR spectrometer, which is a more accurate analyzing method than the hyperspectral analysis. However, for making the IR spectrometer analysis samples may need to be prepared by rinsing the explosive residues with a neutral liquid, which makes the detection of explosives and residues more complicated. After the IR spectrometer analysis collectors were imaged with VNIR, SWIR and MWIR hyperspectral cameras, after which hyperspectral data was analysed with an analyzing software.

The results show that the spectra of TNT, dynamite and PENO can be recorded from pure substances with the IR spectrometer, and that these explosives may be identified and separated with this technology. The explosive residues were, however, found only for TNT. Some of these findings were made by measuring the sample directly on the collector, and some others by measuring the rinsed sample.

The spectra of TNT, dynamite and PENO were also received with all hyperspectral camera types, which means that these three explosives can be identified and separated with VNIR, SWIR and MWIR cameras. Also the post-blast residues were found with all of these three cameras, but only for TNT and not for the two other explosives. All findings of residues which were made with hyperspectral cameras were measured directly from the collector materials which were picked up from the explosion site after each blast.

2. EXPERIMENT

2.1 Research setup

Explosion tests were performed in winter time outdoor conditions by the Department of Mathematical Information Technology and Department of Chemistry of the University of Jyväskylä with the help of the explosives specialists of The Finnish Defence Forces, Bomb Squad of the Finnish Police and the crime scene investigation group of the Central Finland Police Department. For performing the tests, 125-200 grams of TNT, dynamite and PENO were reserved as explosives and various other materials as collectors for the explosion residues. As the explosions were meant to simulate a shopping mall attack, the collector materials were chosen so that they would be likely to be found in a real target of an malicious attack. For example, concrete, laminate and plastic carpet represented the construction and cotton fabric the interior decoration of an attacked building. Accordingly, the plastic bucket, cardboard box, detonator wire and duct tape represented a homemade bomb and its container.

The design of the controlled explosion is presented in Figure 1. The explosive charge was placed in the middle and the ten sample collectors around it at various distances in the range of two meters. All collectors were of different materials, except the cotton fabric which was set on wooden racks at 1, 1.5 and 2 meters from the explosive charge. The cotton fabrics, plastic bucket and cardboard box were placed vertically and the other materials horizontally towards the center of the explosion. The post-blast situation of the explosion site is presented in Figure 2.

The explosive materials in the experiment were 200 grams of Trinitrotoluene (TNT), 125 grams of Dynamite (EGDN-based)and 200 grams of PENO (PENT-based explosive). All explosive materials were used and handled by authorized professionals.

2,4,6-trinitrotoluene (TNT) is a military explosive and it is widely used in various munitions like in mines and grenades. It is being used also as a pure explosive material. The used TNT was obtained as yellow flakes in a tight plastic bag. The used dynamite was a Forcit's FORDYN-trademark and it is an ethylene glycol dinitrate (EGDN) based ammonium nitrate (AN) explosive. FORDYN consist 30-35 % EGDN, < 2 % cellulose nitrate and 50-60 % AN. It is especially suitable for underwater mining and small-amount blasting. PENO is also a trademark of the Forcit Group and it is a plastic explosive for the military purposes. PENO is mainly used for military demolition tasks and for the disposal of unexploded ordnances (UXO). The main components of PENO are the explosive compound pentaerythritol tetranitrate (PENT) and oil. Dimetyldinitrobutan (DMDNB) was added 1 % to PENO for the post-blast identification of the used explosive.[1–4]

Sample material / target	Distance
Cotton fabrics (50*50cm)	1; 1,5 and 2 m
Plastic bucket	< 1.5 m
Cardboard box	< 1.25m
Detonator wire	-
Wiping sample (concrete)	< 0.8 m
Duct tape	< 1m
Plastic carpet	< 1.25m
Laminate	< 1.25m

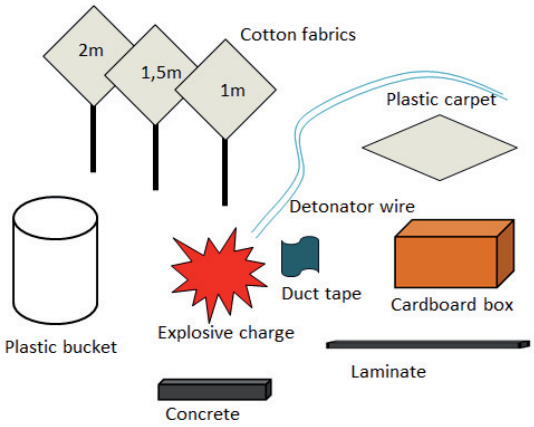


Figure 1. Left: Distances between targets and explosive material. Right: Scheme of the test setup.

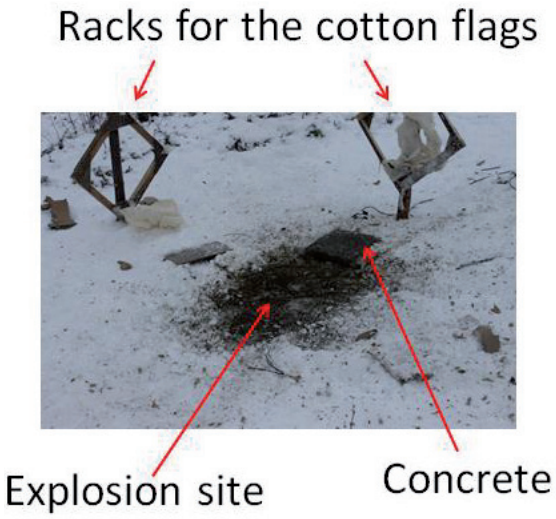


Figure 2. Explosion site after the blast.

The explosions were carried out within one hour at noon in winter conditions with mild wind and frost. There was also a thin snow on the ground. TNT was exploded at first, dynamite as the second and PENO as third. More detailed weather information for the time of each explosion may be seen in Table 1.

Table 1. Weather conditions during the experiment.

	Day	Hour	Min	Temp °C	Humidity %
TNT	22.10.2013	11	20	-2.2	80
Dynamite	22.10.2013	12	20	-2	80
PENO	22.10.2013	12	50	-2	76
	Wind dir.	Wind speed	Wind blasts	Atm. pressure	Visibility
TNT	178	3.6	7	1025.6	50 000
Dynamite	201	2.2	4	1025.5	43 160
PENO	198	1.9	4.7	1025	39 710

After each explosion, remains of the ten sample collectors were gathered and stored by an experienced crime scene investigator by following the approved procedures of forensic inspection. Due to the different kind of explosives and the type of detonation, there was some variation in the size of the remains which were left of the sample collectors. However, as the power of each blast had been defined in advance, pieces could be collected well after each blast. Due to the winter conditions, they were, however, partially covered by snow, and after storing samples in plastic bags the snow melted into water when the bags were brought inside. That may have washed some of the explosion residues away from the samples, but despite of that positive results of the residues were found in some samples with all of the analyzing methods which were used in the study.

When a high energetic material reacts, it can detonate, deflagrate or do the both. The rate of the detonation or deflagration has a major influence on the remaining traces. Detonation is chemically an oxidation reaction which does not involve external oxygen. In the explosion the detonation material involves chemically unstable molecular structures or functional groups that can split into gaseous products and heat (with supersonic reaction speed). Deflagration for its part is a thermal process that proceeds radially outwards away from the ignition source in all directions through the available material. Deflagration can also be incomplete, in which case the reaction can generate various number of different decomposition products.[5]

The physical state of the energetic material has an effect on the proceeding reaction type. For example, using a dense plastic explosive, a shock wave proceeds with the detonation. If the explosive has a granular form, the shock wave of the detonation can terminate and continue as an incomplete deflagration. In this experiment, PENO and dynamite were detonated while granular TNT was deflagrated. As a result of the deflagration, TNT residues were found well on most of the sample materials in the ATR FTIR analysis and quite well also in VNIR, SWIR and MWIR hyperspectral analysis. However, traces of dynamite and PENO were not reliably found in ATR FTIR nor in hyperspecral analysis, which may be explained by their complete explosions, easily evaporated EGDN and high performance compared to TNT.[4]

2.2 ATR FTIR spectroscopy

The ATR FTIR technique is commonly used by military and forensic investigators and by traveling and transportation security officials at the airports. Extensive libraries and advanced device technologies have allowed the wide use of IR- techniques. For example the HazMat FTIR-series is a good example of mobile IR-devices on the market. However, additional basic research is required for the identification of new compounds on complex sample matrixes.[6–9]

In this study IR screening was used for testing this analyzing method on explosives per se, and as a comparative technology for the hyperspectral analysis on the same samples. The preparations of the samples were kept simple. The ATR FTIR-analysis was carried out directly on the explosive materials and on the post-blast

residues. Measurements were made directly on the solid samples and on dried rinse samples on an aluminum foil.

The measurements were made on pure explosives of TNT, dynamite and PENO, and on nine of the ten residue collectors which were used in the tests. Residues on laminate were not measured because of the size of the sample, and because of the melting snow on it. IR spectroscopy results are thereby available from cotton fabric at three distances from the explosive charge, plastic bucket, cardboard box, detonator wire, concrete, duct tape and plastic carpet.

The IR measurements were measured with a Bruker ATR platinum Diamond spectrometer by using the basic measurement mode (range 4000 – 400 cm^{-1}; resolution 4 cm^{-1} and 32 scans). Identification of the explosive materials was carried out by comparing the measured spectra of the pure explosive materials on the cotton fabric with the post-blast residue samples. The absorbance to transmittance-converting and baseline correction of the measured spectra were processed by OPUS 7.0-software.[10]

The ATR FTIR-spectra of the pure explosives were measured by soaking the explosive materials on a clean cotton fabric at first, and by measuring the spectrum of the explosive on the cotton after that. The influence of the background material was reduced of the measurement results after the measures, so the samples represent concentrated wiping samples of the pure explosives used in the test.

The IR analysis of the post-blast residue samples was made in two ways. The residues were at first measured directly on the collected pieces without any sample preparation or wiping in between. After that, rinsed samples of the collected pieces were produced with acetone. Solid samples were rinsed by using 5 ml of acetone, and then filtered (Whatman 40) and evaporated on an aluminum foil. When the dilutions were evaporated completely, IR-spectrum was measured on the aluminum foil.

2.3 Hyperspectral imaging and analysis

The detetction, separation and identification of explosives and explosive residues with hyperspectral analysis was the primary purpose of this study. For veryfying hyperspectral test results, same samples were analysed also with the IR spectroscopy.

Three different types of hyperspectral imagers were utilized and compared for screening efficacy during the study. Spectral range of the devices reached from visible light to mid-wave infrared. Imagers were manufactured by Specim Ltd. Technical details of the imagers are found in the Table 2.

Table 2. Technical properties of the hyperspectral camera equipment used in the study.

material	VNIR	SWIR	MWIR
Spectral Range	400 - 1000 nm	970 - 2500 nm	2000 - 6000 nm
Number of spectral bands	96	256	256
Spectral resolution	2.8 nm	10 nm	35 nm
Number of pixels/image line	1000	320	320

The detection of explosive residues was performed in two phases. First, the spectra of the explosive substances were detected from the samples of pure explosives. After that the target detection algorithm was used for finding the residues of pure substances from the pieces of various materials which had been collected from the explosion site. Test targets were also classified with a spectral classification algorithm for combining the results. False color images of the pure samples imaged with each hyperspectral camera are presented in Figure 3. As Figure 3 reveals one can see from the VNIR data that the pure TNT and Dynamite are clearly visually distinguishable, but the difference between them is not as clear. The false color images of the SWIR and MWIR data suggest that the explosives may have some characteristic features at those wavelengths.

The extraction of the spectra for the explosives was made by using vertex component analysis (VCA).[11] VCA is a widely utilized computationally efficient way to induct endmembers from spectral data. The basic

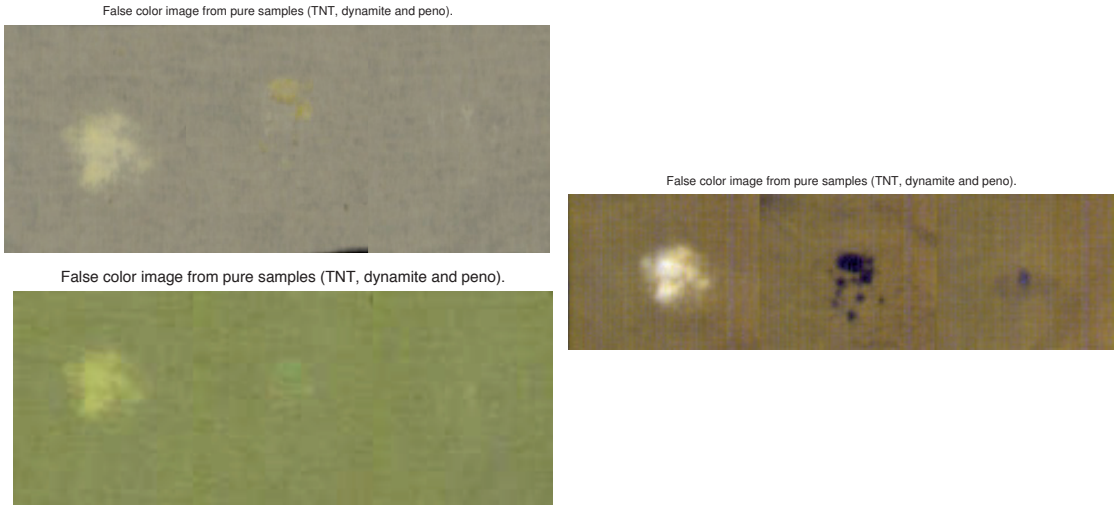


Figure 3. False color images with narrow wavebands showing pure explosives on the piece of cotton fabric. In each image there is a small amount of TNT, dynamite and PENO (from left to right). Top-left: VNIR, Bottom-left: SWIR and Right: MWIR.

idea behind VCA is to orthogonally project spectral data to a lower dimensional space and to detect there an extremeity vertex of the convex hull covering the data points. In the case of the VCA it is a pre-requisite to know how many endmembers the algorithm is intended to generate. The endmember induction process is sensitive to this setting, because it continues from one projection and extremity vertex to next until it reaches the number of endmembers required. Additionally, in VCA the spectral data is assumed to be a linear mixture of endmembers.

In this experiment, VCA was performed separately for each camera's data. As a result endmembers were received for each data set. These spectra are illustrated in Figure 4. Discovered endmembers can be verified by calculating the inversion back to the original spectral data. In this case computationally costly non-negative constraint least squares (NNLS)[12] were used on each pixel of the test samples to determine the abundance images for each inducted endmember.

There is reason to assume that the post-blast explosive residues are more or less subpixel-scale in data. This means that also a subpixel level method is needed for finding these small particles. In this case, a small combination of algorithms, including VCA and NNLS as their core components, was utilized for this purpose. In the the HFC method[13] which was applied in this analysis, the virtual dimension number will be calculated first in order to determine the potential number of endmembers in the data. After that the VCA will be utilized to extract the endmembers. Then the target endmember signature will be added to the results from the VCA step. If the VCA finds an endmember which is very similar to the target endmember, this matching endmember will be displaced by the original target endmember. The comparison is performed with a spectral angle mapper (SAM)[14] algorithm. It measures the spectral similarity by finding the angle (in radians) between endmember $\mathbf{e} = (e_1, e_2, \dots e_L)^T$ and imaged spectrum $\mathbf{s} = (s_1, s_2, \dots s_L)^T$ so that,

$$sam = \cos^{-1}\left(\frac{\sum_{l=1}^{L} e_l s_l}{(\sum_{l=1}^{L}(e_l)^2)^{1/2}(\sum_{l=1}^{L}(s_l)^2)^{1/2}}\right),$$

where L is number of wavebands in spectra. SAM is meant for the signature vector based target discrimination and identification. It gives values for each pixel in the image and is computationally cheap. If the degree of mixing between the imaged spectra is low, SAM should work efficiently, but because in this case we are looking for subpixel traces, SAM will not give very accurate results.

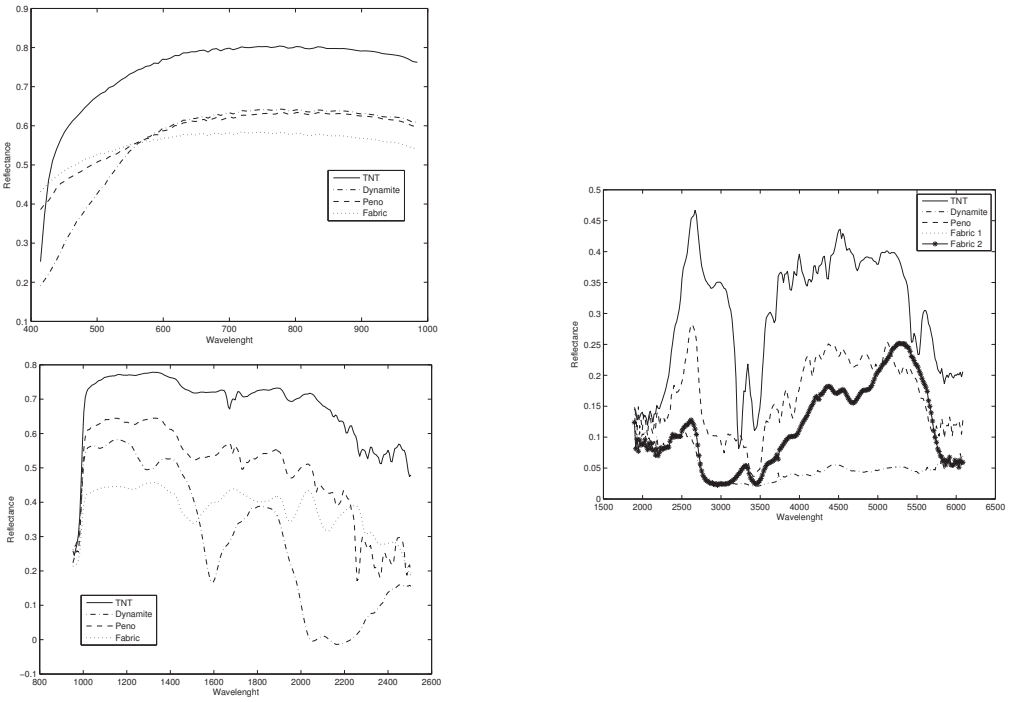


Figure 4. Endmembers extracted from each imager's data with VCA. Top-left: VNIR, Bottom-left: SWIR and Right: MWIR.

After determining the endmember set the NNLS is calculated. As an output the algorithm provides the abundance data for the target endmember. Figure 5 shows these abundance maps for the pure explosive substances. Basically endmembers for TNT and dynamite can be detected in data from all of the three cameras. PENO is distinguishable only with SWIR and MWIR cameras.

3. RESULTS AND DISCUSSION

3.1 ATR FTIR-spectroscopy of the pure explosive materials and post-blast residues

The processed IR-spectra of the wiping samples the tested pure explosive materials are presented in Figure 6. Explosive materials in all of these samples contain -ONO2 or -NO2 groups which are recognized in the IR-spectrum. The main component of the Fordyn-dynamite is AN, which is shown in the same region as the pure AN in its own spectrum. The main differences between TNT, dynamite and PENO are the aromaticity of TNT the molecule, type -NO2 group and the distribution of the components.[15] A characteristic peak of the DMDNB is shown in the fingerprint region of the PENO-spectrum, even if the intensities of the peaks are weak as a result of 1 % concentrate.

The IR-spectra of the post-blast residue samples were compared with the absorbance spectra of the pure explosive materials which were generated to the library of the OPUS-software. The identification was accomplished by using direct-methods.

The post-blast residue samples were measured directly from the samples without any preparations, and from rinsed samples which were produced with acetone. The solid samples were rinsed from the background material with a minimum volume of acetone, which was then filtered and evaporated on the aluminum foil. When the dilutions were evaporated until dry, IR-spectrum was measured on the aluminum foil.

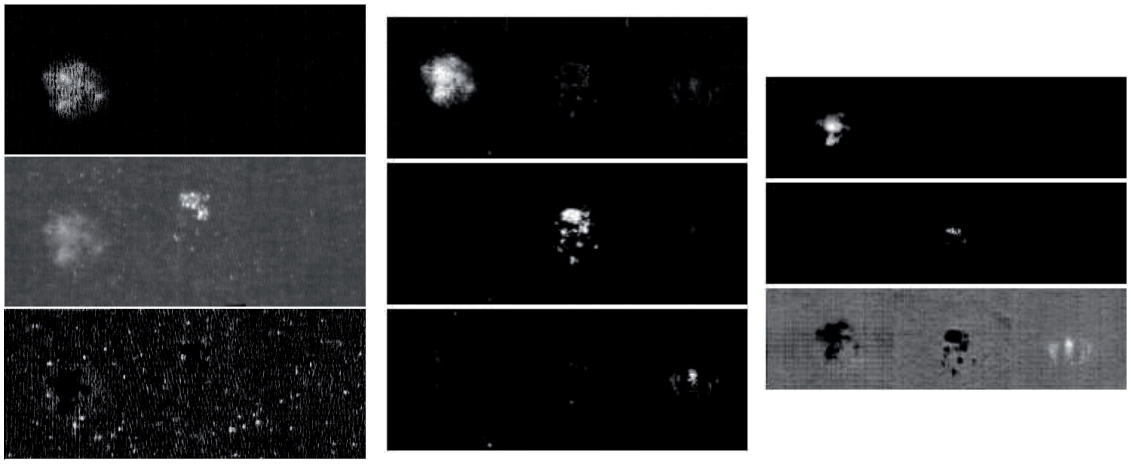


Figure 5. Target detection abundance maps for each imager, VNIR (left), SWIR (middle) and MWIR (right). Top map in each column represents TNT, dynamite in the middle and PENO below. As can be seen below on the left, the endmember for PENO was not found with the VNIR imager. In the SWIR and MWIR data all of the three substances are found.

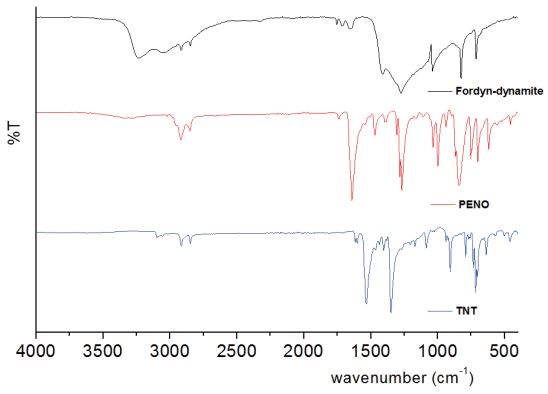


Figure 6. IR-spectrum of the pure explosive materials.

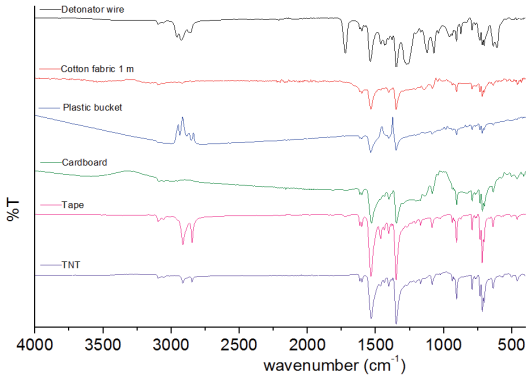


Figure 7. IR-spectrum of the post-blast residue samples, measured directly on the materials without any sample preparation. Identification by the OPUS-software.

Sample / target material	Directly on the material	Rinsed sample
Cotton flag (50*50cm) 1m	+	+
Cotton flag (50*50cm) 1.5m	–	+
Cotton flag (50*50cm) 2m	–	+
Plastic bucket	+	+
Cardboard box	+	+
Detonator wire	+	
Wiping sample (concrete)	–	+
Plastic tape	+	–
Plastic carpet	–	–

+ positive identification; – negative identification

Figure 8. Outline of the TNT sample identification by ATR FTIR

The IR-spectra of the TNT post-blast residue samples, which were measured directly on the materials collected from the explosion site, are presented in Figure 7. The spectra contain almost all peaks of the pure TNT. There are also some additional peaks in some of the materials because of the missing of the background reduction. Nevertheless, all crucial peaks are shown for the identification of the TNT in the post-blast residue samples.

The rinsed samples were produced with an easily evaporating acetone, which is an inert and appropriate solvent for the TNT residues. The aluminum foil was found to be a suitable zero background material for the evaporation and for the measurements of the rinsed and dried samples. In the measurements the rinsed samples were utilized as concentrated wiping samples.

The spectra of the rinsed samples were clearer than the spectra which were measured directly on the objects which were collected from the explosion site. Positive results for TNT were found in all sample materials except on the plastic carpet. The moisture of some of the samples (created by the melted snow) made the search of the explosion residues more difficult, which can explain the missing positive result in some of the measures. An outline of the detection of TNT residues on direct and rinsed samples is illustrated in Figure 8.

3.2 Hyperspectral analysis results

Shortly after the explosion tests the collected sample materials were imaged with three hyperspectral cameras. After the measurements data analysis was carried out as is described in section 2.3. As can be seen in Figures 5 and 9, the SWIR data gives the clearest result for the detection of pure explosive residues.

Using the target detection algorithm gives with some of the samples reasonably clear results. For example in Figure 10 can be found some subpixels, which are identified to contain traces of TNT. However, there are also some false indications, like in the analyzing results of the duct tape and some plastic samples. In these cases

Figure 9. False color image of abundance of pure substances

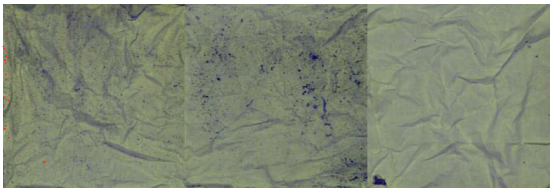


Figure 10. The detection of TNT residues from the cotton fabric. Three fabrics were placed at a different range from the explosive charge (100, 150 and 200 cm; in image from left to right). Traces of TNT were found with all of the three hyperspectral cameras on a fabric which was placed at 100 cm from the charge.

the same algorithm gave indications of dynamite from a sample which was taken from the explosion with TNT. (There is, however, a small chance that the sample contains dynamite, or that the algorithm gives a positive result for dynamite instead of TNT because of the similarities in the chemical structure of these substances.)

It is also possible to use SAM to give some insight on the accuracy of the method. As can be seen in Figure 11, SAM classifies each explosive correctly with pure materials. On the left in Figure 11 are classification results for SWIR data and on the right for MWIR data (TNT = red, Dynamite = blue, PENO = yellow). In Table 3 are represented the minimum values of SAM for each target material and for each camera. As was mentioned earlier, an endmember for PENO could not be extracted from VNIR camera data. If the results for pure explosives and explosive residues are compared, it seems that the minimum SAM for explosive residues is many times higher than for pure substances. Thus, based on this information it is not clear that the correct indications concerning the presence of explosive residues can be confirmed with SAM.

4. CONCLUSION

The objective of this study was to test whether the selected explosives can be detected, identified and separated as pure substances and explosive residues with an IR spectrometer and with three different hyperspectral cameras with the wavelengths of VNIR, SWIR and MWIR areas. The experiment was made as controlled explosions at winter time outdoor conditions, after which the wiping samples of pure explosives and explosion residues on several different test materials were analysed with the ATR FTIR spectrometer and with three different hyperspectral cameras. The analysis with the IR spectrometer included direct measurements on the samples and measurements on the dilluted samples. All hyperspectral analyses were made on data which was measured

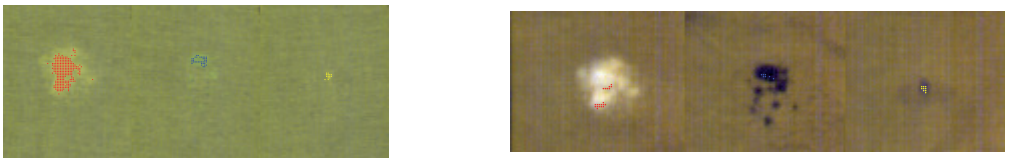


Figure 11. On the left are SAM classification results for SWIR data and on the right for MWIR data (TNT = red, Dynamite = blue, PENO = yellow)

Table 3. Smallest found spectral angle between targets and detected endmembers for explosive materials.

Explosive material	Spectral imager	Pure Sample	Cotton fabric	Plastic bucket	Duct tape
TNT	VNIR	0.006	0.019	0.024	0.025
	SWIR	0.011	0.105	0.063	0.041
	MWIR	0.036	0.135	0.208	0.162
Dynamite	VNIR	0.006	0.031	0.037	0.036
	SWIR	0.057	0.295	0.325	0.347
	MWIR	0.201	0.172	0.285	0.188
PENO	VNIR	n/a	n/a	n/a	n/a
	SWIR	0.022	0.122	0.095	n/a
	MWIR	0.075	0.134	0.172	n/a

directly on pure explosive substances and on objects (residue collectors) which were collected on the explosion site after each blast.

The results show that the spectra of the pure substances of the tested three explosives, TNT, dynamite and PENO, can be detected and separated both with the ATR FTIR spectrometer, and with all of the three tested hyperpectral cameras, VNIR, SWIR and MWIR. Also the post-blast explosive residues of TNT were detected on cotton fabric with all of these four technologies. With the ATR FTIR spectrometer post-blast residues of TNT were also found on plastic bucket, cardboard box, detonator wire, concrete (wiping sample) and on duct tape. Also the hyperspectral cameras found some sparate traces of TNT, for example the VNIR camera on the cotton fabric at three different range from the explosive charge, and SWIR camera on the duct tape. However, post-blast traces of dynamite and PENO were not detected with any of the four IR technologies, which may at one part be explained by the detonation type of explosion of dynamite and PENO, and by the deflagration of TNT.

Table 4. Comparison of TNT results between hyperspectral imaging and ATR FTIR measurements. (+ = found, - = not found)

Target		ATR FTIR	VNIR	SWIR	MWIR
Cotton fabric	100 cm	+	+	+	+
	150 cm	-	+	-	-
	200 cm	-	+	-	-
Plastic bucket		+	-	-	-
Duct tape		+	-	+	-

If the direct measuring results of the explosion residues of TNT are compared between hyperspectral imaging and ATR FTIR spectrometry, one can observe in Table 4 that there might be some correlation between ATR FTIR, SWIR and MWIR results, especially with traces on cotton. From this one can conclude that it might be possible to detect some post-blast explosive residues through the use of hyperspectral imaging. However, further research and experiments are needed for making more confimed conclusions on this topic. As the size of the measurement area is different in ATR FTIR and hyperspectral imaging, in the research ATR FTIR measurements should be taken precisely on the same spot on the target materials as where the hyperspectral imaging is being done. Closer examination may be focused on spots where positive results have been received with either of the technology. In the hyperspectral analysis, it also seems that the HFC is affected by noisy data, so it should be replaced with a less noise sensitive method.

ACKNOWLEDGMENTS

This research has been funded by Tekes - the Finnish Funding Agency for Innovation and by the University of Jyväskylä.

REFERENCES

[1] Gallagher, E. M., [*Molecular Analysis of Active Degraders and metabolic*] (2010).

[2] Republic, C. and Republic, S., "Some experience with trace analysis of post- explosion residues," *AARMS* **3**(4), 633–646 (2004).

[3] Song-Im, N., "Explosive residue analysis : Evaluation and optimisation of sampling," *Storage and Cleanup Protocols* , 1–212 (2011).

[4] Forcit, L., "Forcit defence." www.forcit.fi/en/forcit-defence-2 (2013).

[5] Akhavan, J. E., [*The Chemistry of Explosives, 2nd ed.*], RSC Paperbacks (2004).

[6] Mou, Y. and Rabalais, J. W., "Detection and identification of explosive particles in fingerprints using attenuated total reflection-fourier transform infrared spectromicroscopy," *J.Forensic Sci.* **54**(4), 846–850 (2009).

[7] Primera-Pedrozo, O. M., Y. M. Soto-Feliciano, L. C. P.-L., and Hernandez-Rivera, S. P., "Detection of high explosives using reflection absorption infrared spectroscopy with fiber coupled grazing angle probe/ftir," *Sens. Imaging* **10**(1-2), 1–13 (2009).

[8] Pacheco-Londono, L. C., Castro-Suarez, J. R., and Hernandez-Rivera, S. P., "Detection of nitroaromatic and peroxide explosives in air using infrared spectroscopy: Qcl and ftir," *Adv. Opt. Tech.* , 1–8 (2013).

[9] Furstenberg, R., Kendziora, C. A., Stepnowski, J., Stepnowski, S. V., Rake, M., Papantonakis, M. R., Nguyen, V., Hubler, G. K., and McGill, R. A., "Stand-off detection of trace explosives via resonant infrared photothermal imaging," *Appl. Phys. Lett.* **93**(22), 224103 (2008).

[10] Bruker, [*OPUS, Spectroscopic Software, Reference Manual*], Bruker, 5 ed.

[11] Nascimento, J. and Dias, J., "Vertex component analysis: A fast algorithm to unmix hyperspectral data," *IEEE Transactions on Geoscience and Remote Sensing* **34**(4), 898–910 (2005).

[12] Bro, R. and De Jong, S., "A fast non-negativity-constrained least squares algorithm," *Journal of Chemometrics* **11**(5), 393–401 (1997).

[13] Chang, C., [*Hyperspectral Imaging: Techniques for Spectral Detection and Classification*], Kluwer Academic/Plenum (2003).

[14] Schowengerdt, R. A., [*Remote Sensing, Third Edition: Models and Methods for Image Processing*], Academic Press, Inc., Orlando, FL, USA (2006).

[15] SDBS, "Spectral database for organic compounds sdbs." http://sdbs.db.aist.go.jp (2013).

PII

DRONE BASED HYPERSPECTRAL DETECTION OF CBRNE THREATS

by

Jaana Kuula, 2015

Jussi Paatero & Nils Meinander (Eds.). Proceedings of the NBC-2015 Symposium – How does the landscape evolve? - Helsinki, Finland, May, 2015. ISBN 978-952-93-5586-0.

Drone Based Hyperspectral Detection of CBRNE Threats

Jaana Kuula

University of Jyväskylä, Department of Mathematical Information Technology
P.O. Box 35, 40014 Jyväskylä, Finland

Abstract

For avoiding exposure, further damage and spoiling of the possible crime scene, CBRNE targets should be detected and investigated without touching anything in the place. With the hyperspectral technology substances can be detected without touching and taking a sample. With drones detection can also be made without entering into the site by ground. This article evaluates the feasibility of drone based hyperspectral detection and investigation of CBRNE sites with empirical tests. First the hyperspectral detection of explosives, explosive residues and toxic chemical agents is presented with explosion experiments and laboratory tests with VNIR, SWIR, MWIR and LWIR types of cameras. Secondly, the airborne hyperspectral detection of explosives is presented with field studies with a lightweight VIS type of camera mounted in a drone. The experiments indicate that in eligible imaging conditions it is possible to detect explosives, explosive residues and chemical agents with hyperspectral technology when the selected camera corresponds with the chemical fingerprint of the target. In the outdoor field conditions requirements for precision hyperspectral CBRNE investigation are, however, extremely high, and further development is needed for small hyperspectral imaging devices and possibly also for drones.
Keywords: CBRNE, hyperspectral, detection, airborne, drones, forensic investigation

1 Introduction

In CBRNE situations, malicious substances may need to be detected in many phases of the rescue and investigation process. Detection is needed for example as a

1. preventive measure before the threat has actualized in the target,
2. rescue measure when malicious substances have already been released in the target,
3. recovery measure for detecting and defining contamination for cleaning, and
4. as a verification and forensic investigation method for proving a possible crime.

Detection of CBRNE threats as a preventive measure can be done from distance or near the threat. For example, toxic clouds can be detected from a several kilometers distance with hyperspectral technology, whereas explosives, such as IEDs, HMEs and UXOs are mainly recognized near the suspicious object. When an explosion or other kind of release of lethal threats has already taken place, the presence of toxic substances needs to be detected as the first thing for protecting rescue personnel and survivors. Detection is usually made with close range measures. Unlike in industrial and traffic accidents, in intentional violent acts toxic substances are not always known when they have been released in the environment. With unknown substances it is difficult to make rescue plans and forecast the spread of the threat, and even the identification of various compositions may be difficult. Chemical analysis of mixtures will therefore be made afterwards, even though it would be urgent to identify them immediately.

After toxic substances have been spread, it is urgent to locate and define contamination in the location. This is more than just detecting the presence of toxic materials, and with all detectors it is not possible. Many chemicals evaporate, but they may leave traceable degradation products in the

environment. Sometimes the polluted area is too wide for detailed inspection or it cannot be approached due to hard environmental conditions. Precise spots of contamination like biological agents may also be too small to be found. Detection is needed also for verifying the possible usage of prohibited substances like CWAs, and for revealing a possible crime. In a suspected crime scene every detail is a potential forensic evidence, and before all necessary samples have been collected, principally no one should enter the scene by any means which touches the ground or any other surface, or which causes any other changes at the place. However, in CBRNE incidents rescue needs to be started immediately, and with that a lot of evidence may be destroyed. Investigation and collecting evidence may also not be possible without entering the site by foot or by using robots or other kinds of ground vehicles. Defining contamination, verification and forensic investigation need to be carried out primarily with close range measures.

To summarize key requirements for CBRNE detection, the methods should

- be able to detect and identify CBRNE substances without touching and taking samples,
- be able to detect substances both at a close range and remotely from varying distances,
- be usable both in the laboratory and in the field environments,
- be capable for direct and remote human operation,
- be capable for stand-off operation without human operator,
- be operable by manned/unmanned ground vehicles and robots,
- be operable by airborne UAVs and manned helicopters and planes,
- be able to define contaminated areas,
- be able to take digital images of the CBRNE traces and contamination with the information of the chemical constitution of the substances and store them for later use, and
- be able to make alerts for the detected threats.

No other than hyperspectral detection technology is able to fulfill all these requirements. For the CBRNE detection two of the requirements are critical: one should be able to detect and identify substances without touching and taking samples, and without having a contact on the ground or other surfaces in the place. These requirements together determine that detection needs to be done by hyperspectral technology and that sensors need to be operated from distance by drones.

2 Hyperspectral detection of explosives and toxic chemicals

In this research [1], the feasibility studies for detecting explosives with hyperspectral technology were made by carrying out explosion tests with various mining and military explosives, and by detecting pre- and post-blast traces with high quality hyperspectral imaging devices [2]. Explosion tests were made outdoors in a restricted military testing area with the Finnish Police and the Finnish Defence Forces. Samples were collected by a forensic investigator of the police and results were analyzed indoors with three hyperspectral cameras in VNIR (400-1000 nm), SWIR (970 – 2500 nm) and MWIR (2000 – 6000 nm) wavelength areas [3]. The results were also confirmed with a high quality spectrometer [4]. The pre-blast samples of pure explosives were prepared on cotton and post-blast residues were collected on ten materials which are presented in Figure 2.1.

Pre-blast samples of all tested explosives as pure substances were detected successfully with all three hyperspectral cameras except for one military explosive, which was not detected with the VNIR camera. Post-blast residues were found best for TNT, which deflagrated in the tests. The charge contained 200 grams of explosive material. With the spectrometer TNT residues were found in eight of ten samples (laminate could not be measured and possible traces on plastic carpet were washed out by melting snow). TNT residues were also found on cotton with all VNIR, SWIR and MWIR type of hyperspectral cameras, and in other samples randomly. Positive findings of TNT

residues a cotton fabric are marked with red by the hyperspectral analyzing software in Figure 2.2. Residues were detected on a fabric which was placed 1 m from the explosive charge as presented in Figure 2.1. Residue findings should be confirmed statistically with a larger number of tests. Detection of residues would also be more productive in a dry weather without snow and rain.

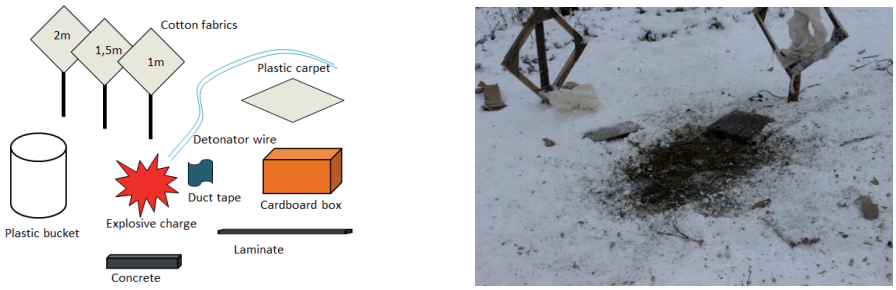


Figure 2.1: Research installation and post-blast image of explosion tests

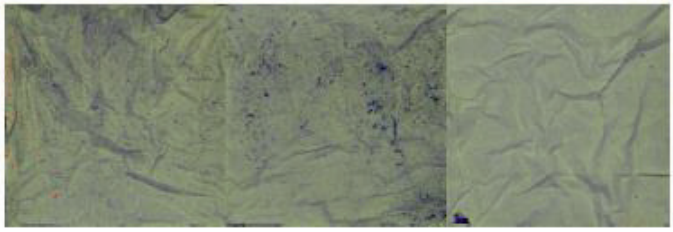


Figure 2.2: A hyperspectral image of the detected TNT residues on cotton marked with red (left)

Feasibility tests were also made for detecting several chemical warfare agents with a hyperspectral technology. A 25 µl drop of all samples were measured on glass with SWIR, MWIR and LWIR (8000-12000 nm) [3] types of hyperspectral cameras in a fume cupboard in the laboratory of the Finnish Institute for Verification of the Chemical Weapons Convention Verifin. Characteristic features were detected for most of the chemicals with all of the three cameras. Some of the MWIR and LWIR measurements however failed because the preferred light source could not be used in the fume cupboard. One sample evaporated before measuring. Reflectance spectra of capsaicin and chloropicrine measured with SWIR type of hyperspectral camera are presented in Figure 2.3.

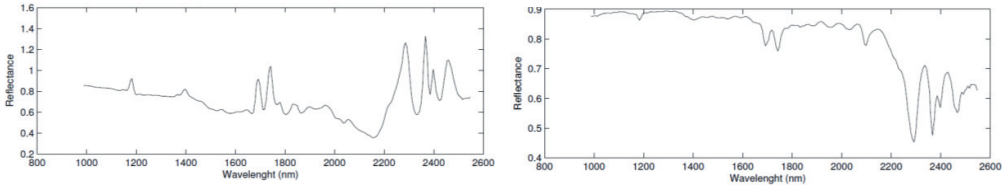


Figure 2.3: Examples of SWIR reflactance spectra of capsaicin (left) and chloropicrine (right)

3 Hyperspectral investigation with drones

The tests of airborne hyperspectral investigation of a CBRNE site were made as a technical test for drone based imaging in a restricted testing area of Oy Forcit Ab. A simulated CBRNE site was created on the ground with several samples of explosives and blood. Samples were imaged with a small hyperspectral camera which was operated remotely with a lightweight drone. The remote control device, drone and small hyperspectral camera are shown in Figure 3.1. The drone was selected among fixed-wing, helicopter and quadcopter types of UAVs. A quadcopter was chosen because it is able to fly flexible routes at different heights and stay still in the air. The desired

imaging device for the test would have been a small hyperspectral IR camera. As that was not available for the tests, a small VIS type of hyperspectral camera was used instead [5]. It was not expected to be able to detect explosives, but the wavelength should be able to detect blood.

Figure 3.1: Hyperspectral imaging with drone

The test design of the simulated CBRNE site with explosives and blood samples is presented on the left in Figure 3.2. Identical samples were prepared on the sand, asphalt and grass. On the upper row on each type of the ground there are 11 samples of different explosives, and on the second row blood from three different donors. The third row is a reference of each type of ground, and the three squares below are color references for white, grey and black. A hyperspectral image of the test situation is shown on the right in Figure 3.2.

Figure 3.2: Imaging design and a hyperspectral image of airborne CBRNE detection tests

Airborne hyperspectral detection tests were designed to be conducted at a sunny, dry and calm weather, and all materials and people were reserved according to weather forecasts. Sunlight was needed for the illumination of hyperspectral imaging and dry and calm weather for flying the drone and protecting samples. Despite of careful planning, an unexpected thunderstorm came up and airborne imaging had to be carried out in a condensed schedule in a cloudy and windy weather.

The drone was flown with the camera below tree tops in 16 – 24 meters. In its normal use in agriculture for imaging forests and fields the tested camera would have produced the hyperspectral image of the inspected area with a computer software from a mosaic of plenty of single images. In these tests all samples were caught within one image, and no processing was needed for the mosaic of several pictures. Due to the wind blasts and clouds the quality of imaging results was weakened. Imaging should also have been made lower, but the drone could not be brought very close to the ground because it needs free space in all sides. There is also a risk that with very close imaging distances the turbulence of the rotors will corrupt the investigation site.

The hyperspectral image in Figure 3.2. shows that the tested VIS type of camera has hardly detected half of the samples which were prepared on the asphalt on the ground. Samples on the sand and

grass have soaked in the ground and cannot be seen in the hyperspectral image with a human eye. In the software analysis of the hyperspectral data of this camera the hyperspectral detection and unmixing could not be made satisfactory for explosives and blood. With an IR camera and more favorable weather conditions chemical spectra would most likely be produced for most of the tested samples.

4 Conclusions

The laboratory tests show that CBRNE substances like explosives, explosive residues and chemical warfare agents can be detected and distinguished in controlled environment with hyperspectral technology. Detection is dependent on the wavelength area of the camera. The identification of substances requires a stored reference of the sample in an identical form. Minimum limit for the detection was not defined. The explosive charge for TNT in the tests was 200 g, and sample size for chemical agents 25 µl. Also the detection of CBRNE samples in field conditions from an airborne drone may succeed, when a right kind of hyperspectral camera is being used and when also other environmental conditions for imaging are fulfilled. The weather, light and steadiness of the camera in the drone are critical for the success and quality of imaging.

Also the usage of drones is dependent on weather conditions, and the type of drone needs to be defined according to the camera which is being used. Many of the current commercially available hyperspectral cameras are bigger and heavier than what was used in this study, and they a mainly designed to be used in a manned aircraft. If they are used in UAVs, they require bigger and stronger drones. Bigger drones with heavier loads also require more space for operating, and with a heavier load they are likely not very capable for precision imaging. Bigger rotors of the drone may also cause more turbulence in the investigation site and thereby spread contamination or distort forensic evidence.

When the camera, drone, weather and other technical and external conditions are satisfactory, also a hyperspectral analyzing software is needed for producing usable detecting results. Detection may refer to discovering latent agents and marks, distinguishing different substances or to the identification of chemical compounds. When spectral references of the chemicals are made in the laboratory, full identification may not necessarily succeed in uncontrolled environments, if chemicals cannot be distinguished from the substrate with an analyzing software. Even in that case contamination may be discovered and defined with the hyperspectral technology.

References

[1] SpeCSI Solutions - Hyperspectral Solutions for Crime Scene Investigation -project, University of Jyväskylä, Dept. of Mathematical Information Technology, Finland, funded by Tekes, 2013 –2014

[2] Kuula, J., Rinta. H., Pölönen, I., Puupponen, H-H., Haukkamäki, M., and Teräväinen, T. (2014) Detecting explosive substances by the IR spectrography. SPIE Proceedings 9073, Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Sensing XV, 90730Q (10 June 2014), Baltimore, USA

[3] http://www.specim.fi/index.php/products/research/spectral-cameras/vis-vnir; http://www.specim.fi/index.php/products/research/spectral-cameras/swir; http://www.specim.fi/index.php/products/research/spectral-cameras/mwir; http://www.specim.fi/index.php/products/research/spectral-cameras/lwir

[4] https://www.bruker.com/products/infrared-near-infrared-and-raman-spectroscopy/ft-ir/ft-ir-accessories/platinum-atr/overview.html

[5] http://www.rikola.fi/site/products/hyperspectral-camera/

[6] http://www.videodrone.fi/en/systems

PIII

USING VIS/NIR AND IR SPECTRAL CAMERAS FOR DETECTING AND SEPARATING CRIME SCENE DETAILS

by

Jaana Kuula, Ilkka Pölönen, Hannu-Heikki Puupponen, Tuomas Selander, Tapani Reinikainen & Tapani Kalenius, 2012

Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI, edited by Edward M. Carapezza, Proc. of SPIE Vol. 8359, 83590P © 2012 SPIE · CCC code: 0277-786X/12/$18 · doi: 10.1117/12.918555

Using VIS/NIR and IR spectral cameras for detecting and separating crime scene details

Jaana kuula*[a], Ilkka Pölönen[a], Hannu-Heikki Puupponen[a], Tuomas Selander[a], Tapani Reinikainen[b], Tapani Kalenius[c], Heikki Saari[d]

[a]Univ. of Jyväskylä, Dept. of Mathematical Information Technology, P.O. Box 35, FI-40014 Jyväskylä, Finland; [b]National Bureau of Investigation, P.O. Box 285, FI-01301 Vantaa, Finland; [c]Central Finland Police Department, P.O. Box 59, FI-40101 Jyväskylä, Finland; [d]VTT Technical Research Centre of Finland, P.O. Box 1000, FI-02044 VTT, Finland

ABSTRACT

Detecting invisible details and separating mixed evidence is critical for forensic inspection. If this can be done reliably and fast at the crime scene, irrelevant objects do not require further examination at the laboratory. This will speed up the inspection process and release resources for other critical tasks. This article reports on tests which have been carried out at the University of Jyväskylä in Finland together with the Central Finland Police Department and the National Bureau of Investigation for detecting and separating forensic details with hyperspectral technology. In the tests evidence was sought after at an assumed violent burglary scene with the use of VTT's 500-900 nm wavelength VNIR camera, Specim's 400-1000 nm VNIR camera, and Specim's 1000-2500 nm SWIR camera. The tested details were dried blood on a ceramic plate, a stain of four types of mixed and absorbed blood, and blood which had been washed off a table. Other examined details included untreated latent fingerprints, gunshot residue, primer residue, and layered paint on small pieces of wood. All cameras could detect visible details and separate mixed paint. The SWIR camera could also separate four types of human and animal blood which were mixed in the same stain and absorbed into a fabric. None of the cameras could however detect primer residue, untreated latent fingerprints, or blood that had been washed off. The results are encouraging and indicate the need for further studies. The results also emphasize the importance of creating optimal imaging conditions into the crime scene for each kind of subjects and backgrounds.

Keywords: Spectral imaging, forensic investigation, crime scene, detection, separation of blood, latent fingerprints

1. INTRODUCTION

The first impression and detecting invisible evidence are one of the most important leads for forensic inspection when arriving at the crime scene for the first time. Critical details should also be identified as soon as possible in order to minimize the time spent on analyzing irrelevant objects. Different subjects and materials should also be separated from each other at a very early stage of the inspection, for example if the examined blood comes from two or more people. While taking and analyzing samples of the inspected targets, the original object should be kept as untouched as possible for preserving the original situation as evidence for the court and further inspection. In many cases, the analysis should also be made immediately before the samples change and degrade in the course of time.

1.1 The competitive advantage of spectral imaging

In the current inspection methods latent targets are usually made visible with the assistance of different treatments and lights, which illuminate a very small area at a time. With these kinds of methods, inspecting a whole room and all items in it is time-consuming, whereas most of the inspected surfaces will not hold anything relevant to the investigation. If something interesting is found, a sample or the whole item will be taken into a laboratory for a closer inspection. The laboratory inspection will then include various kinds of analysis, of which chemical analysis might change the sample permanently.

*jaana.kuula@jyu.fi; phone: +358-40-8053272; fax +358-14-2602209; jyu.fi

Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XI, edited by Edward M. Carapezza, Proc. of SPIE Vol. 8359, 83590P
 · doi: 10.1117/12.918555

In contrast to other current inspection methods, spectral imaging does many of the same things in a shorter time and without touching or changing the inspected target. Depending on the configuration, spectral imaging may be utilized both in a laboratory and at the crime scene, of which both alternatives offer potential advantages for the forensic inspection. When spectral imaging is being used for screening the crime scene, also a great share of the analysis may be done there. Only the most critical items need to be taken into a laboratory for a deeper analysis, which will save time and speed up the performance of the whole process. In all forensic cases, the use of spectral imaging and all of its configurations are however not necessary or useful. Therefore one needs to be aware of which kinds of cases they are suitable for.

Many of the previous research support using spectral imaging in forensic inspection. To select some that are related to this research, for example Malkoff, D. and Oliver [1] refer to portable sensors in crime scene investigations. Since that especially Saari et al. [8], [9], [10] have contributed to the development of small and portable spectral imaging devices. Referring to the spectral analysis of certain kinds of samples which are tested in this study, for example Flynn et al. [2] have studied the analysis of multi-layer paint chips with hyperspectral technology. Several researchers have also contributed to the analysis of blood in its various forms. For example, Dowler [3] has studied the detection of blood, and Payne, G. and Langlois, N. [4] have specialized in studying bruises and ageing of blood. This analysis deals also with the separation of blood and other elements (bile). The detection of latent fingerprints by spectral imaging has been covered thoroughly by Tahtou et al. [5]. The article deals also with the question of detecting latent marks on challenging surfaces.

1.2 Forensic research performed by the University of Jyväskylä

The University of Jyväskylä is currently conducting a project together with the Central Finland Police Department and the Finnish National Bureau of Investigation for testing alternative spectral technologies for the detection and separation of forensic details at an assumed crime scene. The first tests were run with three different types of spectral cameras from two manufacturers. These were VTT's 500-900 nm wavelength VNIR camera [9], [10], Specim's 400-1000 nm VNIR camera [11], and Specim's 1000-2500 nm SWIR camera [12]. Spectral images were then analyzed with several kinds of mathematical algorithms for revealing the actual results of the imaging. The tests covered five different subjects which often appear but may not always be easily found at a typical murder scene or in a place of a violent burglary. These subjects were various forms of blood, gunshot residue, primer residue, fingerprints, and traces of paint, for example left by some tool that has been used in the crime.

The tests were performed indoors in plain conditions and no special forensic methods were used during the study. Additionally, the samples were not treated with any kinds of special lights or chemicals before carrying out the tests.

During the examination, slightly visible subjects like traces of paint and gunshot residue were quite easily detected with a visual inspection and near infrared cameras. These types of cameras could also separate some relevant details of the same subjects like the areas of different kinds of paint in the same objects. The same cameras could also separate burnt gunshot residue from the unburned gunpowder. The VNIR cameras could, however, not reveal subjects which are not visible for the human eye.

The infrared camera performed better with blood, which was tested in three different forms. There were dry blood stains on a ceramic plate, a mixture of four different kinds of blood absorbed in a darkish piece of cloth, and invisible trace of blood that had been wiped off a table with water and some purifying agents. The infrared camera could detect the blood which was absorbed in a piece of darkish cloth. The same camera was also able to separate the four different samples of blood, which were mixed into a same stain and absorbed in a piece of darkish cloth. Two of the samples were from two different males and one female, and one from cattle. However, the invisible subjects like fingerprints, primer residue, and the samples of blood that had been washed off, were not detectable with the infrared camera. This part of the test should, however, be repeated and improved because there were some distracting reflections of light which may have deteriorated the results in this part of the study. For example, according to Tahtou et al. [5], untreated latent fingerprints may be detected by infrared imaging only on backgrounds that are absent from interferences in the C-H bonds.

The results indicate that spectral imaging is a potential technology for revealing latent subjects at the crime scene and for separating relevant details from other subjects and materials. One should, however, be quite precise with choosing the right wavelength for each material being examined because all wavelengths do not reveal all subjects. Also the quantity of inspected materials and the concentration of liquid matters will affect the imaging results. False results may also occur when the used illumination method is not in balance with the inspection scene, camera, and target, and if there are some other external factors which affect the quality of imaging. Detecting latent marks may also be very critical with the surface on which the marks are printed and they may not be found without using some additional methods and treatments

like fluorescent lights or chemical fuming. While evaluating the economy of using spectral imaging at the crime scene, additional treatments will increase the inspection time compared with the detection and analysis of untreated marks. If, however, treatments are necessary for the detection and separation of latent marks, the grounds for using spectral imaging come from the other values of spectral analysis per se.

2. THE RESEARCH SETTING

Spectral technology is currently being used for forensic investigation purposes in laboratory environments, for which for example ChemImage Corporation has commercial applications [6]. However, the usage is not extremely widespread yet and additional research might be useful for proving its overall efficiency and impact on the police work. In this study it is assumed that spectral technology will save costs in forensic inspection and that those savings come both from the inspectors' work and from the laboratory work. Savings in the forensic inspectors' work do not however come primarily from using spectral technology in the laboratory, but from using it at the actual crime scene. Final advantages would come from reducing the lead time of inspection and analysis at the crime scene and in the laboratory, and from increasing the percentage of solved cases of all crimes and the number of solved cases within a certain period of time.

2.1 Requirements for spectral technology in the crime scene investigation

So far, there is not much reported material available of using spectral technology in the policemen's field work. For implementing spectral technology widely in this kind of work, the laboratory technology should first be developed to be compact enough so that it could be taken easily into any kind of crime scene. Regardless of the small size, the technology should reach most of the laboratory equipment's qualities so that it could easily find critical details. For being competitive and useful, it should also be able to find most of the same details which can be found with other inspection methods. It only should do it faster and better. At its best, spectral technology should be able to detect details which cannot be found with traditional methods. Also, it would be able to analyze findings without touching and changing the sample, which is a different feature compared with some other inspection methods.

2.2 Arrangements for performing the tests at an assumed crime scene

In this research, spectral technology is being tested in an assumed field environment at a proposed crime scene. For carrying out the tests, a special research setting was created for searching for latent traces of an assumed crime and for separating relevant details with different portable spectral cameras. Cameras were also equipped with some special accessories in order to enable their convenient use at the crime scene. Accessories were various stands, holders, and illuminators, but not special forensic investigation tools like fluorescent lights.

Referring to the known potential of spectral technology in forensic [1], [5], [6] and other fields like medicine [7], there were positive expectations of being able to detect invisible traces at the assumed crime scene with spectral cameras. It was, however, not known, which subjects particularly would be found, in which concentrates, and with which wavelengths. Different subjects and materials were also expected to be separated from each other, if they were mixed or absorbed into another material.

The technical potential of the spectral technology was planned to be assessed by systematic search. For carrying out the tests, a representative selection of different samples was chosen for the study, all of them representing an assumed crime scene. All samples were prepared and provided by the forensic inspectors of the Central Finland Police Department and by the personnel of the forensic laboratory of the National Bureau of Investigation.

Furthermore, three different types of spectral cameras were selected for the tests in order to find out which kinds of cameras would find the wanted details best. Two of the cameras were visual inspection and near infrared VNIR cameras and one short-wavelength IR camera. VNIR cameras were from two different manufacturers. The 500-900 nm camera was manufactured by VTT Technical Research Centre of Finland and the 400-1000 nm camera by Specim – Spectral Imaging Ltd, also located in Finland. The SWIR camera was manufactured by Specim Ltd.

The assumed crime scene was an ordinary office room, which presented a hypothetic violent burglary scene. Selected seven kinds of samples were brought into the scene, some of them being invisible for the human eye. There were also examples of washing off the trace. After imaging all the samples, spectral images were analyzed with mathematical algorithms, which then gave the actual results of the spectral imaging.

3. CARRYING OUT THE TESTS

The tests were carried out by bringing the selected samples to the assumed crime scene and by imaging them systematically with three different spectral cameras. The whole test consisted of a couple of separate imaging sessions.

3.1 Preparing the tested cameras and samples

Different cameras were used in the same imaging sessions. The cameras needed different accessories and other arrangements depending on the sample. The tested samples were not treated in any way before or during the study. A picture of VTT's VNIR camera without accessories is shown in Figure 1.

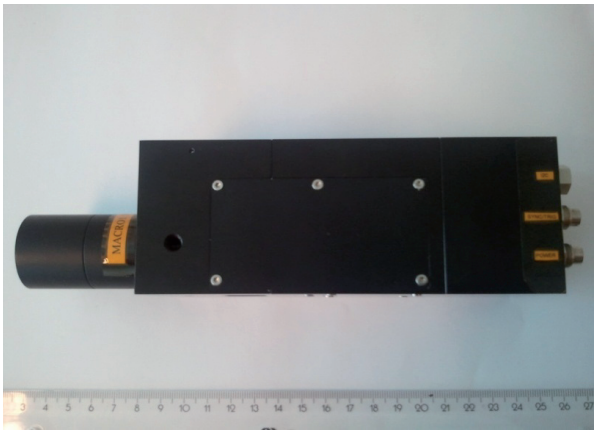


Figure 1. A picture of VTT's 500-900 nm wavelength VNIR spectral camera, which was one of the three cameras used in the tests.

The selected samples presented typical details that could be found at a violent burglary scene. These were:

- a drop of blood, dried on a ceramic plate
- invisible blood, washed with detergents and wiped off a table
- samples of four kinds of human and animal blood, mixed together and absorbed into a darkish denim fabric
- mixture of burnt and unburned gunpowder on a white paper
- invisible primer residue on an adhesive disk
- latent fingerprints on a clear plastic bag
- samples of three kinds of paint and filler, mixed on small pieces of wood.

The samples contained both easy and challenging targets in order to test the capability of different cameras and algorithms. The most challenging targets were those which were not visible for the human eye (latent fingerprints, primer residue) and which had been wiped off by using some detergent for destroying the trace (blood). Also the sample of four different bloods was quite challenging to be separated, and usually tests are performed with one or two types of blood at one time. In this part of the tests the challenge for hyperspectral imaging was to separate the mixed blood samples of two males, one female, and cattle from a single stain which was absorbed into a piece of darkish cloth. The blood stains of humans had been created from a fresh drop of blood. The animal blood had been frozen, and it was thawed before preparing the samples. The concentration of frozen blood may have been slightly weaker than what it is in fresh blood. It had, however, been frozen fresh without any additives (for example coagulation inhibitors) which makes it quite comparable with the fresh animal blood.

The sample of gunshot residue was quite rough and likely to be found and separated by spectral imaging. The primer residue was finer and more difficult to find. It was attached to an adhesive disk and the residue was not visible for the human eye. Also, the fingerprints on a clear plastic were not visible for the human eye. The last sample was a mixture of three different kinds of paint and filler which were layered on small pieces of wood. All of the subjects could not be seen with a human eye.

3.2 The course of the test

There were two kinds of performance tests for the cameras. The first question was whether they can detect such small particles that could not be observed with a human eye or which are hidden or destroyed on purpose. The second question was whether the cameras can separate subjects and materials if they are mixed, for example if various liquids are blended together, or if the liquids are absorbed into some texture, such as fabric.

Samples were at first photographed with an ordinary digital camera as reference pictures, and then imaged with the two different VNIR cameras and with the SWIR camera. If positive results were gained with VNIR cameras, SWIR imaging was not necessarily done. After imaging the samples, final results were created by analyzing spectral images with different types of mathematical algorithms. For enabling the afterward tracing of imaging sessions, all samples and images were named, classified, and registered on the project documentation. Shootings consisted of several sessions.

In some cases there were some distractions during the shootings, which may have affected the results negatively. Distractions were mainly caused by unintended reflections of light. The best positive results (separation of blood) were cross-checked and repeated twice.

4. RESULTS

The results in the tests were positive and promising but not fully successful. With some samples there were also some external factors which may have affected the results negatively. In its entirety, the whole series of tests was successful and gives support for further research.

4.1 Overview of the results

The key results of all the tested samples are presented in Table 1. The detection of the searched details and items is indicated by 'Found' or 'Not Found'. If the sample has not been imaged by a certain camera type, it is indicated by 'Not imaged'. Samples have not always been imaged with the SWIR camera if a positive result has been reached with the VNIR. The separation of mixed and absorbed items is indicated by 'Separated' or 'Not separated'. Distractions during the imaging are also indicated in the table.

Table 1. Outline of samples and results.

	RESULTS WITH VNIR CAMERAS		**RESULTS WITH SWIR CAMERA**
SAMPLE	**VTT VNIR 500-900 nm**	**Specim VNIR 400-1000 nm**	**Specim SWIR 1000-2500 nm**
BLOOD			
- Dried blood on a ceramic plate	Found	Found	Not imaged
- Invisible blood, wiped off a table	Not found, noise	Failed, reflections	Not possible with equipment available
- Mixture of four types of blood, absorbed in a darkish cloth	Found, not separated	Found, not separated	Found and separated 4 different types of blood
GUNSHOT RESIDUE			
- A mixture of burnt and unburned gunpowder on a white paper	Found and separated	Not imaged	Not imaged
PRIMER RESIDUE			
- Invisible residue on an adhesive disk	Not found	Not found	Not imaged
FINGERPRINTS			
- Invisible fingerprints on a clear plastic bag	Not found	Not found	Failed, reflections
PAINT			
- Three different paints and fillers mixed on a piece of wood	Found and separated 3 of 4 mixed samples	Found and separated 3 of 4 mixed samples	Found and separated 4 mixed samples

4.2 Results in detecting items

When detecting interesting items, the best results were obtained in finding blood and paint. Of these single blood stains were found with all of the three tested camera types. All cameras could also find the paint and gunpowder. (Gunpowder was imaged only with 500-900 nm VNIR, but it was evident that it would be found also with the other cameras.) These samples were quite easy to find, so with these kinds of items it is more critical whether the cameras are able to separate different items from the mixed and absorbed samples.

None of the cameras could however detect items which were invisible for the human eye. The invisible items were the blood which had been wiped off a table by using some detergents during the cleaning, primer residue which was attached to an adhesive disk, and latent fingerprints on a clear plastic bag. The trace of blood had been destroyed on purpose and in the imaging of primer residue and fingerprints on a clear base there were some reflections of light which may have distracted the imaging process. Due to these reasons the detection of these invisible and latent samples was very challenging, and it is not surprising that no traces could be found.

It is however possible that in more favorable conditions the SWIR camera might be able to detect invisible blood and other traces invisible for the human eye. The detection of the destroyed trace is dependent among other things on the cleaning method, usage of detergent, and the strength of the trace which has been left on the scene after the cleaning. The detection of latent items might also be possible on some other than a clear plastic base, and with some other wavelengths and better spectral resolution. Referring to Tahtou et al. [5], especially untreated latent fingerprints might be detected by imaging the spectral intensity at a single frequency (non-chemical imaging) or imaging them with infrared frequencies on backgrounds that are absent from interferences in the C-H region (chemical imaging). Tahtou et al. have also imaged latent fingerprints by treating them first with Ethyl Cyanoacrylate fuming [5]. This will make latent prints imageable, but increasing these kinds of additional processes in the work load of the investigators might increase the total time spent on investigation at the crime scene and make the whole examination process more complicated. One must then evaluate the value of the quality of inspections compared with the time spent on each investigation, and decide between the appropriate research methods accordingly. To summarize, latent marks and residue are subjects where further research is in any case necessary.

4.3 Results in separating items

In separating mixed and absorbed items, the cameras were expected to detect four different kinds of blood which were mixed into the same stain and absorbed into a darkish cloth. Also the burnt and unburnt gunpowder were supposed to be separated, as well as the three kinds of paint and filler which were on the same pieces of wood. The different types of blood and the three types of paint and filler could not be separated with a human eye.

The VNIR cameras could separate the burnt and unburnt gunpowder, as well as three of the four items of paint and filler on the small pieces of wood. The gunpowder was quite easy to observe and the burnt and unburnt grains were clearly seen in spectral images. The VNIR image of separating burnt and unburnt gunpowder is shown in Figure 2.

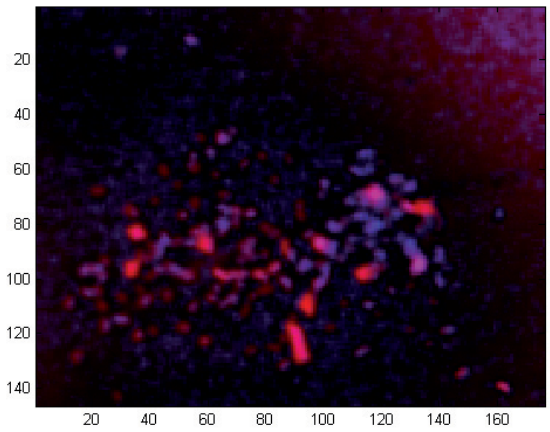


Figure 2. Visualization of separating burnt and unburnt gunpowder based on a processed VNIR datacube.

While examining the painted pieces of wood with VNIR cameras, spectral imaging could separate three of the four items on the wood. The two identified items were green and white paint, whereas the third item which was identified as one, consisted of filler and a black marker pen. The VNIR image of separating three types of paint and filler is presented in Figure 3.

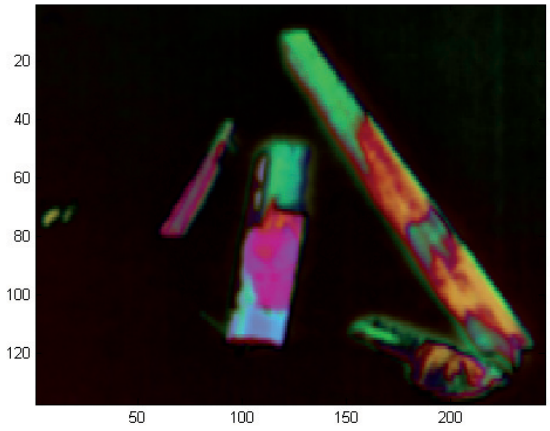


Figure 3. Visualization of the separation of mixed paint and filler on pieces of wood based on a processed VNIR datacube.

The SWIR camera succeeded best in separating mixed and absorbed items, and as the best result of the whole test it could separate the four types of blood which were mixed in the same stain and absorbed in a piece of darkish cloth. The SWIR camera could also separate all four materials on the pieces of wood. Compared to VNIR cameras, SWIR camera performed better in separating the filler and the black marker pen. While the VNIR camera recognized these two items as one, the SWIR camera detected the trace of the black marker pen different from the filler. A processed SWIR PCA RGB

composite image of the mixed paint and filler with three principal components is shown in Figure 4 and a SWIR pseudo color image of the same target in Figure 5.

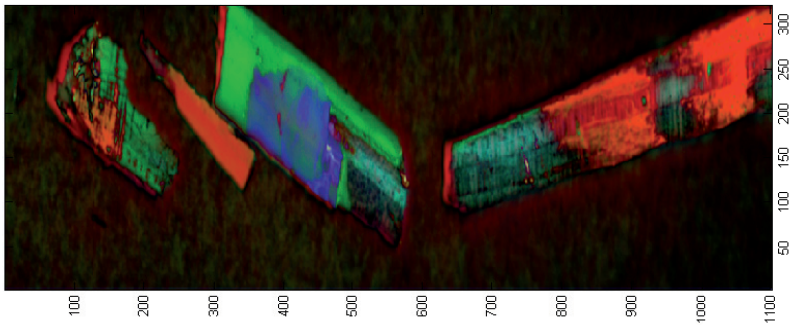


Figure 4. A processed SWIR PCA RGB composite image with three principal components of the separation of mixed paint and filler on pieces of wood.

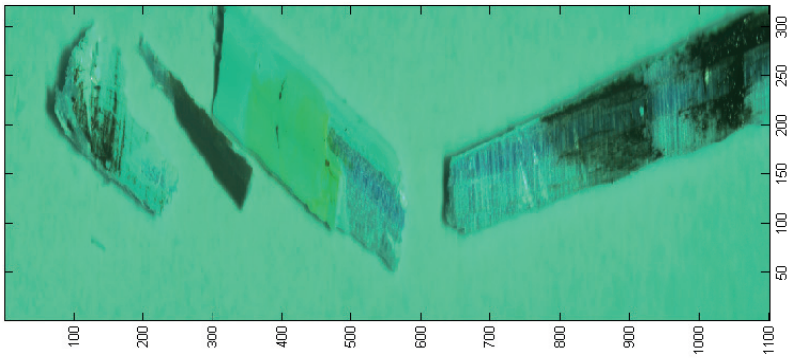


Figure 5. A SWIR pseudo color image of the separation of mixed paint and filler on pieces of wood.

Figures 6-8 present the separation process of four types of blood with digital, VNIR, and SWIR cameras. Figure 6 shows the reference picture of the stain which contains blood from two different males, one female, and one cattle animal. From the picture one cannot tell how many persons' or animals' blood there is in the same stain. In Figure 7 there is a visualization based on a processed VNIR datacube of the same sample, and that cannot indicate how many persons' or animals' blood there is in the stain, either.

The full separation of the four blood types is shown in Figure 8. The successful result is based on imaging the stain with the SWIR camera and on processing images with the right kind of algorithms. Figure 8 presents the visualization of the examined stain based on a processed SWIR datacube.

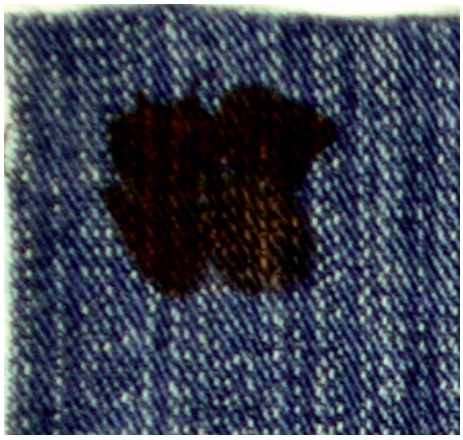


Figure 6. Reference picture of four different types of blood mixed in the same stain and absorbed in a denim cloth.

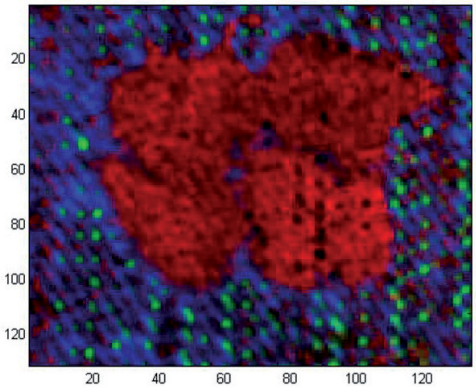


Figure 7. VNIR image of four different types of blood mixed in the same stain and absorbed in a denim cloth.

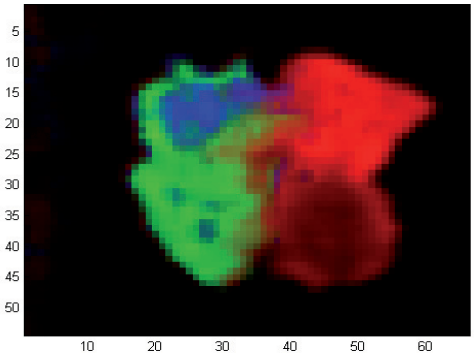


Figure 8. Visualization of four different types of blood mixed in the same stain and absorbed in a denim cloth based on a processed SWIR datacube.

5. SUMMARY AND CONCLUSIONS

In the University of Jyväskylä's research project the aim is to bring spectral imaging technologies from the laboratory into the crime scene as the policemen's help in forensic inspection work. The motivation for using spectral imaging at the crime scene is to detect and separate relevant items better and faster compared with other inspection methods. Improved and faster inspection should also cut down the time spent in examining each case of crime. As the result of more qualified detection and separation of relevant details, faster inspection times as well as the overall percentage of solved cases and the number of solved cases within a certain period of time should increase.

Within this study, three kinds of spectral cameras were tested for detecting and separating interesting items at an assumed crime scene of a violent burglary. The tests were run with VTT's 500-900 nm VNIR camera, Specim's 400-1000 nm VNIR camera, and Specim's 1000-2500 nm SWIR camera. All of these cameras were used for detecting and separating samples which were related to the assumed violent burglary. The tested samples were the following: dried blood on a ceramic plate, invisible blood which had been wiped off a table with detergents, a sample of four types of human and animal blood which were mixed into the same stain and absorbed into a darkish fabric, a mixture of burnt and unburnt gunpowder, primer residue, latent fingerprints on a clear plastic bag, and a sample of three kinds of paint and filler on small pieces of wood.

The tests showed that the VNIR cameras can detect visible samples and separate some items which are mixed together. For example, VNIR cameras can separate various types of paint on the same object. However, in these tests VNIR cameras could not detect or separate items that are invisible for the human eye. Additional research is therefore recommended on the detection of very small particles and latent objects.

The tests also showed that the SWIR camera is better than the VNIR cameras in detecting and separating various items. For example, unlike VNIR cameras the SWIR camera was able to detect and separate four different types of blood which were mixed into the same stain and absorbed into the darkish piece of cloth. The SWIR camera could also detect and separate the three types of paint and filler on the piece of wood. Based on these results it is suggested that additional research would be done on the detection and separation of blood with the spectral technology.

The results of the study are encouraging and it is suggested that additional research will be made on developing the use of spectral imaging in the forensic field. Especially the equipment and research methods related to the use of spectral technology at the crime scene are worth studying further. The spectral imaging technology especially in the VNIR spectral range will lead to devices which are similar in size to compact digital cameras [13]. Improvements may also be achieved with the laboratory equipment. As a conclusion, development on both the laboratory equipment and the field inspection methods will reduce the workload of forensic inspectors, policemen, and criminal laboratory workers as well as enable solving more criminal cases in a shorter period of time.

6. ACKNOWLEDGEMENTS

We would like to acknowledge Tekes – the Finnish Funding Agency for Technology and Innovation and the University of Jyväskylä for funding this research project called *Crime Scene Investigations by Spectral Imaging –SpeCSI* (2623/31/2011). TEKES has funded 60 % and the University of Jyväskylä 40 % of the project.

REFERENCES

[1] Malkoff, D. and Oliver, W.R., "Hyperspectral imaging applied to forensic medicine", Proc. SPIE 3920, 108 (2000)

[2] Flynn, K., O'Leary, R., Lennard, C., Roux, C. and Reedy, B. J., "Forensic Applications of Infrared Chemical Imaging: Multi-Layered Paint Chips", J Forensic Sci, July 2005, Vol. 50, No. 4

[3] Dowler, S. W., [Applications of Hyperspectral Imaging Techniques to Forensic Image Analysis], A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering, The University of Auckland (2010)

[4] Payne, G. and Langlois, N., "Applying visible hyperspectral (chemical) imaging to estimate the age of bruises", *Med Sci Law July 2007 vol. 47 no. 3 225-232*
[5] Tahtouh,M., Kalman, J. R., Roux,C., Lennard,C. and Reedy,B.J., "The Detection and Enhancement of Latent Fingermarks Using Infrared Chemical Imaging", J Forensic Sci, Jan. 2005, Vol. 50, No. 1
[6] "Forensic analysis", www.chemimage.com/markets/forensics/
[7] Seong G. Kong, S. and Park, L., [Hyperspectral Image Analysis for Skin Tumor Detection], Springer (2009)
[8] Saari, H., Aallos, V., Akujärvi, A., Antila, T., Holmlund, C., Kantojärvi, U., Mäkynen, J. and Ollila, J., "Novel Miniaturized Hyperspectral Sensor for UAV and Space Applications", Proc. SPIE 7474 (2009).
[9] Saari, H., Aallos, V., Holmlund, C., Malinen, J., Mäkynen, J., "Hand-Held hyperspectral imager," Proc. SPIE 7680, 76800D (2010)
[10] Saari H., "Spectrometer and interferometric method", US Patent US 8,130,380 (Mar. 6, 2012)
[11] Data sheet of Specim VNIR Spectral Camera www.specim.fi/media/specam-datasheets/ps-spectral-camera-v1-11.pdf
[12] Data sheet of Specim SWIR Spectral Camera www.specim.fi/media/specam-datasheets/swir-specam-ver3-11.pdf
[13] Antila, J., Mannila, R., Kantojärvi, U., Holmlund, C., Rissanen, A., Näkki, I., Ollila, J:, and Saari, H., "Spectral imaging device based on a tuneable MEMS Fabry-Perot interferometer", to be published in Proc. SPIE 8374, 8374-15 (2012).

PIV

THE CHALLENGES OF ANALYSING BLOOD STAINS WITH HYPERSPECTRAL IMAGING

by

Jaana Kuula, Heikki Rinta, Ilkka Pölönen & Hannu-Heikki Puupponen, 2014

Sensing Technologies for Global Health, Military Medicine, and Environmental Monitoring IV, edited by Šárka O. Southern, Mark A. Mentzer, Isaac Rodriguez-Chavez, Virginia E. Wotring, Proc. of SPIE Vol. 9112, 91120W · © 2014 SPIE · CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050180

The challenges of analysing blood stains with hyperspectral imaging

Kuula J.[a], Puupponen H-H.[a], Rinta H.[b], Pölönen I.[a],

[a]Department of Mathematical Information Technology, University of Jyväskylä, Mattilanniemi 2, 40100 Jyväskylä, Jyväskylä, Finland;
[b]Department of Chemistry, University of Jyväskylä

ABSTRACT

Hyperspectral imaging is a potential noninvasive technology for detecting, separating and identifying various substances. In the forensic and military medicine and other CBRNE related use it could be a potential method for analyzing blood and for scanning other human based fluids. For example, it would be valuable to easily detect whether some traces of blood are from one or more persons or if there are some irrelevant substances or anomalies in the blood. This article represents an experiment of separating four persons' blood stains on a white cotton fabric with a SWIR hyperspectral camera and FT-NIR spectrometer. Each tested sample includes standardized 75 μl of 100 % blood. The results suggest that on the basis of the amount of erythrocytes in the blood, different people's blood might be separable by hyperspectral analysis. And, referring to the indication given by erythrocytes, there might be a possibility to find some other traces in the blood as well. However, these assumptions need to be verified with wider tests, as the number of samples in the study was small. According to the study there also seems to be several biological, chemical and physical factors which affect alone and together on the hyperspectral analyzing results of blood on fabric textures, and these factors need to be considered before making any further conclusions on the analysis of blood on various materials.

Keywords: hyperspectral analysis, analysis of blood

1. INTRODUCTION

The forensic and military medicine, forensic investigations and various screenings in the CBRNE field require quick and nonivasive methods for having an overview of the state and constitution of blood and other biological fluids. The hyperspectral analysis is known of its ability make untouched basic analyses of the structure and content of the selected targets. It is, however, unclear whether it would be able to detect, identify and separate small particles in blood and in other body fluids. The small particles may refer to the healthy or abnormal components and structure or to the foreign substances in blood.

In this research the hyperspectral analysis has been focusing on the constitution and structure of blood in order to find out whether two or more people's blood can be separated by hyperspectral technology and in which factors this separation would be based on. If the basic elements and structure of blood could be detected by common hyperspectral technologies, one might assume that also some inappropriate substances and anomalies in blood could be detected with the same technology.

In the earlier study[1] four different blood samples, one from female, two from different men and one from cow, were separated successfully with a 1000-2500 nm SWIR type of hyperspectral camera. It was, however, not revealed, which factor or factors in blood caused the differences for being able to define the samples as different blood.

In this article the earlier study has been repeated with new carefully produced and analyzed blood samples from four people for explaning why different persons' blood shows up different in hyperspectral analysis. In this test the hyperspectral analysis has been supported with an additional analysis of the structure of blood made by professional medical personnel and equipment.

Further author information:
Jaana Kuula: E-mail: jaana.kuula@jyu.fi, Telephone: +358 40 8053272

Sensing Technologies for Global Health, Military Medicine, and Environmental Monitoring IV, edited by Šárka O. Southern, Mark A. Mentzer, Isaac Rodriguez-Chavez, Virginia E. Wotring, Proc. of SPIE Vol. 9112, 91120W · © 2014 SPIE · CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050180

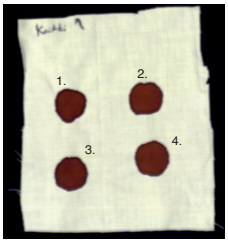


Figure 1. Four persons blood stains on cotton fabric.

The new tests support the earlier findings of being able to separate different persons' blood with hyperspectral analysis. The results also indicate slightly that the erythrocytes might be the explaining factor for the separation of blood. It should, however, be noted that the sample size in this study is small (n=4) and thus no statistically meaningful conclusions can be drawn. Instead, further in the paper we concentrate on describing the utilized analyzing method and on the potential for further study in this subject.

2. METHOD

2.1 Research design and preparation of samples

The tests were started by taking pure blood samples from four healthy volunteers by professional healthcare personnel. The volunteers were about 25-50 years of age, three men and a woman. All were non-smokers and had never used drugs. They also had not eaten, drunk or taken any alcohol in 12 hours before giving blood. In the laboratory a blood count was made on the samples. 8 ml of blood was taken from each volunteer and the blood samples were stored refrigerated for two days before sample preparation. The results from laboratory tests are presented in Table 1 and an image of the tested blood stains on cotton fabric in Figure 1.

Table 1. Measured blood constituents and correlations between identified spectra's mutual spectra angle matrix and distance matrix of measured component.

Blood component	Person 1	Person 2	Person 3	Person 4	Correlation
Leukocytes $*10^9$/l	3.2	6.9	4.9	6	0.32
Erythrocytes $*10^{12}$/l	4.87	4.29	5	5.17	**0.74**
Hemoglobin g/l	153	133	147	146	0.5
Thrombocytes $*10^9$/l	161	268	239	278	0.24
Basophils $*10^9$/l	0	0	0	0.1	0.23
Eosinophils $*10^9$/l	0	0.1	0.1	0.1	0.26
Neutrophils $*10^9$/l	1.8	4.5	2.7	3.9	0.35
Lymphocytes $*10^9$/l	1.2	1.9	1.5	1.4	0.47
Monocytes $*10^9$/l	0.3	0.4	0.5	0.5	0.49

Blood stains were deposited on pieces of cotton fabric. The cotton fabric was selected to present commonplace non-bleached fabric. The base fabric was washed and ironed before the sample preparation took place. Volume of 75 μl was placed on the fabric with automatic pipette and allowed to dry off on rack in normal room temperature. Function of the rack was preventing direct contact between any surface and wet opposite side of the fabric before samples were fully dry. Off-white cotton fabric was chosen to provide a moderate background contrast. Blood stain samples had a diameter of approximately 7 mm on cotton fabric base.

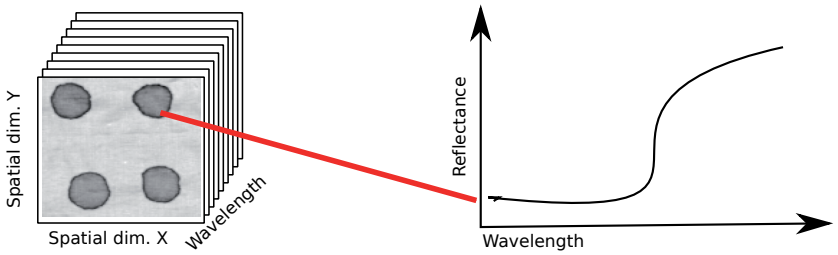


Figure 2. Illustration of hyperspectral image. Spectral image is stack of grayscale intensity images. Each spatial pixel in stack forms reflectance spectrum.

2.2 Hyperspectral imaging and analysis method

As the term indicates, hyperspectral imaging combines spectroscopy with imaging techniques. In hyperspectral data cube each pixel forms spectrum trough data cube as illustetrated in Figure 2. For the imaging we used Specim Ltd's short-wave infrared imager (SWIR), which is capable of capturing spectral data from 1000 to 2500 nm.

In paper[1] we examined various stains and materials, which could be identified at a crime scene. In the study we were also able to separate blood stains originating from three different persons and one animal from each other. The analysis was performed with vertex component analysis[2] and inversion was computed with non-negative least squares algorithm.[3] These algorithms are utilized also in this study.

Basic idea behind vertex component analysis is that imaged spectra are linear mixture of pure spectra, often termed endmembers. Vertex component analysis determines these endmembers from the vertices of the convex hull of measured data points. Method is sensitive to the number of endmembers to be extracted. This number has to be estimated before running VCA.

Spectral angle mapper (SAM)[4]is a method to compare different spectra with each other. It measures spectral similarity by finding the angle (in radians) between reference spectrum $\mathbf{e} = (e_1, e_2, \dots e_L)^T$ and imaged spectrum $\mathbf{s} = (s_1, s_2, \dots s_L)^T$ so that,

$$d_{sam}(\mathbf{e}, \mathbf{s}) = \cos^{-1}\left(\frac{\sum_{l=1}^{L} e_l s_l}{(\sum_{l=1}^{L}(e_l)^2)^{1/2}(\sum_{l=1}^{L}(s_l)^2)^{1/2}}\right),$$

where L is number of wavebands in spectra. Because we are here dealing with four samples it is possible to calculate a distance matrix, through use of SAM to determine degree of difference between each sample spectra.

Because we also had laboratory analysis performed on the blood samples, we can calculate different distance matrices with results from different samples. After this calculation it is possible to compute correlations between these distance matrices to find interpretative factors between the samples. With the correlation information it is possible to draw conclusions about what the potential cause is for the differences in the measured spectra from each blood stain.

2.3 ATR NIR spectroscopy measurements

The near infrared spectral measurements of the blood stain samples on the fabrics were measured on a Thermo Fisher Scientific Antaris II FT-NIR spectrometer using the basic measurement mode (range 10000-4000 cm $^{-1}$/ 1000-2500 nm; resolution 4 $^{-1}$cm and scans 32). Data collection was processed by OMNIC 9 -software and the collected data was processed by TQ Analyst and Microsoft Excel 2010 software. The average spectrum of the samples was a measurement of three replicates.

Measurement results varied depending on the spatial location on the spot. With spectroscopy it was not possible to separate blood stains from each other.

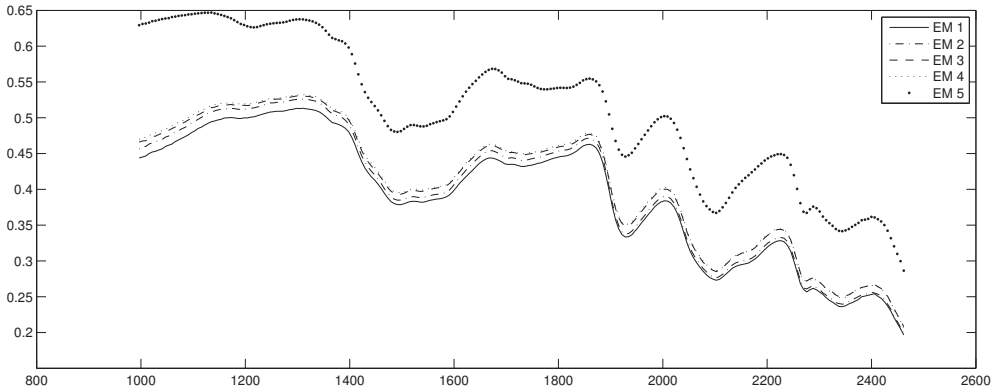


Figure 3. Endmembers inducted with VCA.

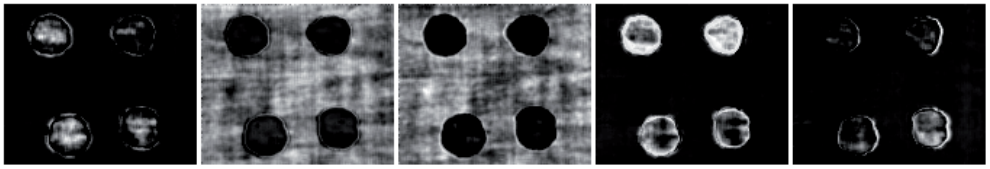


Figure 4. Abundance images of extracted endmembers. VCA fails to discover four different traces. However, it seems that stains on the right side differ from other two.

3. RESULTS

Fully dry blood stains were imaged after a couple of days from sample preparation.

As in Kuula et. al.[1] we strived to repeat the earlier excellent blood stain separation results. In this case, we were less successful. Figure 3 displays extracted endmembers and Figure 4 shows abundance maps calculated for these endmembers. It would appear that stains 2 and 4 have components, which cause them to differ from others.

Next we examined another possible approach. We selected pixels from each stain and calculated average of these pixel spectra to derive a representative single spectrum for each of the four stains. In Figure 5 we see four different spectra, which all differ from each other. It seems that there are slight differences in the relative intensity of the spectra over the whole wavelength range.

If we visually compare known strong wavebands for blood components in Table 2 with calculated mean values for each stain, presented in Figure 5, it seems clear that there are no noticeable peaks which would explain the differences.

Inversion can be calculated also for these spectra. If we add mean value of the background fabric to the group of mean spectra we obtain abundance images that all differ from each other and also give slightly different spatial distribution for each spectrum. This is illustrated in Figure 6.

We are next looking for an explanation as to why these differences appear. We have the laboratory results for the four blood samples in Table 1. One possibility is to examine if distances between these values could correlate with a distance matrix calculated from the mean stain spectra. This is relevant because each value in Table 1 and each mean spectra can be identified with a certain person.

We can build a distance matrix based on spectral angle mapper between these mean value spectra. This

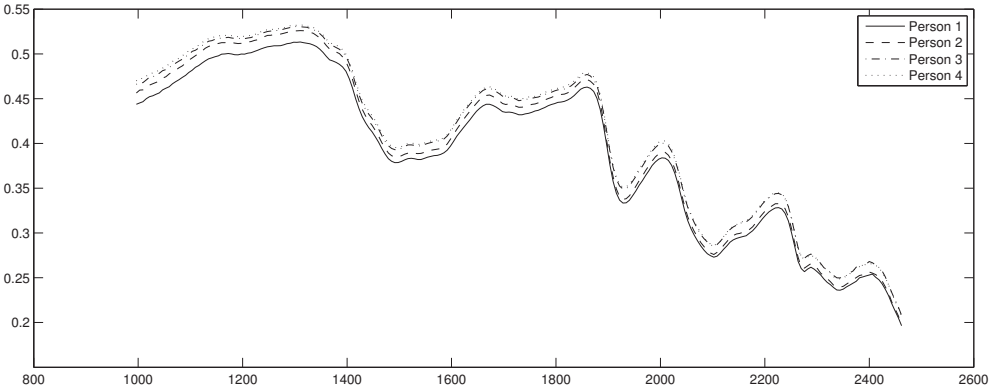


Figure 5. Mean values of the spectra, which are taken from different samples.

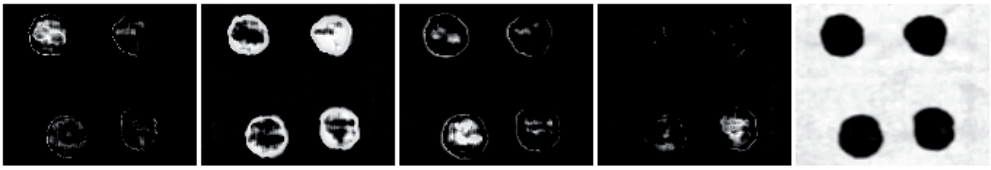


Figure 6. Non-negative least square inversion-provided abundance maps for the mean value spectra.

distance matrix of the four mean blood stain spectra is

$$D_{sam} = \begin{bmatrix} 0 & 0.0051 & 0.0065 & 0.0062 \\ 0.0051 & 0 & 0.0094 & 0.0086 \\ 0.0065 & 0.0094 & 0 & 0.0026 \\ 0.0062 & 0.0086 & 0.0026 & 0 \end{bmatrix}$$

Distance matrices D_{comp} for each component was calculated based on L2-norm. Now correlation coefficient is calculated between D_{sam} and D_{comp} following:

$$r = \frac{\sum_n \sum_m (D_{sam,n,m} - \overline{D}_{sam})(D_{comp,n,m} - \overline{D}_{comp})}{\sqrt{(\sum_n \sum_m (D_{sam,n,m} - \overline{D}_{sam})^2)(\sum_n \sum_m (D_{comp,n,m} - \overline{D}_{comp})^2)}}$$

In the last column of 1 we see these correlations. It seems that highest correlation was with erythrocyte's distance matrix

$$D_{eryth.} = \begin{bmatrix} 0 & 0.3364 & 0.0169 & 0.09 \\ 0.3364 & 0 & 0.5041 & 0.7744 \\ 0.0169 & 0.5041 & 0 & 0.0289 \\ 0.09 & 0.7744 & 0.0289 & 0 \end{bmatrix}.$$

4. DISCUSSION AND CONCLUSION

As Figure 7 illustrates there exists a possibility to distinguish the blood stains from each other. It seems that spectral similarity of mean values of these stains correlates with the amount of erythrocytes in blood. This would seem to be reasonable, as the amount of red blood cells also affects the optical properties of the blood. Greater amounts of erythrocytes would also result in darker and thicker blood. It could be possible to through

Table 2. Typical features expressed by the human blood in SWIR -region.

Wavelength (nm)	Component	Bond
930	Oxyhemoglobin	3. overtone of -CH and -CH2 stretching vibrations
970	Water	Combination of H-O-H symmetric and asymmetric
1454	Water	Combination of H-O-H symmetric and asymmetric
1690	Hemoglobin, albumin, globulin	1. overtone of -CH stretching vibrations
1740	Hemoglobin, albumin, globulin	1. overtone of band at 3477 nm
1940	Water	Combination of H-O-H bending and asymmetric stretching vibrations
2056	Hemoglobin, albumin, globulin	Combination of amide A and amide II or another
2170	Hemoglobin, albumin, globulin	Combination of amide B and amide II or
2170		overtone of amide II
2290	Hemoglobin, albumin, globulin	-CH stretching and deformation combinations
2350	Hemoglobin, albumin, globulin	-CH stretching and deformation combinations

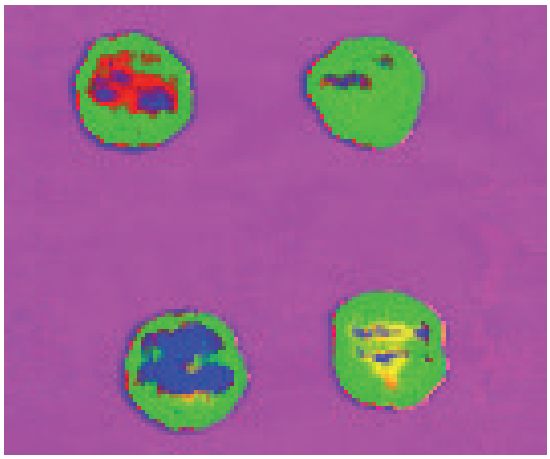


Figure 7. False color illustration of mean value spectra's abundance. There is a visual difference in each stain.

use of hyperspectral imaging to estimate erythrocyte content from blood stains and that way potentially offer an alternative for hemocytometer. At the accuracy level of erythrocytes there might also be a chance to detect other substances and phenomena in blood, althogh they were not available in the samples which were used in this study.

Although these results are interesting, they have not been confirmed statistically due to the small size of the sample. Also some possible sources of error which can affect the results were not eliminated. One of these is the background material. Although waved tightly, a cotton fabric as a basis for highly accurate optical analysis might not be sufficiently homogenous, and therefor there might be a possibility for error, caused by the physical properties of the texture. Imaging instruments might also be capturing geometry, so that if we rotated the samples 90 degrees, would the results remain the same? Based on these tests it seems possible to separate blood stains originating from one person from ones originating from another. However, based on these tests we cannot

be certain on the degree of accuracy the measuring results, so we recommend that the tests would be repeated with a much higher number of samples. Also, as there is a need to detect other anomalies in the blood, further research is needed to confirm whether they can be detected or not.

ACKNOWLEDGMENTS

This research has been funded by the Finnish Funding Agency for Innovation and by the University of Jyväskylä.

REFERENCES

[1] Kuula, J., Pölönen, I., Puupponen, H.-H., Selander, T., Reinikainen, T., Kalenius, T., and Saari, H., "Using vis/nir and ir spectral cameras for detecting and separating crime scene details," *Proc. SPIE* **8359**, 83590P–83590P–11 (2012).

[2] Nascimento, J. and Dias, J., "Vertex component analysis: A fast algorithm to unmix hyperspectral data," *IEEE Transactions on Geoscience and Remote Sensing* **34**(4), 898–910 (2005).

[3] Bro, R. and De Jong, S., "A fast non-negativity-constrained least squares algorithm," *Journal of Chemometrics* **11**(5), 393–401 (1997).

[4] Schowengerdt, R. A., [*Remote Sensing, Third Edition: Models and Methods for Image Processing*], Academic Press, Inc., Orlando, FL, USA (2006).

PV

SMARTPHONES AS AN ALERTING, COMMAND AND CONTROL SYSTEM FOR THE PREPAREDNESS GROUPS AND CIVILIANS: RESULTS OF PRELIMINARY TESTS WITH THE FINNISH POLICE

by

Jaana Kuula, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen & Tuomo Korhonen, 2013

Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013, T. Comes, F. Fiedrich, S. Fortier, J. Geldermann and T. Müller, eds

Smartphones as an Alerting, Command and Control System for the Preparedness Groups and Civilians: Results of Preliminary Tests with the Finnish Police

Jaana Kuula
University of Jyväskylä
jaana.kuula@jyu.fi

Vili Auvinen
University of Jyväskylä
vili.auvinen@jyu.fi

Olli Kauppinen
University of Jyväskylä
olli.kauppinen@jyu.fi

Pauli Kettunen
University of Jyväskylä
pauli.kettunen@jyu.fi

Santtu Viitanen
University of Jyväskylä
santtu.viitanen@jyu.fi

Tuomo Korhonen
Central Finland Police Dept.
tuomo.korhonen@poliisi.fi

ABSTRACT

Traditional mobile phones have been used for alerting purposes by utilizing their SMS and cell broadcasting features. They do however not suit for demanding alerting and command purposes, for the observation of special forces, rescue officers and civilians, or for the post-evaluation of the operation. Current 3G and 4G/LTE smartphones can do all this, but the empirical evidence is missing.

This article reports of the preliminary tests which the University of Jyväskylä has made with the Finnish Police for alerting civilians and for commanding two special groups of the police with smartphones. Smartphones were also used for observing police officers' position and status and for post-evaluating action during and after the operation.

The study supports using smartphones for alerting, command and control purposes. Because of external distractions alerts are noticed better at night than in the daytime. In active hours personal alerts should be given not only by a voice alarm but by stimulating 2-3 senses at the same time. Noticing of smartphone alerts might be improved also by using some additional reception device with the handset.

Keywords

Smartphones, mobile alerting systems, command and control systems.

INTRODUCTION

Personal mobile phones are being used for giving public warnings in emergencies but not as much as one might expect. After the Asian tsunami in 2004 a great interest was paid to them, but the usage did not expand rapidly (Chorist 2009, Ceasa 2010, Nederlandalert). One reason for that was the debate between different messaging systems, especially between cell broadcast and SMS (Sillem et al. 2006). Mobile alerting systems were also considered expensive, because governments were expected to pay all of their development and maintenance costs. From the government's side returns on the investment are difficult to receive (Klafft and Meissen, 2011). Also private people have expressed criticism against emergency alerting systems, for example because of creating a surveillance society (Al-Akkad and Zimmermann 2011) or because of not getting enough benefits of using them (Aloudat and Abbas 2009, Haataja et al. 2011). In areas where extreme nature catastrophes like hurricanes, tsunamis, floods and earth quakes are likely, investments on alerting systems can be justified more easily. Mobile alerting systems may also be implemented in politically unstable areas where hostile terroristic activities are common. Examples from more stable are found, for example from Australia (Aloudat et al., 2011) and Luxemburg (Fema 2012).

For finding alternative ways to cover the costs of building and operating public warning systems, and for developing a smarter mobile alerting system compared to the older SMS and cell broadcasting systems, the

University of Jyväskylä started a series of research projects on mobile alerting systems in Finland. In the first phase a new alerting system was built on smartphones in 2009-2011. After that alternative maintenance and financing models were developed for supporting the implementation and usage of these systems in 2011-2012. The project produced new ideas of how smartphone based alerting systems could be used for warning people in various environments, and how they could be financed with other than full government funding. The project also started a close cooperation with the Central Finland Police Department, which then led into national cooperation with the Finnish Police.

With the police, a three-phased series of empirical tests was started in order to evaluate smartphones' ability to support emergency communication within the internal and external communication of the police. The first test was carried out with two different preparedness groups of the police. The test showed clearly, that smartphones have many advanced features which support emergency communication both in the police forces' internal and external communication. In addition, the first test showed that smartphones can support security authorities' command and control activities during specific protection and rescue operations. They also include features which enable operation managers to observe the security forces', rescue officers' and civilian people's status during the emergency operations. Smartphones also enable post-operational evaluation of the incidents after the situation is over.

As an overall result, the test indicates that the smartphone technology itself is a quite promising media as a part of security authorities' emergency alert, command and control systems. This has however not been studied much, which makes the empirical results of this study interesting. Current smartphones give users a much better chance to notice the emergency alerts than older 2G phones and they give also a chance to give valuable information back to the security authorities about the situation and location of the user. Within the security professionals' use smartphones turn into a multifunctional operation management system which enables warning people and managing the operation which will be needed for saving them.

THE RESEARCH DESIGN

In this study a performance of a smartphone based alarm system was tested in police forces' use in Finland in November 2012. Performance was measured with four indicators, which were 1) the police officers' ability to perceive commands and alerts, 2) readiness to take action after receiving commands and alerts, 3) operation manager's ability to observe the position and status of police officers during and after the operation, and 4) the police officers' ability to post-evaluate emergency operations. At the side of the policemen there was also a control group of civilian users, who received same alerts as the police. The tested smartphone system has been created at the University of Jyväskylä and it was originally designed as the security authorities' warning method for alerting citizens of serious safety threats. In this study the system was tested within the national organization of the Finnish police. The test indicated that the smartphone system could be used also as a command and control system for the police or for other security authorities and groups. The test with the police and civilians is described in the following chapters.

The Smartphone Based Alerting and Command System Which Was Used in the Test

The test was performed with a university based alerting system which operates on a server and on smartphones. The system can send alerts and commands in two ways: Firstly, alerts may be sent for selected groups of people independently of their geographical location. Secondly, messages can be sent through a GIS-based user interface for all or profiled people within a selected geographical area whose diameter may vary from zero to unlimited. This feature reminds the work that has been done in Korea (Lee et. al, 2011). Alerting methods may be varied in the system by changing the alerting sound, visual image, vibration and textual parts of each message.

Messages are sent in the system as the smartphone's push messages through wireless data transfer lines. If the receiving device cannot take in push messages the system will automatically deliver the data content as an SMS message to that particular device. The system is programmed on the Android platform and it can deliver alerts into all kinds of mobile devices. It also operates in a multichannel environment by delivering messages to mobile phones, pc's, laptops and tablets, electronic information boards, social media, news media, etc. Also the two-way communication is supported in the system and the recipients can sign each command or alert, and inform the situation center of whether they are all right or need help. Each mobile device may also be localized in real time and the location and status of users may be viewed on a situation map immediately after each command or alert.

The system is independent from telecommunication operators and the delivery of messages within the system is free from costs. The system owner will pay separate data transfer costs only for those messages which cannot be delivered as a smartphone's push message and which therefore need to be delivered as a SMS message. The smartphone users need not to pay anything extra in addition to their ordinary data transfer subscription for being able to receive messages through the system. Messages may also be received and signed for free without a commercial telecom subscription if the mobile device is connected into an open WLAN network.

Smartphone Devices Which Were Used in the Test

In the earlier stages of the study the Android platform was selected in 2009 as an operating system for the first version of the mobile alerting system that was used in this test. Android operating system was selected because it was a very widely used smartphone platform in the World and because it was able to perform those alerting operations which were defined for the new alerting system. For example, the new system should be able to play the wanted alerting sounds and strike up vibration when the alert arrives on the phone. The phones should also be able to play the alerting sound even if the device was muted. Currently Android has been the World leading in platform since 2010 (Canalys 2011), and in Fall 2012 three out of four shipped smartphones Worldwide were Android phones (IDC 2012).

The selection of the Android platform simultaneously determined which smartphone brands could be used in the test. For this reason the test was carried out with Sony Xperia Go, HTC Explorer, HTC Desire, Samsung Xcover GT-S5690, Samsung Galaxy S II and Google Nexus S type of smartphones.

The Test Group and the Course of the Study

The purpose of the study was to evaluate the performance and usability of a smartphone based mobile alerting system for the alerting, command and communication purposes of the national police. The test was also expected to give information of the smartphones' usability for alerting large groups of civilian people.

All activities were designed and operated with the Central Finland Police Department, which collected and commanded all police forces who were participating in the test around the country with the authorization of The National Police Board. Test group of ten policemen was formed from two different preparedness groups of the police. At the side of the police group also a small reference group of civilians was formed in order to monitor results in these two groups.

During the test the leading police officer in the situation room sent test events of simulated real-like incidents to the test users' mobile phones around the country. Users were obligated to sign all messages immediately no matter where they were and what time of the day or night it was. Immediately after sending the alerts all users' location and status appeared on a real-time map on the screen in the situation room. Each user's position and status was indicated with a green, red or yellow flag. Green flag indicated that the user had received and signed the message, and that (s)he was in full operating condition. Red flag indicated that the user had received and signed the message, but was not well and needed help. Yellow flag demonstrated that the user had not been reached and that there might be some problems which needed further investigation or action. After the simulated incidents and operations were over, users could track their operation history by viewing the messaging log on their phones. In each alert the signaling voice, vibration, icon and textual content of the message were altered. By changing these features the researchers could follow how the police officers and civilians would notice and react on alerts which were given in a different form and in different situations and times.

Test users' identity was protected during the test and each user was given a code name which was linked with the smartphone device which they were using. Depending on the professional background and type of the device which they were using, test users were given an individual code name and divided in smaller subgroups. These groups were named according to Finnish wild animals as the Bears, Wolves, Wolverines and Bobcats. All Bears were policemen who had Sony Xperia Go devices, and Wolves policemen with HTC Explorers. Wolverines were policemen with Samsungs and Bobcats civilians with Sony, HTC and Google Nexus devices. Test devices except the private Samsung phones were provided by the University of Jyväskylä for the police officers' use.

The test was operated for two weeks in November 2012. Alerts were given mainly within the police forces' active working hours. All policemen carried out their everyday operations normally while participating in the test. Alerts and commands were given randomly in different times of the day, including night time. There was no advance planning of where the users should stay and what they should be doing during the test. Alerts would therefore reach policemen either in a favorable or in a bad situation, and despite of that they were expected to react immediately.

After the test users were interviewed with an internet questionnaire which included numeric evaluations and written open answers about the experiment. Some key persons in the different levels of the police organization were also interviewed face to face.

The Variables for Measuring the Performance of the Smartphone Based Alerting System

The overall performance and usability of the alerting system was evaluated in the study by the police officers' and civilians' ability to notice, understand and react on the incoming alerts. Users' ability to notice and understand alerts was evaluated from the auditory, sensory, visual and cognitive senses' point of view. Overall performance was also evaluated by the operation manager's ability to observe the police officers' and civilians' location and status during and after the operation, and by the police officers' ability to post-evaluate emergency operations.

The following chapters describe in a more detail the variables which have been used for measuring the performance.

Police Officers' and Civilians' Ability to Perceive Commands and Alerts

It was assumed in the test that if the incoming alerts would stimulate more senses than one the users would notice and understand them better. Therefore many of the smartphones' technical features were utilized in the test for ensuring that the police officers and civilians would notice and understand alerts and take action as fast as possible in all situations.

The possibility of noticing of the alerts was enhanced in the study by stimulating the users' auditory, sensory, visual and cognitive senses with the alerting messages. This was made by utilizing the plentiful selection of alerting sounds and the vibration feature of the smartphone devices. The visual sense of the user was stimulated with colorful icons, which were added as a teaser in the alerting messages. As the fourth sense the cognitive perception was affected by the textual part of the alerting message.

According to these principles the users' ability to perceive alerts with the four senses was converted as research variables. These were

- noticing of the signaling voice of the alert,
- noticing of the vibration of the smartphone device,
- noticing of the alerting icon on the screen of the phone, and
- noticing of the textual message on the alerting message.

Auditory, visual, sensory and cognitive stimulation was altered during the test by changing the alerting tune, vibration, visual icons and form of the textual message. While testing the auditory perception three alternative signaling sounds (siren, alert and warning) were used and silent as the fourth. The siren was a high siren kind of voice and it was the highest tone that could be created on the smartphone devices. The other sounds called alert and warning had a slightly lower and softer tone and they also were used at the highest possible volume on the phones. The silent sound had no signaling sound at all.

While testing the sensory perception of the alerts the vibration function of the smartphones was set on or off.

In order to test the visual perception, alerting icons were altered between a red warning triangle with an exclamation mark in the middle, sole red exclamation mark, and blue police logo with a symbol of sword.

For testing the cognitive perception and reaction time of the users, a description of the nature of the incident and a request to sign the alert were enclosed in the textual part of the alerts. Textual messages might also have written instructions to take some kind of action, or some other information concerning the situation.

Police Officers' Readiness to Take Action After Receiving the Command or Alert

The policemen's readiness for taking action was measured by their reaction time and signing of commands and alerts. Reaction time was counted from the time of sending the alert until the time when it was signed. Policemen's further activities after signing the alerts were not observed and they were not asked to follow any physical or operational procedures after receiving the message.

Operation Manager's Ability to Observe the Status of Police Officers and Civilians

The operation manager's ability to observe the position and status of the police officers and civilians was evaluated by measuring how well they can follow the status information with the system during the operation. The tested smartphone system includes features which make it possible to observe in real time from the GIS-based user interface whether the police officers and civilians are in or outside the endangered area and whether they need help. Status information may be analyzed also afterwards from the log.

Police Officers' Ability to Post-Evaluate Operations

The policemen's ability to post-evaluate their action during the emergency operation was measured by their ability to read and evaluate the log information on their smartphone. Additional information about the course of the action was also found on the user interface of the server-end of the system. The system recorded all alerts and commands which were given during the mission, as well as exact times when they were sent, received and signed. The system also recorded the status of those officers who were called into the mission, but who did not receive or sign the calls.

Background Variables

In addition to the research variables there were some background variables in the test, which may have affected the users' perception and reaction on the alerts. These factors were

- the brand and type of the smartphone
- the operating system and its commercial version, and
- the operator whose data communication subscription was implemented on the phone.

The test was carried out by using Sony Xperia Go, HTC Explorer, HTC Desire, Samsung Xcover GT-S5690, Samsung Galaxy S II and Google Nexus S type of smartphones. All phones were running on the Android operating system. All Sony devices had the version 2.3.7, HTC version 2.3.5, Samsung version 4.0.x and Google Nexus version 4.1.2.

The availability and capacity of mobile telecommunication networks are crucial for the operation of mobile alerting systems. Often mobile phone lines get crowded during mass events and accidents. This will disturb also the operation of SMS based alerting systems. The smartphone system which was tested in this study operates on data communication lines, which do not get crowded in the same way as SMS messaging on mobile telephone lines.

The operation of this kind of system is, however, dependent on the capacity and coverage of the telecommunication networks all over the country. It is unlikely that networks are similar in all parts of the countries or on different sides of the cities. The operation of the alerting system may also be dependent on the telecommunication operator of the mobile device, because all operators do not offer full or any services in all areas. In this test all phones were provided either with the telecommunication subscription of TeliaSonera, Elisa/Saunalahti or DNA, which are the main commercial mobile operators on the Finnish market.

RESULTS

The results of testing a smartphone based alerting system with the police are described on the following. The police officers' experiences of noticing commands and alerts in various situations are explained first and after that their readiness to take action. The operation manager's ability to observe the police officers' location and status, as well as the police officers' ability to post-evaluate the operation are reported later in the text.

The Perception of Commands and Alerts

This chapter explains how the police officers managed to notice and understand alerts in various situations. The auditory, sensory, visual and cognitive perception of alerts is reported in their own sections below.

The Auditory Perception of Alerts

The auditory perception of the commands and alerts was based on the volume and tune of the signaling sound which turned on when the most critical alerts arrived on the phone. Three different alerting sounds were used in the test and all of them were played at the 90-100 % volume of the phone. Some alerts were given with no sound

at all.

In a numeric evaluation in scale 1-5 (1=poor, 5=excellent) more than 70 % of the respondents evaluated the sound and volume of the alerts as good or excellent. In the written evaluation one user considered the volume too strong and got sometimes scared about it. Some other users reported that their co-workers at work and family at home in the evening were amused about some of the sounds.

The perception of the sounds was strongly dependent on the situation in which the users were at the time of the alert. In quiet indoor situations like in the user's own office sound alerts were noticed immediately. In other indoor situations where there were plenty of people around, alerts were noticed more weakly and sometimes not at all. For example, in a big lobby or in a lunch room full of people the sound could not be heard because of the background noise. In the noisy situations perception was also dependent on where exactly the mobile device was at the moment of the alert. If it was in the user's hand, on the lunch tray or on the table in front of the user, the alert may have been noticed despite of the noise. Instead, if the phone was in the user's hand bag or pocket, the alert was not necessarily noticed (unless the vibration was on). Sometimes the alerting sound was mixed with other voices and the users may have thought that the sound came from the television or outside from an emergency vehicle which was passing by. Also in outdoor situations alerts were noticed weakly because of the background noise. Outside people also kept their phones in the pocket or bag, which prohibited them from hearing the sound.

Some alerts were sent without any signaling sound, so the users could not hear them. If the phone was close to them on the table or in contact with their body, they could notice it by seeing the alert on the screen or by feeling the vibration against their body. Many users were at their own office during the alerts, which helped noticing them. Silent alerts were tested because in the police work they are needed in certain kinds of assignments.

The Sensory Perception of Alerts

The sensory perception of the alerts was based on the vibration of the mobile device at the moment of receiving alerts. In the written comments users mentioned that in a real situation the vibration and silent alerts would be useful. In indoor situations the vibration helped to notice alerts which were sent without the sound. In outdoor situations vibration helped to notice also alerts which were sent with the voice, if the sound could not be heard because of the background noise.

The Visual Perception of Alerts

The visual perception of the alerts was based on three different icons, which popped on the screen when the alert arrived. In the numeric evaluation 85 % of users evaluated the usability of alerting icons as good or excellent. The figure itself may have not affected much on noticing the alert, but the conception of the message may vary depending on the figure. For example, an image with a striking red color might be taken more seriously than a message with an unnoticeable figure and color.

Different icons may also have contextual or cultural meanings, which may effect on how they are perceived. In this test, among two red colored alerting signs there was also a blue colored police logo. Among the ordinary people police is respected and considered as an authority in Finland, for which reason it would have been expected that the police logo would get people's attention well. In this test most of the users were, however, policemen who see these logos every day. For these users the police logo had no added value and might not mean any serious alert at all.

The Cognitive Perception of Alerts

The cognitive perception of the alerts was based partially on the alerting sound and icon of the message, and mainly on the written text that was delivered within the alert. The alerting sound and icon were the first information to the users about the event which was going on, and the textual message gave literal information of what the incident was about. The literal information may also have given additional information about the operating procedures and actions which the person should take because of the alert.

In the test, users recognized easily the first part of the textual message, which indicated the nature of the emergency and requested to sign the message. Further parts of the textual messages were left on less notice. If the alerts would have been given in a real situation, users may have read all of the information more carefully. In a test situation as an extra work to police officers' normal duties, users may have focused on signing the alerts and switching off the alert sound quickly, rather than reading carefully everything what was written in the message.

In real emergency situations users should read the textual part of the message, because it is the only way to identify the nature of the emergency. Sounds and icons may illustrate the situation in some extent, but if the sounds and symbols do not hold an established status in the society, people may misunderstand them. Also, if symbols are culture related, all people from different cultures cannot understand them. In those cases the role of textual parts of the emergency notifications is even more important.

The Readiness to Take Action

The police officers' readiness to take action was measured by their reaction time on the received messages. The reaction time was dependent on how well the messages were recognized and in which situation the users were at the moment of receiving alerts. If alerts were noticed at once, they were also signed immediately. Possible obstacles may have been for example driving a car at a high speed amongst a hectic traffic. Referring to the situations where the users where at the time of receiving alerts, 28,6 % of the respondents indicated that it was very easy to sign the alerts. For another 28,6 % it was quite easy and for 28,6 % fairly easy. The rest 14,2 % of the respondents indicated that in most of the times it was quite difficult to sign the alerts.

Reaction times between daytime and night alerts varied quite a lot. In average 22 % of the users signed the daytime voice alerts within the first minute, 60 % in two minutes, 82% in five minutes and 88 % in ten minutes. For the rest 12 % signing of daytime alerts took more than ten minutes, but in average not more than one hour. At night when the users were sleeping, alerts were noticed even better. In a silent room the alerting sound was loud, and the users woke up and signed the alerts fast. One police officer reported of waking up even if the phone was in a bag in another room outside the bedroom. At the night time the average reaction time was fastest of all alerts which were sent during the test. 80 % of the users signed the alert within the first minute and the rest 20 % within two minutes.

The reaction times to silent alerts were slightly longer than to voice alerts. In average 17% of the users signed silent alerts within the first minute and 44 % within two minutes.

Compared with the recommended delivery times of emergency notices with SMS in Finland, the delivery and reaction times of smartphone alerts were excellent in this test. According to government's instructions of giving emergency notices to civilian people as SMS messages, one hour's delivery time is considered fully acceptable and two hours fair (Liikenne- ja viestintäministeriö 2009). In this test, 82 % of messages were delivered, received and signed within 1-5 minutes, even if the people we at sleep at the time of receiving the messages.

The Ability to Observe the Status of Police Officers and Civilians During the Operation

During the test the operation manager had an instant view on the map for observing each police officer´s position, status and reaction time on alerts and commands. If all officers did not sign the call immediately, their status was updated on the map after signing the task. The status of signing alerts was indicated on the map with different colored flags. Officers who had signed the task and were in a good operating condition were indicated with a green flag. Those who had signed the task and who were not well or needed help were indicated with a red flag. Persons who were not reached were indicated with a yellow flag.

The visual view on the map gave to the operation manager a good comprehension of the resources which were assigned for the mission. The map view showed instantly where geographically the called officers were, and how long it would take to get them on duty. Map view would also help designing transportations, if personnel should be shifted from one part of the country into another.

The Ability to Post-Evaluate the Course of the Operation

The post evaluation of the operation was based on the automatically recorded log information of the action. Log information was stored on the server and on each one´s own mobile phone, where it could be analyzed easily afterwards. Some of the test users did not see much importance with the log, whereas some others saw it as a valuable support for evaluating the course of the operation. They also reported that sometimes people understand the required tasks differently, and with the written log it is easy to confirm afterwards what the exact assignment was. In the numeric evaluation 67% of the respondents evaluated the possibility to page through the received commands and alerts as quite necessary or very necessary. Other 33% could not say clearly whether the log information was necessary or not.

The Influence of the Background Variables

The background variables in the study determine the primary conditions for the usage of mobile alerting

systems. Some observations of the influence are presented on the following:

The Brand and Type of the Smartphone

All equipment in the test were able perform the required functionalities and no particular observations were reported about the differences between various brands. The devices may, however, have differences in the volume and tune of the alerting sounds, which may effect on the recognition of alerts and on the reaction times of the users. For example, in this test some of the users may have not noticed the alerts in certain situations, because some smartphone brands may have a weaker alerting sound than others. Identifying these kinds of technical differences would require additional tests.

The Version of the Operation System

All phones in the test had an Android operating system. For this reason they were expected to operate identically during the test. This is however not always the case. There is a chance that the Android operating system may not run fully identically in all manufacturers' devices. For that reason also those applications which run on the Android platform may not operate exactly in the same way in different devices. As this test was quite small and only few manufacturers' devices were used in it, the study cannot give any clear indication of the differences between different brands.

There is, however, evidence of minor differences in the operation of different versions of the operating system. For example, in November 2012 there were around 10 different versions (versions 1.5-4.1) of the Android operating system on the market (Android 2012) and the tested alerting system would not run perfectly in all of them. The Android versions of 2.1 and older do not support or deliver push messages. The studied smartphone system would however deliver alerts to these phones as SMS messages. In November 2012 versions 2.1 or older represented only 3,5 % of all Android users in the World, so the tested alerting system should run in 96,5 % of Android phones Worldwide (Android 2012).

For getting better understanding of the operation on different versions of the operating system, one should run systematic laboratory tests with different devices and versions of the same operating systems. In ordinary consumer applications possible differences may not cause any noticeable problems for users, but in systems which are built for protecting people's lives they might have a greater importance. If updating causes great changes in different versions, each new version of the operating system might include a risk for critical systems. The risk would be bigger, if the updating of operating systems or client applications would be left on the users' own responsibility.

The Telecommunication Operator

All phones in the test operated in TeliaSonera's, Elisa/Saunalahti's and DNA's networks. The users did not report of any problems which could be connected to a certain operator. Problems in telecommunications may however occur both in normal times and during a crisis (Kuula, 2012b). If also emergency alerts should cross international borders that might cause problems in the delivery of alerts as well (Kuula, 2012a). In this case most users stayed in the city during the whole test, so they may not be aware of possible problems outside the cities. They may also be unable to observe possible delays in the delivery times of the alerts or in their own responses. The performance of mobile networks was measured separately during the test.

SUMMARY AND CONCLUSIONS

Along with the vast expansion in the usage of mobile a growing interest has been paid towards using common mobile phones as a media for public alerts in various emergencies. In older types of 2G mobile devices public alerting systems have been built on SMS and cell broadcasting systems. These have technical limitations which prevent their usage for more advanced purposes. For example, they focus on one way communication, and they are not very flexible for defining the geographical range of sending messages. Also the price for sending masses of SMS messages is quite high, and in many countries the national infrastructure for delivering cell broadcasting messages is missing.

3G and 4G/LTE smartphones represent common technologies and offer many advanced features which 2G devices do not have. Because of these features they should perform better than 2G devices in alerting people of emergencies, but experiences of this kind of usage have not been reported much.

This article reported of an experiment where a smartphone based command and alerting system was tested in police officers' use. The test included members from two different preparedness groups of the Finnish police

and a small reference group of civilian people.

In the test the reception of command and alerting messages was evaluated from the auditory, visual, sensory and conceptual perspective. In addition, police officers' reaction time and readiness to take action after receiving alerts was evaluated. Also operation manager's ability to observe the position and status of police officers and civilians in the insecure area, and the police officers' ability to post-evaluate operations was estimated.

The users' overall evaluation of the usability of smartphones for command and alerting purposes was good. Most of the users carried the devices actively with them and gave plenty of written and numeral evaluations of the device and system on the internet survey which was addressed to them after ending the test. All except one answered the survey in time. The overall evaluation of the usability of the system was good or excellent for 71,4 % of the respondents, fairly good for 14,3 % and poor for 14,3 %.

While evaluating the overall usefulness of the system, 57% evaluated smartphones very important for the police work and 43 % quite important. For the question of whether they would recommend the tested kind of smartphone system for the policemen's use, 43% would recommend it very strongly and 28,5 % quite strongly for the policemen's use. Another 28,5 % was not able say whether they would recommend it for the police.

As a conclusion, the study shows that smartphone based alerting and command systems are usable and useful for the policemen's use. Received evaluations were considerably high on most of the questions and strong negative comments were not received. Improvement could, however, be made in the certainty of receiving alerts in active and noisy situations at the daytime and in the evening (or in noisy night time working hours). The average daytime reaction times of 60 % of messages signed within the first two minutes, and 88 % in 10 minutes are considerably high compared with other alerting methods the television and radio broadcast. Specific user groups like the police might still require even greater certainty of receiving and signing alerts, and that could be done for example by using 2-3 different (auditory, sensory, visual) alerting methods at the same time, or by using some additional sensor devices together with the handset of the phone. For example ear tabs or some kinds of sensor devices might be useful in touch with the skin. With the usage of ear tabs the volume of voice alerts should however be used carefully for not causing any harm for the users' ears. As the number of users was quite small in this study, various alerting methods of smartphones require further research for confirming their effect in different situations.

ACKNOWLEDGMENTS

The authors wish to thank The Central Finland Police Department for their support and participation in this University of Jyväskylä's research on the mobile smartphone systems of crisis communication. Authors also thank the National Police Board and Helsinki, Espoo, Tampere, Jyväskylä, Joensuu, Kuopio, Vaasa and Rovaniemi police units for participating in the test. Also, authors are grateful for Tekes – The Finnish Funding Agency for Technology and Innovation, University of Jyväskylä, Magister Solutions Ltd., Parco Group Ltd, Jämsän Apteekki and the European Regional Development Fund for funding this research.

REFERENCES

1. Al-Akkad, A. and Zimmermann, A. (2011). User Study: Involving Civilians by Smart Phones During Emergency Situations. *Proceedings of the 8th International ISCRAM Conference*, Lisbon, Portugal.
2. Aloudat, A., Michael, K. and Abbas, R. (2009). Location-Based Services for Emergency Management: A Multi-Stakeholder Perspective. *Eighth International Conference on Mobile Business*, 143 - 148. ICMB.
3. Aloudat, A., Michael, K. and Abbas, R. (2011). Recommendations for Australia's Implementation of the National Emergency Warning System Using Location-Based Services. *Journal of Ubiquitous Systems & Pervaisive Networks,* 3(2):59-66.
4. Android (2012). Platform versions. http://developer.android.com/about/dashboards/ index.html, cited 30.11.2012
5. Canalys (2011). Google's Android becomes the world's leading smart phone platform. http://www.canalys.com/newsroom/google%E2%80%99s-android-becomes-world%E2%80%90s-leading-smart-phone-platform.
6. CEASA (2010). Position Paper Cell Broadcast as a tool for civil alert. http://www.ceasa-int.eu/wp-content/uploads/2010/04/EU_Position-Paper-Version-5-1-1.pdf.
7. CHORIST (2009) http://chorist.eu

8. FEMA (2012) http://www.fema.gov/commercial-mobile-alert-system.
9. Haataja, M., Häkkinen, M. and Sullivan, H. (2011). Understanding User Acceptance of Mobile Alerting Systems. *Proceedings of the 8th International ISCRAM Conference,* Lisbon, Portugal.
10. IDC (2012). Press release. http://www.idc.com/getdoc.jsp?containerId=prUS23771812.
11. Klaffen, J. and Meissen, U., (2011). Assessing the Economic Value of Early Warning Systems. Proceedings of the 8th International ISCRAM Conference - Lisbon, Portugal.
12. Kuula, J., Häkkinen, M. and Jalasvuori, J. (2012a). The Need for International Harmonization of Emergency Notification Systems: The Case of Finland. *The Proceedings of the Global Research Forum*, Davos, Switzerland, 1922 February, 2012.
13. Kuula, J., Räsänen, J., Kettunen, P., Kauppinen, O. and Panasenko, V. (2012b). Mobile Emergency Messaging and the Vulnerability of Crisis Communication. *Proceedings of the NBC 2012 – 8th Symposium on CBRNE threats: How does society scope?,* Turku, Finland, 11 - 14 June, 2012 .
14. Lee, J., Niko, D., Hwang, H., Park, M. and Kim, C. (2011). A GIS-based Design for a Smartphone Disaster Information Service Application. First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering. IEEE
15. Liikenne- ja viestintäministeriö (2009). A proposal for taking focused authority notifications in use in emergency communication (in Finnish), http://www.lvm.fi/c/document_library/get_file?folderId=612147 &name=DLFE-8025.pdf&title=Ehdotus kohdennettujen viranomaistiedotteiden käyttöönotosta väestön hälyttämisen ja varoittamisen tukena (17.6.2009)
16. Sillberg, P., Rantanen, P., Saari, M., Leppäniemi, J., Soini, J. and Jaakkola, H. (2009). Towards an IP-Based Alert Message Delivery System. *Proceedings of the 6th International ISCRAM Conference*, Gothenburg, Sweden, May 2009.
17. Sillem, S. and Wiersma, E. (2006). Comparing Cell Broadcast and Text Messaging for Citizens Warning. *Proceedings of the 3rd International ISCRAM Conference*, Newark, NJ (USA), May 2006.
18. Steenbakkers, W. A Dutch case study: Cell Broadcast for Public warning, The road ahead. http://www.nederlandalert.nl/systemen/A_Dutch_case_study-cell_Broadcast_for_Public_warning_The_road_ahead.pdf. Ministry of the Interior and Kingdomrelations, the Netherlands

PVI

ALERTING SECURITY AUTHORITIES AND CIVILIANS WITH SMARTPHONES IN ACUTE SITUATIONS

by

Jaana Kuula, Olli Kauppinen, Vili Auvinen, Pauli Kettunen, Santtu Viitanen & Tuomo Korhonen, 2013

Proceedings of the 12th European Conference on Information Warfare and Security ECIW-2013, Jyväskylä, Finland, 11-12. July, 2013

Alerting Security Authorities and Civilians with Smartphones in Acute Situations

Jaana Kuula[1], Olli Kauppinen[1], Vili Auvinen[1], Santtu Viitanen[1], Pauli Kettunen[1] and Tuomo Korhonen[2]
[1] University of Jyväskylä, Department of Mathematical Information Technology, Finland
[2]Central Finland Police Department, Jyväskylä, Finland
[1][first].[last]@jyu.fi
[2]tuomo.korhonen@poliisi.fi

Abstract: The speed of communication and the recognition of emergency notifications are key issues in alerting people in acute situations. This article describes case studies which The University of Jyväskylä has made for studying how well smartphones can be used for emergency alerting in different situations. In the study empirical tests were carried out with three different test groups. The first test was carried out with security professionals within the internal organization of the Finnish police. In the second test police sent emergency alerts to the private citizens' personal smartphones. The third test was carried out in a school of 500 pupils. All tests were carried out by using a smartphone based alerting system that has been developed at the University of Jyväskylä. The alerting system utilizes multiple technical features of smartphones for ensuring that the alerts will get through and become noticed in all circumstances. It also operates independently from commercial telecommunication operators, and if open WLAN is available, emergency alerts can be sent even if mobile phone base stations are down. The tests show that for ensuring the perception of safety alerts in all situations smartphone alerts must be given in different forms at the same time. For example, in noisy environments voice alerts need to be intensified with the vibration feature of the phone. Voice alerts may also be supplemented with a visual and textual message. Alerts also need to be given in a different form for different users if the users are security professionals, adult aged private citizens or if they involve underage children. The tested smartphone based alerting system may be used both in normal times and during the state of emergency.

Keywords: smartphones, mobile alerting systems, public warnings, crisis communication

1. Introduction and background

Mobile alerting systems are becoming more common and important at the side of broadcasting type of notification systems. For example, Aloudat et al. (2011) consider them as an established part of mobile government strategies worldwide. Meissen and Voisard (2008) see the effective implementation of early warning systems as one of the best investments for disaster prevention and mitigation. As an example, during the Tohoku Earthquake in 2011 in Japan warnings were sent to circa 52 million people by SMS and CBS. First warning was given in 8.6 seconds from first wave and to Tokyo warnings arrived 65 seconds before earthquake (Yamasaki, 2012).

At the same time as new emergency alerting systems are taken in use, in the modern world people are already stressed up with many other kinds of alarms and signals. There might even be a risk that the individuals' overload of digital signals is so heavy that people are not able to recognize critical emergency signals, even on their personal mobile phones.

Häkkinen has studied the failure of alarms in his doctoral thesis (Häkkinen, 2010) and notes that many people ignore alarms even if they can be crucial for life. He sees many causes for the failure. One reason is that human alarms are often implemented through a variety of technical means and presented as abstract signals. Häkkinen suggests that multimodal alarms should be used for addressing the sensory and cognitive factors that impact alarm detection and understanding. According to Coombs (2007) fast reaction to crisis is important. The first reaction should also be logical and correct. This causes pressure for authorities and for crisis management. Ready-made notification templates will help making correct response actions, and wide usage of communication channels will help reaching a high adoption rate.

Häkkinen (2010) sees the alarm process as detection, perception, recognizing and responding. All of these phases must success for taking an appropriate action. Due to the environment for example voice alarms may not be heard at a crowded railway station and a vibration alarm may not be noticed in the pocket of a motorcycle rider. Perceiving alerts means that the detected alarm should receive attention and be processed. If attention towards it cannot be maintained, the alarm can be lost among other signals or noise. After perceiving the alert, existing knowledge will be used for recognizing the signal. People will then use the received information and earlier known protection procedures for surviving the situation. According to Sillem and Wiersma (2006) people are very capable in receiving information and the successful design of warning messages maximizes the probability of having each step of the alerting process to be completed.

According to Häkkinen (2010) many physical, environmental, sensory or cognitive disabilities do not match with the alarm processing. People's sensory systems can also be temporarily weakened by fatigue, acute illness or injury, stress, foreign language or methods, background noise and intoxicants. Also false and pointless alerts decrease the motivation to respond alarm.

A research group at the University of Jyväskylä made an empirical study for testing the usage of smartphones for emergency alerting purposes in three different user groups. The first test was performed within the internal organization of the Finnish police in order to measure how well smartphone alerts will be noticed and reacted by security professionals. The second test was addressed to civilian people in order to find out how well similar alerts will be noticed by private citizens and in which way authorities should structure the alerts which are directed to the private people. The third test was carried out in a public school of 500 children. The purpose of this test was to find out issues which authorities have to take in notice when considering mobile alerts in schools.

All tests were carried out in November 2012–February 2013 and they were made by using a smartphone based alerting system which was developed at the University of Jyväskylä in 2010–2012.

2. The system design of the tested alerting system

The tested mobile alerting system is based on a combined server and smartphone application which also operates with other kinds of media. The server end includes an integration interface with several external systems like with emergency response centers and other security authorities. It also contains a web-based application for the input of manually given notifications. The server also collects and stores information. According to Amailef and Lu (2011) alerting systems are highly data dependent, for which reason databases play a significant role in these systems.

The mobile application is connected to the server and it is the primary communication channel in the system. So far it runs on the Android platform. The Android platform was chosen as the operating system because it is the most widely used mobile platform in the World and can perform various multiform alerting operations. (Kuula et al. 2013) For others than Android phones alerts are delivered as SMS messages with the assistance of a third party SMS gateway service.

The system can also exchange information with other communication channels. In many situations multichannel messaging is needed and more efficient than delivering alerts through one channel only. In addition to smartphones, messages may be delivered to PC's, laptops and tablets, social media, electronic bulletin boards and public media. According to Vihalemm et al. (2012) the use of alternative sources and channels of warning messages will help people to emotionally and cognitively cope with crises. Also Hughes and Palen (2009) suggest that emergency management could use Twitter and similar micro-blogging technology as a way of getting information to the public. They expect that this would also fuel personal technology adoption and instruct operation in emergency warning, response and recovery situations. Muralidharan et al. (2011) have noticed that nonprofit and media organizations use information dissemination and disclosure effectively, but fail to capitalize the two-way communication nature of social media. The tested smartphone phased system has all these abilities. The operating concept of the system is presented in Figure 1.

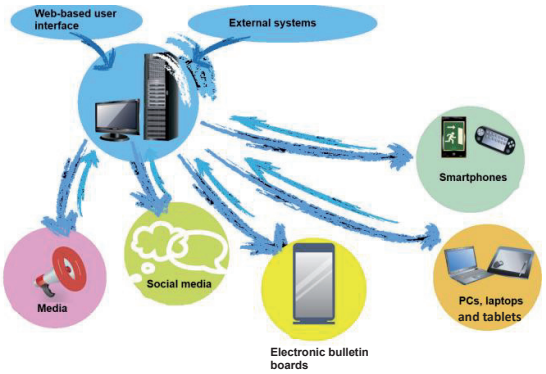


Figure 1: The operating concept of the tested smartphone based alerting system

With the system emergency alerts can be sent to selected location-based areas or for selected groups. The location-based alerting area will be defined for each emergency individually by giving the geographical coordinates and range of the influence area of the emergency to the system. The range

of the alerting area can vary from one building into the whole city or wider. In group-based alerts notifications will be sent for selected user groups regardless of their geographical location.

The system also includes a GIS-based graphical user interface and it supports multilingual and multimodal presentation. Multimodality is the system's main advantage compared with Common Alerting Protocol (CAP) and it is based on Häkkinen's (2010) Multi-Modal Alarm Specification Language (MMASL).

Figure 2 illustrates the selection of the alerting area through the GIS-based graphical user interface and some visual images which can be used as a part of MMASL based alerting messages.

Figure 2: Visual alerting icons and the Web- and GIS-based user interface of the tested system

The mobile end of the system operates on the Android platform. Requirements are Android version 2.2 or newer and Google account. The application runs at the background of other operations and sends the user's location information to the server timely. The native Android application enables using all available functionalities of the smartphone. It's main advantage is that the emergency notifications can be forced through to the user over other services. The user will be notified even if the ringtone is muted.

The Android platform handles the location information and network connection without the user's or application's need to think about it. Localization methods depend on the user settings and features of the device. Normally the system uses GPS-, WLAN- and mobile network-based localization.

The system operates on ordinary mobile networks (2G/GPRS/EDGE, 3G/UMTS/HSPA, 4G/LTE) and WLAN (IEEE 802.11). The usage of WLAN and web-based connections is a big advantage, because they are not dependent on mobile telecommunication operators. This is critical in emergencies where the base stations of mobile networks are down. That may happen in ordinary storms and because of heavy loads of snow on trees in winter, which both cut trees and break off the electricity supply on base stations. Also other problems may occur in telecommunications both in normal times and during crises (Kuula et al., 2012). For avoiding the vulnerability of mobile networks, also the device-to-device communication and mobile ad-hoc networks (MANET) could be used. That would help avoiding communication overload on base stations and enable communication without mobile networks.

In the emergency the user will receive a notification with an alert (alerting cue) and a message. Both parts can be customized with different auditory, visual and tactile effects. Customization enables sending notifications with a different priority and with selected effects which give the users fast a truthful understanding of the situation. Figure 3 illustrates how the alert (cue) is received on the smartphone and how textual message will be shown on the screen after that. The latter view includes also a question to user. By answering to that question the user may ask for help.

A big challenge in the real life is how to get people to use these systems. Users often have concerns about their privacy while using real time location-based systems and therefore the privacy mode should be enabled in such systems (Aloudat et. al., 2009, Al-Akkad and Zimmermann, 2011). According to Al-Akkad and Zimmermann (2011) some people fear for creating a surveillance society while gathering masses of data from mobile phones.

Wu (2009) sees that the usefulness of SMS-based alerting systems has multiple levels of meanings to the users. The ease of use is more about the users' ability to control the system behavior. It is also a subjective norm which needs to be examined with relation to its originating source. According to

Kaasinen (2005) user acceptance and intention to use are built on the perceived value of the service, perceived ease of use, trust and on the perceived ease of adaption in the actual usage phase.

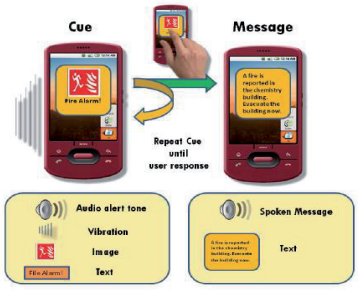


Figure 3: Notification receiving process on smartphone (Häkkinen, 2010, p. 78)

The two-way communication of the tested system enables to gain information from the people in the hazard zone. Figure 4 illustrates the map view of the real time situation in the emergency area after giving a location based emergency alert. Users who need help are indicated with a red flag (not in the picture) whereas the green flag indicates that the user is all right. A yellow flag means that the user hasn't signed the question, for example because of getting hurt and not being able to use the phone. The phone may also be lost or out of order.

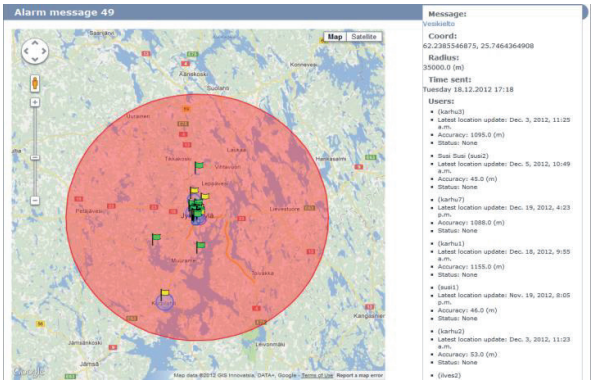


Figure 4: Overview of a given notification

Table 1 contains a summary of some central features of the tested system. The table has been modified from the original table of Lee at al. (2011) and it concludes the major differences between the tested smartphone system and other alerting systems which operate on ordinary mobile phones.

Table 1: Comparison of older and smartphone based services, modified from Lee et al. (2011)

	Base station based mobile emergency alerts	**Smartphone based emergency alerts**
Basic device	Cellular phone	Smartphone
Network	3G, 4G	3G, 4G, WLAN
Service Type	SMS, CBS, LBS	Push messages, mobile client application
Time of being used	During the emergency	All the time
Type of message	Text	Voice signal, image, text, vibration, map
Need for client application	Not needed	Installation needed

3. The research design

It is difficult to define how public warnings should be given. The research problem was therefore split and divided into smaller problems. As the police and the city are in charge of the public safety, a close cooperation was started with the Central Finland Police Department and with the City of Jyväskylä for testing the university's alerting system.

With the police, two pilot studies were designed. One was organized within the internal organization of the Finnish Police and another with civilians. In the first pilot emergency alerts were given by the police to the test users of two preparedness groups of the police around the country. In the second test police gave security alerts to the private citizens' personal mobile phones. The third pilot was carried out in a 500 pupils' school in the City of Jyväskylä, because in recent years there have been some unfortunate shootings, bomb threats and other violence at schools in many countries. The police were observing also the school pilot.

The participation of the Central Finland Police Department and the City of Jyväskylä in the empirical tests was extremely valuable. According to Aloudat et al. (2009) it is important to investigate the perspectives of the crucial stakeholders, like of the prospective users and the government. Aloudat et al. (2009) noticed that these users believe that location-based services have the potential to aid people in emergencies, but there are several major disagreements for example about the privacy, cost, specification and management issues of these systems.

3.1 Case study with the police

The first pilot was organized with the Central Finland Police Department and with the Finnish Police. Detailed results of the pilot have been published in the ISCRAM 2013 Conference (Kuula et al, 2013).

The purpose of the study was to evaluate the performance and usability of a smartphone based mobile alerting system for the alerting, command and communication purposes of the police. The study should also give information of the smartphones' usability for alerting civilian people. The test was carried out with the standardized smartphones which were given to the police officers' use.

For the study a test group of ten policemen was formed from two different preparedness groups of the police and introduced to the use of the system in a video conference. The leading police officer then sent in the situation room test events of simulated real-like incidents to the test users' around the country. Users were obligated to sign all messages immediately regardless of where they were and what time of the day it was. Immediately after sending the alerts all users' location and status appeared on a real-time map on the screen in the situation room. Each user's position and status were indicated with a green, red or yellow flag.

The overall performance and usability of the alerting system was evaluated by the police officers' and civilians' ability to notice, understand and react on the incoming alerts. Users' ability to notice and understand alerts was evaluated from the auditory, sensory, visual and cognitive senses' point of view. The policemen's readiness to take action was measured by their reaction time on commands and alerts which were sent in the working hours and at the free time and night.

In a numeric evaluation in scale 1-5 (1=poor, 5=excellent) more than 70 % of the police users evaluated the sound and volume of the alerts as excellent or good. Sometimes the background noise was so loud that alerts could not be heard well. In the written comments users mentioned that in a real situation the vibration and silent alerts would be useful. Vibration helped to notice alerts in noisy situations. The alerting sound and icon gave to the users the first information about the incident, and the textual message gave additional information about it.

Table 2 presents the users' reaction times to all alerts. Data has been taken from the log from the server and it indicates the time between sending the alert and getting a receipt about it from the user. The table shows average reaction times for all alerts without separating them into categories. When day and night time alerts as well as voice and silent alerts are viewed separately, reaction times vary.

More than 60 % of users signed all alerts in less than two minutes and more than 70 % in less than five minutes. Some of the 25.1 % of users whose reaction time was more than ten minutes or who did not sign some alerts at all have according to the log obviously not carried the test phone with them after the office hours. In that case they have not been able to sign alerts in the evening or at night.

The visual map view gave to the leading police officer a good comprehension of the course of the action after giving the alert to the other police officers. The map showed instantly where geographically the police officers were and how fast they could be got on duty to handle the crisis.

Table 2: Shares of different reaction times in the test with the police (N=195)

Less than 2 minutes	64.1 %
More than 2 and less than 5 minutes	8.7 %
More than 5 and less than 10 minutes	2.1 %
More than 10 minutes or no signature at all	25.1 %

3.2 Case study with the police and civilian people

In the second test police send mobile emergency alerts to the private citizens. The test group was formed from twenty-five volunteers who were searched through various mailing lists and a short introduction about the system was given to them by a written document and email. The testers' age varied from 20 into 60 years or older. People were very eager to participate in the test with the police. Sillem and Wiersma (2006) had also noticed that earlier in their own studies and say that people are open for new technologies and very keen to participate in a research about citizens warning.

The police sent location based emergency notifications to the test group around the City of Jyväskylä and wider. Most notifications were given with a tight geographical limitation and directed into different sub areas of the city. The range of the widest alerts was 500 kilometers and they reached the City of Helsinki in the South, Arctic Circle in the North, Russian border in the East and Sweden in the West.

The purpose of the study was to gain empirical knowledge about how smartphone alerts should be given by the security authority to the population. The test simulated real emergencies and after the study information was collected from the users with an internet survey. Test alerts warned users for traffic accidents and jams, armed and dangerous persons, intruders, escaped criminals, missing persons, industrial fires and for spoiled drinking water. The police were also prepared for giving authentic alerts to the test users and on 21.12.2012 at 8:11 the Central Finland Police Department gave its first authentic smartphone alert by warning people for a severe traffic accident on the Vaajakoski motor highway. This alert was at the same time the first real smartphone based warning message from the Finnish Police to the civilian people ever.

The range of the alerting area, visualization and the alerting tone of the message were decided individually each time depending on the type of the incident. Also the two-way communication was tested in order to help the work of the police. For example, users were informed about a dangerous person in their neighborhood and asked if they had seen the person.

The civilian testers were active technology users and almost all used in the test their private phones. When the users were asked to answer the internet survey after the test, the response rate was 90%.

One of the questions enquired about the users' experiences of severe and dangerous situations and about the tested system's usefulness in those situations. A half of the users had experienced dangerous situations and evaluated that a smartphone based warning system would have been of help in those cases. Some results of the questionnaire are presented in Table 3.

Table 3: Civil users' evaluations concerning the tested alarm system (1 = poor, 5 = excellent) (N=20)

Question	**Average**	**Variance**
Overall usability of the alerting system	3.95	0.47
Easiness of the interpretation of the messages	4.25	0.72
Usefulness of the messages	3.42	1.26
Personal relevance of the messages to the user	2.90	1.36
Superiority of the application-based alerting compared to SMS messaging	4.39	0.49
Possible constraints in taking the system in real use (1 = very much, 5 = none)	3.26	0.94
The system's ability to improve the user's personal feeling of safety	3.65	0.87
Gained benefits compared to the required effort of using the system	4.10	1.25
Recommendation of taking a finalized system in real use	4.65	0.34

3.3 Case study at the school

The third pilot was carried out in a school because the school violence has been discussed a lot lately and because the school differs from the other tests with the police. Test users were teachers and other personnel of the school but as the environment was full of underage children that caused special requirements for the test. Users were introduced to the use of the system in a face to face group meeting at school.

Arranging physical protection in schools is a separate issue whereas this study focused on giving security alerts in schools. This study was arranged in Kilpinen school which represents an average school of the ca. 50 public schools in the city. The school building was built at the end of 1960's and there are nearly 500 children of 13–16 years old in that school.

The limitations of the building became obvious in the beginning of the study when the signal strength of the 3G mobile network appeared to be so weak inside the stony walls that the test could not be run on it. The 3G network was then strengthened so that the signal could be reached better inside the building but even that left some shadow areas inside the school. These were caused by the structure of inner walls and by some heavy objects which the school needed. The representatives of the city told that the signal strength of the 3G network may be weak even inside the newest schools because of the 3–4 layered energy saver windows. According to Waitinen's (2011) studies of the physical safety in primary and secondary schools in Helsinki good safety cultures include good safety management practices, well-developed understanding of safety hazards and the requirements of basic safety, open and communal safety-related work and an appreciation of safety evidenced through everyday practices.

Another obstacle in schools is that the employer may not have provided mobile phones for teachers or that the teachers are forbidden to use mobile phones in the class. Teachers may also not want to install security systems on their personal phones. Security alerts can be received also with tablet computers, PCs, smartboards etc. and from the technical point of view smartphones are not necessarily needed in class. For preventing panic and chaos amongst the children, it might however be better to give security alerts discretely to the teachers first. That is possible only with the teacher's personal devices which children cannot see or hear.

The personnel were asked about their attitude towards school safety before starting the study. According to the survey personnel wanted panic buttons into the school. Existing systems did however not enable installing more than two buttons in the building and a private company was ordered to install more buttons into the school. Also mobile buttons were given to the personnel. The call buttons were then integrated into the tested smartphone system so that all alerts which were made with the buttons would trigger an alarm on the test users' mobile phones.

During the test alerts were given with fixed and mobile panic buttons, call buttons which were built on the smartphones and through the alert system's user interface on the web. All alerts were directed to the school personnel's smartphones and the most serious alerts to the private security company. In the most serious incidents a 112 emergency call would be made to the emergency response center.

Table 4 shows the personnel's attitudes towards the school safety. Answers show that the teachers and other personnel are interested in security issues. Most interest was paid to panic buttons and some teachers, student counsellors and school nurses had asked for getting them in their offices and class already earlier. Especially the student counsellors and nurses work alone and sometimes they may need to call their co-workers for help to relieve the threatening situation. The tested smartphone based alerting system was not familiar in the school in advance but the personnel's attitude towards it was quite positive. The employer has provided mobile phones only for a small number of teachers, but if all teachers would have them they would be willing to install the security system on their phones. Many of them would however not want to install security systems on their private phones at school.

The survey showed also that even if many of the interviewed persons do not need a personal security system, they still want to install it for helping their colleagues. Attitude towards external security professionals is mixed. It looks like the personnel would like to handle threatening situations by themselves or that they see it as a police issue. It also looks like they are unwilling to call the private security company to the school because the school needs to pay extra each time when the security guard comes to the school. The services of the police are free but the police will be called for help only in serious incidents. All schools also have a named school police who visits the school regularly and gives security education for the pupils. When the researchers interviewed the school police he said that the personnel talks only about is the pupil's safety and not about themselves.

Table 4: Some examples of the personnel's attitudes towards school safety before starting

Statements	Average	Variance
Built-in panic buttons inside the building are a good enhancement in the school's safety	4.15	0.88
Panic buttons on the personnel's mobile phones are good enhancement in the school's safety	4.12	1.41
Mobile devices would suite well as the personnel's internal communication channel at school	3.53	1.39
I would take a mobile communication and security application in use on my phone at work	4.03	2.20
I would take a mobile communication and security application in use on my private mobile phone	3.50	2.26

4. Summary and conclusions

The study shows that even if the emergency is the same, smartphone based alerts need to be given in a different way in different environments and user situations. In the study user tests were made with police officers, adult aged private citizens and in a school of underage children.

One common feature with the three cases is that the society is not yet fully prepared for a wide implementation of smartphone based emergency systems. For example the open air mobile communication infrastructures are inadequate in some places which might cause problems for the full exploitation of mobile emergency systems. Mobile communication infrastructures are also vulnerable. If for example base stations will lose their energy supply or if they are destroyed, all mobile phones in the area will be muted. If however, there is an open WLAN available the tested kinds of smartphone based alerting systems will be able operate even if all base stations are down.

The study in the school pointed out that wireless infrastructures can be inadequate also inside the buildings. Although this was proved only in one building it is quite evident that in every country there are plenty of old or technically tricky buildings in which there are hundreds or thousands of people inside daily and that inside those buildings networks may not operate properly. Wireless networks are also vulnerable for overload, and when something bad happens the risk for overload will increase.

When public smartphone based emergency alerting applications will be installed widely also the peripheral devices may cause some problems. In this study all tests were made with standardized smartphones which operate on the Android platform. In a real situation the variety of mobile devices among the population is much bigger and not all of them are able to receive smartphone messages. With the tested alerting system these devices may be though reached with SMS. All people do also not have mobile phones at all or they are not allowed to use them at work.

When people receive smartphone based alerting messages, according to this study more than 60 % of them would react on them within the first two minutes. If the reaction time will be counted for voice alerts or night time alerts only the average reaction time will be even shorter. During the daytime voice alerts are distracted in many places by background noise and by many other tones and signals which disturb the detection and perception of emergency alerts. The vibration of the phone will improve the detection and it will be useful also in situations where voice alerts cannot be used. In the study best reaction times were received at night when 80 % of the test users signed alerts within the first minute. At the night time most of the users were at home in bed and there was no background noise which would have drowned the alerting sound.

Finally, even if the technology runs smoothly, the success of emergency alerting is dependent on the user him/herself. If the user does not care about the alerting message, or if he/she does not receive it in time because the alerting device is not in hands or if it is not working, the alert will not be noticed. In this study for 25 % of the test users it took more than 10 minutes to sign the alert and some did not sign all alerts at all. In these cases the users may not have carried the test device with them all the time. In a real situation, part of the people might be careless with their phones as well, and for that reason all people would not receive emergency alerts even if they would have a personal phone and even if the alert would reach their personal device.

The study concludes that smartphones are an appropriate and flexible alerting technology for many situations and in many ways they are better than several other technologies on the market. Alerting needs however be planned carefully according to the environment, user group and situation. One must also consider each time whether the benefit of the intended message would be bigger that the harm which it would cause. This decision has to be made also now when most of the public alerts are given by broadcasting methods, but when emergency alerts will be transferred to the private people's personal devices that decision will become even more important.

Acknowledgements
Authors wish to thank Tekes – The Finnish Funding Agency for Technology and Innovation, University of Jyväskylä, Magister Solutions, Parco Group, Jämsän Apteekki, and the European Regional Development Fund for funding this research. Authors also thank Central Finland Police Department, National Police Board and the City of Jyväskylä for their support and participation in this study.

References
Al-Akkad, A. and Zimmermann, A. (2011). User Study: Involving Civilians by Smart Phones During Emergency Situations. *Proceedings of the 8th International ISCRAM Conference*, Lisbon, Portugal.
Aloudat, A., Michael, K. and Abbas, R. (2009). Location-Based Services for Emergency Management: A Multi-Stakeholder Perspective. *Eighth International Conference on Mobile Business*, pp 143–148. ICMB.
Aloudat, A., Michael, K. and Abbas, R. (2011). Recommendations for Australia's Implementation of the National Emergency Warning System Using Location-Based Services. *Journal of Ubiquitous Systems & Pervaisive Networks,* Vol. 3, No. 2, pp 59–66.
Amailef, K. and Lu, J. (2011). A mobile-based emergency response system for intelligent m-government services. *Journal of Enterprise Information Management*, Vol. 24, No.4, pp 338–359.
Coombs, T. (2007). *Ongoing Crisis Communication: Planning, Managing, and Responding*. SAGE Publications, New York, NY.
Hughes, A., L. and Palen, L. (2009). Twitter adoption and use in mass convergence and emergency events. *International Journal of Emergency Management*, Vol. 6, No. 3-4, pp 248–260.
Häkkinen, M. (2010). *Why alarms fail: a cognitive explanatory model*. Doctoral thesis. Jyväskylä studies in computing, 127, University of Jyväskylä, Finland.
Kaasinen, E. (2005). *User acceptance of mobile services - value, ease of use, trust and ease of adoption.* VTT Publications.
Kuula, J., Räsänen, J., Kettunen, P., Kauppinen, O. and Panasenko, V. (2012). Mobile Emergency Messaging and the Vulnerability of Crisis Communication. *Proceedings of the NBC 2012 – 8th Symposium on CBRNE threats: How does society scope,* Turku, Finland, June, pp 11–14.
Kuula, J., Auvinen, V., Kauppinen, O, Kettunen, P., Viitanen, S. and Korhonen, T. (2013). Smartphones as an Alerting, Command and Control System for the Preparedness Groups and Civilians: Results of Preliminary Test with the Finnish Police. *Proceedings of the 10th International ISCRAM Conference,* Baden-Baden, Germany, May.
Lee, J., Niko, D., Hwang, H., Park, M. and Kim, C. (2011). A GIS-based Design for a Smartphone Disaster Information Service Application. *First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering. IEEE*
Meissen, U., Voisard, A. (2008) Increasing the Effectiveness of Early Warning via Context-aware Alerting. In: Fiedrich, F.; Van de Walle, B. *Proceedings of the 5th International ISCRAM Conference*, pp 431–440.
Muralidharan, S., Rasmussen, L., Patterson, D. and Shin, J.-H. (2011) Hope for Haiti: An analysis of facebook and twitter usage during the earthquake relief efforts. *Public Relations Review*, Vol. 37, No. 2, pp 175–177.
Sillem, S. and Wiersma, E. (2006). Comparing Cell Broadcast and Text Messaging for Citizens Warning. *Proceedings of the 3rd International ISCRAM Conference*, Newark, NJ (USA), May.
Vihalemm, T., Kiisel, M. and Harro-Loit, H. (2012). Citizens' Response Patterns to Warning Messages. *Journal of Contingencies and Crisis Management*, Vol. 20, No. 1.
Waitinen, M. (2011). *Turvallinen koulu?: Helsinkiläisten peruskoulujen turvallisuuskulttuurista ja siihen vaikuttavista tekijöistä*. Helsingin yliopisto, Unigrafia.
Wu, P. F. (2009). User Acceptance of Emergency Alert Technology: A Case Study. *Proceedings of the 6th International ISCRAM Conference* – Gothenburg, Sweden.
Yamasaki, E.(2012).What we can learn from Japan's early earthquake warning system.*Momentum*, 1.