Information Influence in Society's Information Environment: An Empirical Analysis Using the Grounded Theory

E Mustonen-Ollila[1], MJ Lehto[1], J Heikkonen[2]

[1]Faculty of Information Technology
University of Jyväskylä
Jyväskylä, Finland

E-mail: erja.mustonen-ollila@quicknet.inet.fi; martti.lehto@jyu.fi

[2]Department of Future Technologies,
University of Turku
Turku, Finland

E-mail: jukka.heikkonen@utu.fi

***Abstract**: This paper investigates information influence in society's Information Environment. The Grounded Theory approach was used to collect and to analyse the data. A conceptual framework of the thematic categories and item categories was developed on the basis of empirical evidence and past studies that reflect the findings of the field. The most fundamental components in this conceptual framework were six thematic categories (information influence, information operations, cyber operations, psychological operations, kinetic operations, and deception), their item categories, the items themselves, and the interrelationships between the thematic categories. The propositions regarding the thematic categories and the interrelationships between them showed 13 higher levels of abstractions of statements in the conceptual framework, which was a unique result of this study*.

Keywords: *Information Influence, Society, Information Environment, Information Operations, Cyber Operations, Psychological Operations, Deception, Kinetic Operations, Grounded Theory*

Introduction

Information influence aims to systematically influence public opinion, human behaviour, and decision-makers, thus affecting the functions of society. The means of influencing through Information Operations (IO) are, for example, the distributing and highlighting of false and misleading information. This activity aims to steer the target to make harmful decisions against its own interests. Information influence can, in general, be produced by state or non-state actors and by different organisations.

This study uses the following definition of IO:

> The integrated military operations in which information is used in operations to influence own decision-making and get desired effects on the will or defend itself from enemies',

> potential enemies', decision-makers', cultural groups', and international communities' information operations and impact. (Armistead 2004, p. vii)

To counter information influence in the Information Environment (IE), it is crucial to identify and to analyse the possible different forms and levels of information influence and IO within the IE. In this study, IE is defined as

> Information, aggregate of individuals, organizations, and systems that receive, collect, process and convey/disseminate the information, or act on information, and the cognitive, virtual and physical space in which this occurs. (NATO 2012, p. 3)

The focus of this study is on society's IEs, in which a society is defined as "a group of individuals involved in persistent social interaction, or a large social group sharing the same geographical or social territory, typically subject to the same political authority and dominant cultural expectations" ('Society' 2018).

Past studies (NATO StratCom COE 2016, 2015; Lehto 2014; Tähtinen 2013; Sigholm 2013; NATO 2012; Armistead 2004; Rantapelkonen 2002) show that a great deal of studies on information influence and IO in IEs exist, but that qualitative research of the origins of information influence and IO and how a society becomes aware of them is lacking. In order to obtain a clear understanding of their impact, information influences and IO must be examined in a real society. Such an investigation would improve the understanding of the new possible information influences and IO of the future. This study addresses some of the issues previously mentioned. Its goal is to describe in detail the different information influences and IO that society has faced, the extent to which these information influences and IO are shaped by the IE context, and how these information influences and IO are interrelated.

In this study, past studies and empirical evidence are applied in a qualitative in-depth case study (Yin 2003) that identifies the information influences and IO in a society's IE. The collected data were analysed using the Grounded Theory (GT) approach and a conceptual framework was developed with thematic categories, item categories, and the relationships among these (Glaser & Strauss 1967).

The GT approach follows different phases of data analysis and uses content analysis as part of its categorisation method as follows: 1. Identify thematic categories in the empirical data using content analysis. 2. Define the thematic category based on the empirical data. 3. Search for appropriate literature to be used as evidence for the identified thematic category. 4. Search for similar thematic categories in the empirical evidence to enable mutual exclusion (it is not wise to use thematic categories that use the same definition but are labelled [titled] differently). 5. Search for relationships between the thematic categories. 6. Determine a higher level of abstraction of statements about the relationships between the thematic categories and propositions for the categories. These statements are based on empirical evidence. 7. Create a conceptual framework of thematic categories and their relationships in order to visualise results. The final product resulting from creating a theory from the case studies may be a concept, a conceptual framework or propositions, or possibly a mid-range theory (Eisenhardt 1989; Mustonen-Ollila & Heikkonen, 2009; Mustonen-Ollila,

Lehto & Heikkonen 2020a; 2020b). According to Eisenhardt (1989), the combination of case study and GT approaches has three major strengths: it produces a novel theory; the emergent theory is testable; and the resultant theory is empirically valid (Mustonen-Ollila & Heikkonen 2009). GT is used in interpretive studies and can be extended to inductive theory creation (Mustonen-Ollila & Heikkonen 2009).

The data should be categorised under several identifiable themes. These themes can also form the main categories or concepts in the data. This is a selective way of finding the concepts and categories in the data and is based on the researcher's own intuition or knowledge. The concepts must be categorised according to relevant terminology and theories that form the most refereed work in categorising concepts in the research area. After the categories have been discovered, their number must be decided upon. The problems with the categories are whether enough proof can be found in the data to make them and the concepts valid and reliable, and whether the concepts and categories discovered are the correct ones. Some other concepts and categories may emerge from the data later. If the concepts and categories are not correct, the researcher must return to the data and discover new concepts. After the abstract concepts are found, they can be coded according to the instructions of Glaser and Strauss (1967), using selective coding to search the data categories. The abstract concepts can also be found using the content analysis approach (Krippendorff 1985), which is a text analysis method. The approach requires the researcher to construct a category system, to code the data, and to calculate the frequencies or percentages that are used to test the hypotheses on the relationships among the variables of interest. It is assumed that the meaning of a text is objective, in the sense that a text corresponds to an objective reality (Mustonen-Ollila, Lehto & Heikkonen 2020a; 2020b).

The text is interpreted and understood without extraneous contextual knowledge. In case studies such as this one, the concepts are sharpened by building evidence that describes them. The data and concepts are constantly compared so that accumulating the evidence converges on simple and well-defined concepts—that is, categories or constructs. In this study, the constant comparison between data and the concepts in past studies, in order to accumulate evidence converged on simple, well-defined thematic categories, led to a higher level of abstraction of statements about the relationships between the thematic categories. This theorising was in line with Pawluch and Neiterman's (2010) suggestions of creating a GT using Glaser and Strauss's (1967) approach, in which intuition and knowledge are also used to determine the categories and a chain of evidence is created: the thematic categories are derived from the empirical data and then validated using past studies. In this study, Pawluch and Neiterman's (2010) GT analysis instructions, together with those of Glaser and Strauss (1967), support the finding of categories from data and their being based on the researchers' own intuition and knowledge.

Each thematic category was further broken down into multiple traits (items) by deriving the items from the data and validating them with past studies. The total number of item observations was 411, and they were categorised using GT analysis (Glaser & Strauss 1967) and content analysis (Krippendorff 1985). The thematic categories were information influence, IO, cyber operations, psychological operations, deception, and kinetic operations. The information influence category was the highest-level category and consisted of 16 different information influence item categories and 77 empirical item observations. Information influence also contained an IO subcategory. The

IO category contained 18 different IO item categories and 75 empirical item observations. It also contained four subcategories, each of which contained the following item categories and empirical item observations. Cyber operations, for example, information influence operations occurring in cyber environments (Lehto 2015; Ottis 2015), consisted of 14 item categories for 137 empirically supported item observations. The psychological operations category, that is actions and means that aim to influence the opinions, minds, and behaviour of the target audience either directly or indirectly (Saressalo 2012, p. 3), consisted of eight item categories for 109 empirically supported item observations. The deception category, defined as a tactic to distract and delay and in which the influencing method of IO is military deception (Bachmann & Gunneriusson 2015; Saressalo 2012), consisted of two item categories for four empirically supported item observations. Finally, kinetic operations, defined as the physical destruction of the target carried out by military forces, terrorists, or intelligence operatives working for the government (Renz 2016; Information Operations 2012; Saressalo 2012; NATO 2009; Armistead 2004), consisted of one item category for nine empirically supported item observations. The 1–18 multiple item types (item categories) in each thematic category amounted to a total of 59 different item categories. Evidence was found for the propositions in terms of the thematic categories and relationships between the thematic categories. Finally, 13 higher levels of abstraction of statements were found in the conceptual framework.

The rest of the paper is organised as follows: the next section discusses the related research. Next, the authors present the research method; after which the following sections outline data categorisation and show the data analysis. Finally, the authors offer discussion and conclusions.

Related Research

Information influence includes trolling information on the Internet and then spreading incorrect information. Trolls can be people or trolling factories, or the exercising of propaganda by supporting rulers in Internet discussions (Bachmann & Gunneriusson 2015; Luoma-aho 2015). Information influence occurs at different levels and can be carried out through IO (Secretariat of Security Committee 2018). IO refers to an organised series of actions by which influence on information and information systems is supported and coordinated in order to achieve a certain goal. One type of influence is pressure targeted towards a society's vital activities, activities of the enemy's economy systems, energy supply, and logistics' functions (Tähtinen 2013; Hollis 2011; Armistead 2004). Luoma-aho (2015), Lehto (2015, 2014), Sirén, Huhtinen & Toivettula (2011) and Armistead (2004) claim that public relations influence is targeted at both domestic and foreign media as well as audiences. During wartime, this is to prevent receiving or sending the adversary's own messages before, during, and after war operations. In order to influence public opinion or to blur the truth, information is deliberately and often covertly spread as rumours ('Disinformation' 2017; Bachmann & Gunneriusson 2015; Kantola & Hämäläinen 2013).

The new tools of social media can also be used by immoral actors for illegal purposes of undermining stability. In social media, hoax messages are connected to legitimate messages, and they spread very quickly via mobile apps and text services, disseminating false information (Goolsby 2013).

Bachmann and Gunneriusson (2015), and Sirén, Huhtinen & Toivettula (2011) argue that IO are non-lethal performances that are targeted at enemies' management and communication systems and propaganda machines in order to disturb, prevent, and destroy these systems and processes.

Information systems are linked together through information networks and hacking into these systems causes confidential information to leak out, information to be misused, or information systems to become crippled by denial of service**.** Military systems, fighters, cruise missiles, and anti-aircraft systems are dependent on complex real-time data processing (Puttonen 2015; Ojala 2014; Holt & Kilger 2012). According to Salminen (2018), information technology control reaches beyond ICT and the Internet, and creates a new, specific way in which to influence, which is called cyber physical influence.

Cyber operations can use cyber weapons, which form military-grade, world-class malicious software in information networks and cause a great deal of damage to enemies. Cyber weapons use code clusters, which make it possible to bring down foreign states' electronic networks by attacking them through information networks. They can bring down net banks and information networks by adjusting the control logistics of oil transport, in order to cripple states and their critical infrastructures (Geers 2015; Mäntylä 2014; Ojala 2014; Isometsä 2013).

According to Lehto (2015), Geers (2015), Jaitner (2013), Nissen (2012), and Berger (2010), hard cyberattacks are carried out as Denial-of-Service attacks (DoS); Distributed Denial-of-Service (DDoS) attacks include damaging government websites (strategic attacks) and preventing their services; hacking emails and mobile phones; using false social media accounts; using botnets; manipulating audio visual material; conducting espionage; committing identity theft and disseminating propaganda; and destroying critical infrastructures and control systems. Hard cyberattacks are viruses, worms, trojans, hacking, and kracking (Lehto 2015; Geers 2015; Jaitner 2013; Nissen 2012; Berger 2010). Lehto *et al.* (2017) state that hard cyberattacks can also be attacks on the Internet of Things (IoT), cloud services, Big Data, devices using mobility and Bring-Your-Own Device (BYOD) philosophy-using devices.

Huhtinen and Rantapelkonen (2016), Renz (2016), Paavola *et al.* (2016), Lehto (2015), Sartonen, Huhtinen & Lehto (2015), Saressalo (2012), Hollis (2011), and Berger (2010) state that pressure using military power and deterrence are psychological operations, and that soft psychological operations can consist of social engineering, control, data gathering, psychological operations, and propaganda.

IO also include kinetic operations denoted as the physical destruction of the target carried out by military forces, terrorists, or intelligence operatives working for the government (Information Operations 2012; NATO 2009; Armistead 2004).

Thus, despite a large amount of excellent past studies on information influence and IO, the literature has largely neglected the relationships between information influence and IO. Past studies have focused on different types of information influences and IO in general. Therefore, this study responds to the need for further research, and offers both practical and theoretical knowledge on information influence and IO in a society's IE, exploring their relationships with information influence and IO.

An extensive analysis of past information influence and IO research thus leads the researchers to formulate two research questions (RQs): 1) What are the information influences and IO in a so-

ciety's IE? 2) How are the information influences and operations in a society's IE related to each other?

Research Method

A qualitative case study (Yin 2003; Creswell 2007) using the GT approach (Eisenhardt 1989; Glaser & Strauss 1967) was chosen to help answer the two research questions. The unit of analysis in this case study was the IE of a specific society. Due to research limitations, the sample consisted of only 10 interviewed experts, who represented eight different organisations in Finland. When qualitative data reached saturation point, data collection ended. The saturation point means that a theoretical saturation point has been reached, that is, even if new data are collected, they would offer no new knowledge about the studied phenomena (Glaser & Strauss 1967). In this study, this point was reached when the same categories started to be repeated in the data.

Nine audio-recorded, unstructured, and semi-structured interviews (Metsämuuronen 2006) were conducted, which investigated experiences of information influences and IO. These interviews (described in **Table 1**, below) consisted of eight individual interviews and one two-person group interview between January and May 2018. The interviewees were or had been involved in several civil and military information influence activities and IO in their own fields of expertise during their working careers, which extended over a period of 6 to 30+ years, in different positions and organisations in Finland and abroad. Archival material was also studied (Metsämuuronen 2006), representing a secondary source of data, which included public news and past scientific studies on the information influences and IO in Finland or abroad. Triangulation (Yin 2003) was used to combine different data sources simultaneously to improve the reliability and the validity of the data.

Each interview transcript was analysed, and the major emergent themes and concepts were identified in order to form categories (Myers & Avison 2002). The interviewees received the questions before the interviews in order to become familiarised with them beforehand (Creswell 2007), and they could check their content in order to reduce mistakes. After each interview, the interview questions were improved to better suit the next interview.

Interviewee number	Role of interviewee	Length of interview in minutes	Group or individual interview
1	Chief of Cyber Division	215	Individual interview
2	Military Professor	235	Individual interview
3	Civilian Security Officer	151	Individual interview
4	Civilian Official & Senior Adviser of the Security Committee	135	Group interview
5	University Teacher	31	Individual interview
6	Expert of the Security Committee	66	Individual interview
7	Military Professor	117	Individual interview
8	Officer of the Defence Command Finland	200	Individual interview
9	Researcher (Digitalisation, Cyber Security)	181	Individual interview
Total:		1341	

Table 1: Interviewee details

Data Categorisation

The audio-recorded interviews included frequent elaboration and clarification of the meanings and terms and were transcribed, yielding over 240 pages of transcriptions. A qualitative research method based on GT (Glaser & Strauss 1967) and content analysis (Krippendorff 1985) were applied. The data were categorised under the thematic categories of information influences and IO, and four IO subcategories, according to relevant terminology and theories from the research area.

After drawing the hierarchy of the six thematic categories, each thematic category was further broken down into multiple items (traits) using content analysis. These items were derived from the data and validated using past studies. In this specific analysis phase, information influence and IO definitions and past studies were used to determine which items belonged to each specific thematic category. A chain of evidence was created: all the information influences as well as IO and their subcategories were derived from the empirical data, and all of them were validated using past studies. An example of an item observation concerning the 'Information Influence' category is presented in **Table 2**, below. In **Table 2**, the first column contains the definition of an information influence item derived from the empirical evidence; the second column contains the empirical evidence for the item; the third column contains the evidence from the literature for the item in the second column; the fourth column contains the name of the literature source of the third column; and finally the fifth column contains the transcript number of the empirical evidence.

Item definition derived from empirical evidence: item category	Empirical evidence of item	Evidence from literature of item in second column	Literature source	Transcript number
Politicians' confrontation to justify issues	IO between politicians, confrontation to justify the issues. These kinds of set-up are built from this knowledge over a long period of time.	The new tools of social media can also be used by immoral actors for illegal purposes to undermine stability. In social media, hoax messages are connected to legitimate messages, and they spread very quickly via mobile apps and text services, disseminating false information.	Goolsby, 2013, pp. 1–8	TC9

Table 2: Example of item observation concerning the information influence category

Table 3, below, shows the six thematic categories and their item types (called item categories). The first column consists of item categories for each thematic category; the second column shows the sum of the item observations; and the third column shows the item number. Each item category contains a different number of observations. **Tables 4–8**, below, follow the same procedures as **Table 3**. A total of 411 different empirical observations under 59 categories were found using Glaser and Strauss's (1967) GT analysis and Krippendorff's (1985) content analysis instructions, which support the finding of categories based on data and on the researchers' own intuition and knowledge.

Information influence consisting of item categories	Sum of item observations	Item number
Confrontations, mood battles	20	1
Social media influencing	22	2
Hindering authorities' work	3	3
Foreign media-minded media influencing	7	4
Modifying the Information Environment	4	5
Modifying the atmosphere in companies	5	6
Preventing legal issues	3	7
Influencing research and science	3	8
Burst influencing	1	9
Discussions of superpowers influencing Finland	1	10
Influencing citizens' daily lives	1	11
Western influencing	1	12
Influencing outside state and society	2	13
Influencing other countries' coalitions	1	14
Influencing from inside society	2	15
Influencing human beings' communication	1	16
Total:	77	
Total number of item categories:		16

Table 3: Thematic category of 'Information influence' and its item categories

Information operations (IO) consisting of item categories	Sum of item observations	Item number
Influence of culture and modifying local environment	4	1
IO in war	4	2
IO against own citizens living in another country	3	3
IO against own citizens	6	4
Media's IO during war	3	5
Media's IO in organisations	3	6
National advertising, information blows to own citizens	13	7
IO by politicians	6	8
IO by the press	5	9
IO to weaken the state	5	10
IO against human beings	1	11
IO against allies	1	12
IO against enemies	1	13
IO against the whole world	1	14
Enemies' IO against Finland	2	15
IO against peacekeeping	3	16
Enemies' IO against countries other than Finland	1	17
Aggressive military IO	13	18E
Total:	75	
Total number of item categories:		18

Table 4: Thematic category of 'Information Operations' and its item categories

Cyber operations consisting of items categories	Sum of item observations	Item number
IoT attacks	2	1
IS hacking	3	2
Hard cyberattacks	20	3
Cyber weapons	16	4
Blackmail programs	2	5
Information networks intelligence	6	6
Cyber intelligence	4	7
Cyber espionage	5	8
Cyber operations	28	9
Cyberattacks	5	10
Network attacks	38	11
Security violations	4	12
IT control over ICT and the Internet	2	13
Cyber threats	2	14
Total:	137	
Total number of item categories;		14

Table 5: Thematic category of 'Cyber operations' and its item categories

Psychological operations consisting of item categories	Sum of item observations	Item number
White psychological war	6	1
Grey psychological war	8	2
Black psychological war	24	3
Propaganda, rumours	19	4
Trolling	16	5
Reflexive control	1	6
Psychological influencing	2	7
Threats of war	33	8
Total:	137	
Total number of item categories:		8

Table 6: Thematic category of 'Psychological operations' and its item categories

Deception consisting of item categories	Sum of item observations	Item number
Deception in war situation	3	1
Preventing enemies' transmissions	1	2
Total:	4	
Total number of item categories:		2

Table 7: Thematic category of 'Deception**'** and its item categories

Kinetic operations consisting of item categories	Sum of item observations	Item number
Kinetic operations	9	1
Total:	9	
Total number of item categories:		1

Table 8: Thematic category of 'Kinetic operations' and its item categories

Data Analysis

After data categorisation and data collection, the conceptual framework of the discovered categories was formulated on the basis of the empirical evidence and theories reflecting the findings in the field (Glaser & Strauss 1967). The suggestions of Glaser and Strauss (1967) were followed to involve fragmentation and to reassemble the data into thematic categories by trying to capture a broader conceptual foundation based on the interviewees' experiences and practical knowledge of information influences and IO.

Figure 1, below, shows the thematic categories as ellipses, and the relationships between the thematic categories are marked by solid lines with letters (A to I). The small arrows with numbered circles pointing to the thematic categories are the multiple items (traits) of each category composed by content analysis.

After finding the thematic categories and their relationships, the properties of the categories and propositions (hypotheses) regarding how they were related to each other on the basis of the data were determined (Glaser & Strauss 1967). Due to their vast number, **Table 9**, below, presents only some examples of these relationships in detail, based on the empirical data.

The data and thematic categories and their item categories were constantly compared with each other, and this comparison led to 13 higher levels of abstractions of statements about the relationships between the categories. The higher level of abstraction of statements is presented in the conclusions and discussion section.

Discussion and Conclusions

Based on eight individual and one two-person group in-depth interview, this study tackled the information influence issues in a society's IE. The interview questions were improved many times, and sometimes, due to the schedule of the interviewee, shortened. The largest interview consisted of 70 questions, and the shortest consisted of 30 questions. The interviewees recommended new interviewees, because they knew who it would be useful to interview.

In this study, the GT analysis (Glaser & Strauss 1967) found evidence of six thematic categories in a society's IE, using the inductive approach. The thematic categories (information influence, IO, cyber operations, psychological operations, deception, and kinetic operations) were improved by evidence discovered from collected empirical data, which identified items for the thematic categories and further identified that these items had been categorised into different classes. Glaser and Strauss (1967) claim that constant comparison of concepts and data showed evidence of new item categories. The decomposition of each thematic category into multiple items (traits) using content analysis helped derive new item categories and validate them using past studies and respected definitions. After the item categories were determined, the properties of the thematic categories and propositions (hypotheses) regarding how they were related were defined.

Finally, a conceptual framework of the thematic categories and item categories was developed on the basis of empirical evidence and past studies reflecting the findings of the field. The most fundamental components in this conceptual framework were the thematic categories, item categories, the items themselves, and the relationships between the thematic categories. This hierarchical item category classification was a unique result of this study, because it showed so many different influences and operations.

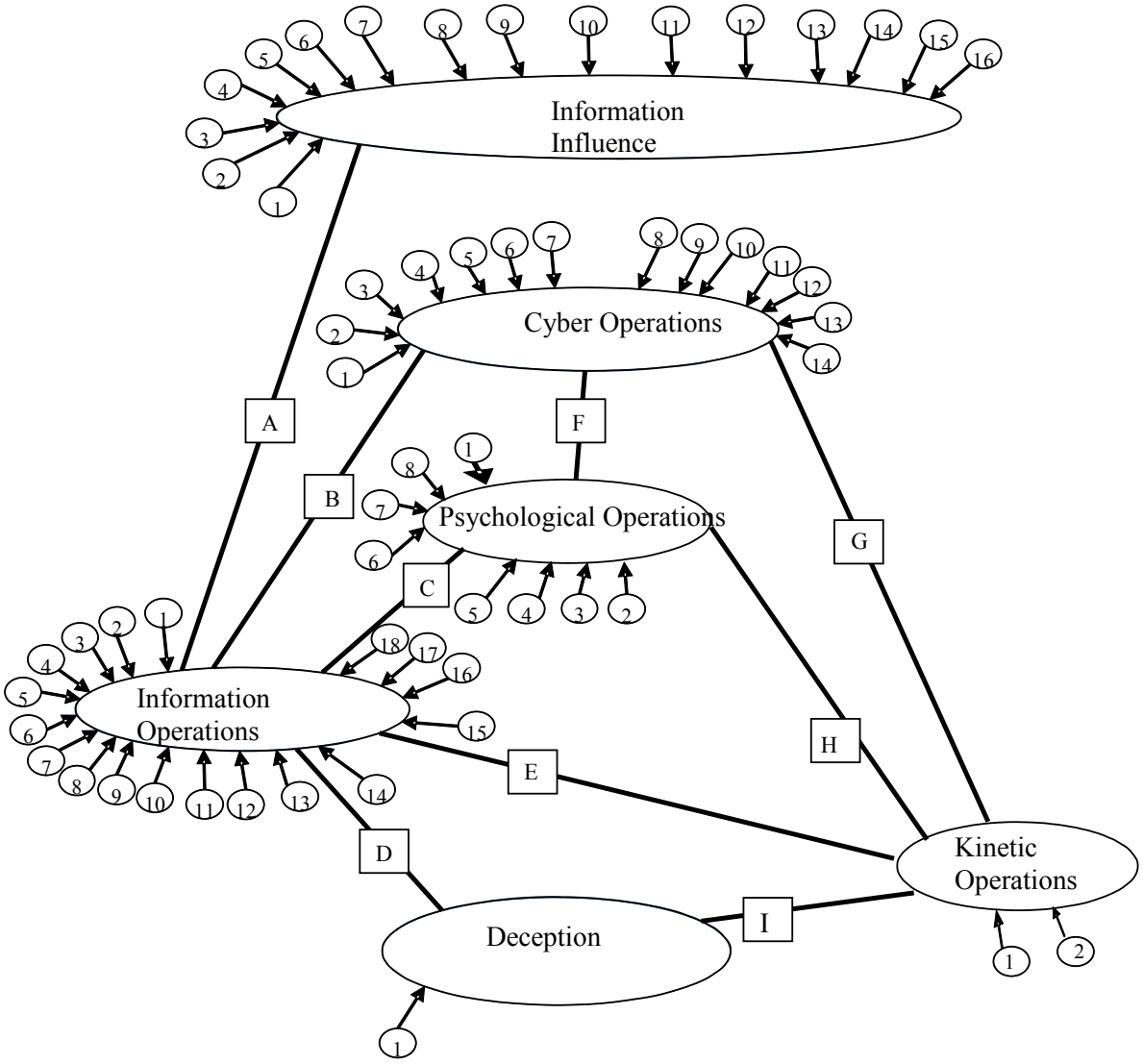

Figure 1: Conceptual framework of six thematic categories and their item categories

Thematic category/categories	Properties of thematic categories and propositions (hypotheses) regarding how the categories are related (lines marked with letters A to I in Figure 1) on the basis of data	Lines marked with letters in Figure 1
Information influence, IO	The strategy can be understood in many ways in this situation, but generally in such an IO, the probable method used is the personal approach. This is very close to acquaintanceship.	A
IO, cyber operations	Cyberattacks become important when an ordinary person is going to a shop to buy food and cannot get it or cannot pay his or her bills.	B
IO, psychological operations	It may be that some things go unseen. It can be that a person's activity and information is given, leaked, or the actor gains an advantage from the information.	C
Information influence, IO, deception	Deception is a military operation (MILDEC).	A, D

Thematic category/categories	Properties of thematic categories and propositions (hypotheses) regarding how the categories are related (lines marked with letters A to I in Figure 1) on the basis of data	Lines marked with letters in Figure 1
Information influence, IO, kinetic operations	One kind of IO is when somebody threatens to carry out small kinetic attacks, all around European small cell strokes.	A, E
Cyber operations, psychological operations	Emails are filled with spam and phishing messages and are smarter, because they come through filters and telecommunications.	F
Information influence, IO, cyber operations, kinetic operations	The state department's computers had an espionage program for years until one friendly western country said 'you have an (cyber) espionage program in your computer'.	A, B, G, E
Psychological operations, kinetic operations	Social media is used to threaten war, support warfare actions, or justify war.	H
Information influence, IO, psychological operations	In psychological warfare, some people's feelings are influenced so that the goal is achieved through mental pressure.	A, C
Information influence, IO, cyber operations	Hackers are carrying out a cyber operation when they penetrate the server of the democratic party and download all its content.	A, B
Information influence, IO, cyber operations, psychological operations	After hacker penetration, the hacker gives the downloaded emails on a memory stick to the psychological operator, who is the actor of the IO. This expert understands who is talking to whom, what information is confidential and sensitive, and what information is not. The expert plans when this information will be published and in what context, and what kind of influence this operation aims for.	A, B, F, C
Information influence, IO, psychological operations, kinetic operations, deception	When warfare is alienated in reality, be it physically, through assassinations or some other cyber operations, it seems far away and unlikely that anyone can use these methods in the real world. A close eastern neighbour uses all possible methods during war and would capitalise on any gullibility.	A, C, H, I
Information influence, IO, psychological operations, deception	It is possible to keep one's own issues secret at the same time as (psychological operation ability) deception. Then, operation security is the culture of the whole organisation.	A, C, J, D
Information influence, IO, cyber operations, psychological operations, kinetic operations	A cyber operation influences in a different way to psychological influencing because its goal is to damage systems and other things. Cyber issues involve nerds and psychological operations involve masterminds.	A, B, F, H, I
Cyber operations, psychological operations, IO, information influence	In organisations, traditional hacking and cyber security know-how has increased so much that penetrating the systems is more difficult. It is easier to take advantage of the human dimension. People say incomprehensible things on the phone.	F, C, A

Table 9: Properties of thematic categories and propositions (hypotheses) on how information influence and the IO categories are related on the basis of the data

The result was evidence of six thematic categories, and the finding of 411 item observations and 1-18 multiple item types (item categories) for each thematic category consisting of a total of 59 different item categories, propositions regarding the thematic categories, and the relationships between them. The comparison with past studies led to 13 higher-level abstractions and statements about the relationships between the thematic categories. This theorising was in line with the advice of Glaser and Strauss (1967) on how to create a GT by deriving it from empirical data and letting it emerge from the data.

The 13 higher level abstractions found were as follows: 1) It is very difficult to know when a specific information influence or IO has started, what its goals are, and who it is targeting; 2) In a

certain action, either an activity or a person can be the target of any kind of information influence and the targets may not even know that they are being influenced by someone; 3) It is difficult to see what background forces are driving the influences and operations and what their political goals are; 4) Society's IE, decision-makers, and people are being undermined by information influences and information; 5) Cyber operations have led to questioning the ability of society to handle the crises that cyber operations cause; 6) Crisis situations test decision-makers' abilities to do things correctly when the critical infrastructure is hacked; 7) The conflicts caused by the moods of politicians, decision makers, and influential people can prevent them from making proper decisions; 8) During wartime, the goal of information influences and IO is to affect enemies directly by weakening their sprit to fight. 9) Information influences, IO, and psychological operations may also be targeted at one's own citizens and can either directly or indirectly influence IE; 10) The aim is to shape the IE so that society will divide against itself and external forces can rule politics and the economy; 11) The actions of social media and the normal media are critical because, in social media, news spreads extremely fast and the other media does not always check the truth or reliability of the social media information; 12) In psychological operations and influences, the goal is to influence citizens so that they give in to psychological pressure and give up unless they have enough support, criticality, and common sense to trust their own situation awareness and understanding of things; 13) The actors are somewhat hidden while working at different levels of society or outside society, coordinating these influences and operations carried out at different levels and aimed at different types of people in society, although they do exist and try to influence strongly.

This study is in line with those of Bachmann and Gunneriusson (2015) and Luoma-aho (2015), who state that information influence includes trolling information on the Internet, that trolling is used to spread incorrect information, and that trolls can be people or trolling factories exercising propaganda by supporting rulers in Internet discussions. The findings also support the claims of Armistead (2004), Tähtinen (2013), and Hollis (2011) that one type of influence consists of pressure that is targeted at society's vital activities, the activities of the enemy's economy systems, energy supply, and logistics functions; as well as those of Luoma-aho (2015), Lehto (2015, 2014), Sirén, Huhtinen & Toivettula (2011), and Armistead (2004) that public relations influence is targeted at domestic and foreign media and audiences, and, during wartime, at preventing the adversary's own messages from being received and sent before, during, and after war operations.

This study confirms the claim of "Disinformation" (2017), Bachmann and Gunneriusson (2015), and Kantola and Hämäläinen (2013) that information is deliberately and often covertly spread as rumours in order to influence the public opinion or blur the truth; that of Goolsby (2013) that the new tools of social media are also used by immoral actors for illegal purposes to undermine stability and to spread hoax messages that are connected to legitimate messages; and that hoax messages spread extremely quickly in mobile apps and text services, disseminating false information. The findings were also in line with those of Bachmann and Gunneriusson (2015), and Sirén, Huhtinen & Toivettula (2011) that IO are non-lethal performances that are targeted at enemies' management and communication systems and a propaganda machine that aims to disturb, prevent, and destroy these systems and processes. In addition, the result confirmed those of Puttonen (2015), Ojala (2014), and Holt and Kilger (2012), which found that information systems are linked together by information networks and that hacking into information systems can cause confidential information to leak out, information to be misused, or information systems to become crippled by denial of service. Military systems, fighters, cruise missiles, and anti-aircraft systems are dependent on complex real-time data processing.

The empirical evidence also confirmed that ICT control is moving beyond ICT and the Internet, and that this is causing a new, specific way of influencing, called cyber physical influence (Salminen 2018). It also supports the claims of Geers (2015), Mäntylä (2014), Ojala (2014), and Isometsä (2013) that cyber operations use cyber weapons, which are military-grade, world-class malicious software of information networks and cause a great deal of damage not only to enemies, but also to one's own side. Cyber weapons use code clusters which enable the cutting down of foreign states' electronic networks by attacking them through information networks. It is, therefore, possible to bring down Internet banks and information networks by adjusting the control logistics of oil transport, and to cripple states and their critical infrastructure (Geers 2015; Mäntylä 2014; Ojala 2014; Isometsä (2013).

Furthermore, this study confirms the findings of Lehto (2015), Geers (2015), Jaitner (2013), Nissen (2012), and Berger (2010) regarding hard cyberattacks being carried out as Denial-of-Service (DDoS) attacks damaging government websites (strategic attacks) and preventing access to their services, hacking emails and mobile phones, trolling (using false social media accounts), using botnets, manipulating audio visual material, conducting espionage, identifying theft and propaganda, and destroying critical infrastructure and control systems. Hard cyberattacks consist of viruses, worms, trojans, hacking, and kracking (Lehto 2015; Geers 2015; Jaitner 2013; Nissen 2012; Berger 2010). Lehto *et al.* (2017) also agree that hard cyberattacks can be attacks on IoT, cloud services, Big Data, devices using mobility, and BYOD philosophy-using devices.

The results are also in line with the findings of Huhtinen and Rantapelkonen (2016), Renz (2016), Paavola *et al.* (2016), Lehto (2015), Sartonen, Huhtinen & Lehto (2015), Saressalo (2012), Berger (2010), and Hollis (2011) regarding pressure through military power and deterrence being psychological operations; and social engineering, control, data gathering, psychological operations, and propaganda being soft psychological operations. The findings support those of Information Operations (2012), NATO (2009), and Armistead (2004) that IO, including kinetic operations, denote the physical destruction of the target by military forces, terrorists, or intelligence operatives working for the government.

However, this study has some limitations. First, the knowledge on information influence and IO was limited in general because only 10 people were interviewed, due to research resource limitations. Second, the use of only one society and one IE affected the findings, making it difficult to generalise the results. Third, the research area was so large and contained so many different issues and concepts that it was sometimes difficult to categorise the items from the data. Fourth, the categorisation of the items into subcategories and the creation of suitable definitions from past studies for so many items and categories took more time than expected. Fifth, there was no access to secret or to confidential material; only open access sources were used, which may also have influenced the results.

Five conclusions emerge from this study. These five conclusions are logically derived on the basis of the explored categories and are drawn from the implicit context of the interviews by going beyond explicitly stated and logically implied meanings. First, even if the study did not focus on information war, the data and findings showed that an information war is in fact in progress. This means that there is a greater goal to influence society from both inside and out. The political goals of the actors carrying out information influence and IO in the IE are to weaken society and its IE. Second, hard cyber operations and hard cyberattacks are linked, and the IE is modified suitably

for some actors by carrying out further information influences and operations, and psychological influences (operations). Third, it seems that there is a strategic goal to harm society's IE with fake news, cyber operations, and psychological influence in order to win the information war without actually doing 'anything other' than influencing opinions and making the population give up the fight before it has even started. Fourth, the goal of the information war is to affect decision making: this is a political goal to beat society's own procedures. Fifth, hostile organisations also have skills to rapidly change their strategies and use propaganda to recruit more supporters. They use the newest Internet channels and social media to get more people to do their work and to apply their hostile ideology, and they use the emotions of their supporters in order to get them to carry out hostile actions. In a psychological way, these hostile organisations have both a bad and a good ego from which they draw their propaganda, and a great motive to do so. They also have financers whom they use for their own hostile purposes.

The practical and managerial contribution helped the actors outline what information influences and IO exist. The most important practical benefit was the determination of the vast number of existing items concerning information influence and IO in practice in the real world. The managerial contribution lies in making every decision maker in society aware of these information influences and IO issues and in making them find more information before making any decisions that affect the IE.

The methodological contribution is the way in which diverse qualitative research methods, such as GT (Glaser & Strauss 1967), content analysis (Krippendorff 1985), and rigorously applied methods can be used together to conduct a high-quality literature study (Wolfswinkel, Furtmueller, & Wilderom 2013).

Finally, to improve the depth of understanding about information influence in complex social systems, one might argue that quantitative data analysis techniques, such as classical statistical hypothesis tests and/or data clustering, could also be applied (Goertzen 2017). In this case study, because the phenomena to be analysed were initially poorly understood, and little prior information was available about the possible categories and final findings, the quantitative research design was challenging, also because the number of interviews was limited. Moreover, quantitative methods require encoding the interview responses into numerical forms, which is easy for closed-ended questions (for example, yes/no questions) (Goertzen 2017), but very complicated for unstructured and semi-structured interviews, such as those in this case. In particular, the coding should not implicitly dictate the results obtained, as the interest lay in analysing the phenomenon in all its possible directions, including the induction and deduction phases for exploring and finding subtle patterns (Goertzen 2017). Hence, the qualitative research approach played a more natural and particularly helpful role in enabling the seeking out and conceptualising of categories and the creation of new theories on information influence in society's IE.

In this study of a society's IE, the cases were selected so that they would either predict similar outcomes (for example, literal replication) or produce contradictory results for predictable reasons (for example, theoretical replication) (Yin 1994). Theory triangulation was applied by interpreting a single data set from multiple perspectives to understand the research problems (Denzin 1978). The concepts (categories) and their relationships were validated using the GT approach (Glaser & Strauss 1967; Eisenhardt 1989). According to Eisenhardt (1989), combining a case study with the GT approach has three major strengths: it produces a novel theory that is testable, the resultant

theory is empirically valid, and the resultant theory emerges from the data (Eisenhardt 1989), as it did in this study.

The operatives behind information influences and IO, and how to build up proper information security and defence against information influence and IO, are interesting subjects of study for the future.

References

Armistead, EL 2004, *Information operations: Warfare and the hard reality of soft power,* Issues in Twenty-First Century Warfare, Potomac Books, Washington, DC, US.

Bachmann, SD & Gunneriusson, H 2015, 'Russia's hybrid warfare in the east: The integral nature of the information sphere', *Georgetown Journal of International Affairs*, pp. 198-211.

Berger, H 2010, '*Venäjän informaatio-psykologinen sodankäyntitapa terrorismintorjunnassa ja viiden päivän sodassa'* ('Russia's pattern of information-psychologic warfare in counter terrorism and five day war'), National Defence University, Edita Prima, Helsinki, FI.

Creswell, JW 2007, *Qualitative inquiry and research design: Choosing among five approaches*, Sage Publications, Thousand Oaks, CA, US.

Denzin, NK 1978, *The research act: A theoretical introduction to sociological methods*, McGraw-Hill, New York, NY, US.

'Disinformation' 2017, *Merriam-Webster,* viewed 22 August 2017, <https://www.merriam-webster.com/dictionary/disinformation>.

Eisenhardt, KM 1989, 'Building theories from case study research', *Academy of Management Review*, vol. 14, no. 4, pp. 532-50.

Geers, K 2015, '"Coder, hacker, soldier, spy", Cyber security: Analytics, technology and automation', M Lehto & P Neittaanmäki (eds.), Dortdrecht, Springer-Verlag, DE, pp. 73-87.

Glaser, B & Strauss, AL 1967, *The discovery of the grounded theory: Strategies for qualitative research,* Aldine, Chicago, IL, US.

Goertzen, MJ 2017, 'Introduction to quantitative research and data', *Library Technology Reports*, vol. 53, no. 4, pp. 12-8.

Goolsby, R 2013, 'On cybersecurity, crowdsourcing, and social cyber-attack', *Policy Memo Series*, L Shanley & A Lovell (eds.), Wilson Center, Commonlabs, vol. 1, pp. 1-8.

Hollis, D 2011, 'Cyberwar case study: Georgia 2008', *Small Wars Journal*, viewed 30 January 2017, <http://smallwarsjournal.com/jrnl/art/cyberwarcase-study-georgia-2008>.

Holt, TJ & Kilger, M 2012, *Know your enemy: The social dynamics of hacking*, viewed 12 January 2017, <http://holt_and_kilger_-_kye_-the_social_dynamics_of_hacking%20(2).pdf>.

Huhtinen, AM & Rantapelkonen, J 2016, 'Junk information in hybrid warfare: The rhizomatic speed of social media in the spamosphere', *Proceedings of the European Conference on Cyber Warfare and Security–ECCWS 2016,* Academic Conference International Limited, Munich, DE, pp. 136-44.

Information operations 2012, *Joint Publication 3–13,* viewed 24 January 2017, <http://www.dtic,mil/doctrine/new_pubs/jp3_13.pdf>.

Isometsä, M 2013, '*Yhteiskunnan toiminta uusia uhkia vastaan'* ('Society's action against new threats'), Thesis, National Defence University, Helsinki, FI.

Jaitner, M 2013, 'Exercising power in social media, *The fog of cyber defence,* J Rantapelkonen & M Salminen (eds.), Juvenes Print, Tampere, FI, pp. 57-77.

Kantola, H & Hämäläinen, J 2013, 'Modelling cyber warfare as a hierarchic error effect of information', *Proceedings of the 12th European Conference on Information Warfare and Security–ECCWS 2013*, Academic Conferences and Publishing International Limited, GB, pp. 322-27.

Krippendorff, K 1985, *Content analysis. An introduction to its methodology*, Sage Publications, Thousand Oaks, CA, US.

Lehto, M 2014, '*Kybertaistelu ilmavoimaympäristössä*' ('Cyber battle in the air force environment'), *Kybertaistelu 2020*, T Kuusisto (ed.), National Defence University, Helsinki, FI, pp. 157-78.

——2015, 'Phenomena in the cyber world', *Cyber security: Analytics, technology and automation*, M Lehto & P Neittaanmäki (eds.), Springer-Verlag, Dortdrecht, DE, pp. 3-30.

——Limnéll, J, Innola, E, Pöyhönen, J, Rusi, T & Salminen, M 2017, '*Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi'* ('Finland's cyber security: The present state, vision and the actions needed to achieve the vision'), Publications of the Government´s Analysis, Assessment and Research Activities, Series 30, Prime Minister's Office, Helsinki, FI.

Luoma-aho, V 2015, 'Understanding stakeholder engagement: Faith-holders, hateholders & fakeholders', *Research Journal of the Institute for Public Relations,* vol. 2, no. 1, pp. 1-27.

Metsämuuronen, J 2006, '*Tutkimuksen tekemisen perusteet ihmistieteissä*' ('Essentials of research methods in human sciences'), Gummeruksen kirjapaino, Jyväskylä, FI.

Mustonen-Ollila, E & Heikkonen, J 2009, 'Historical research in information system field: From data collection to theory creation', A Cater-Steel & L Al-Hakim (eds.), *Information Systems research methods, epistemology, and applications,* Information Science Reference (an imprint of IGI Global), Hersey, New York, US, pp. 140-60.

——, Lehto, M & Heikkonen, J 2020a, 'Components of defence strategies in society's information environment: A case study based on the grounded theory', *Security and Defence Quarterly*, vol. 28, no. 1, *forthcoming.*

——2020b, 'Hybrid warfare in society's information environment: An empirical analysis using the grounded theory', *Proceedings of the 19th European Conference on Cyber Warfare and Security–ECCWS 2020*, 25–26 June 2020, GB, Academic Conferences and Publishing International Limited*, forthcoming.*

Myers, MD & Avison, DE (eds.) 2002, *Qualitative research in information systems: A reader,* Sage Publications, London, UK.

Mäntylä, J 2014, '*Kyberaseiden vaikutus kriittisen infrastruktuurin tietojärjestelmiin'* ('Cyber weapons impact on critical infrastructure information systems'), Thesis, National Defence University, Helsinki, FI.

NATO 2009, *Allied joint doctrine for information operations*, viewed 24 January 2017, <https://info.publicintelligence.net/NATO-IO.pdf>.

NATO 2012, *NATO Military policy on information operations*, viewed 24 January 2017, <https://info.publicintelligence.net/NATO-IO-Policy.pdf>.

NATO StratCom COE 2015, *Mapping on StratCom practices in NATO countries; Results of the study*, viewed 15 May 2017, <http://www.stratcomcoe.org/mapping-stratcom-practices-nato-countries-0>.

——2016, *Social media as a tool of hybrid warfare*, viewed 30 May 2017, <http://www.stratcomcoe.org/social-media-tool-hybrid-warfare>.

Nissen, TE 2012, *Social media's role in 'hybrid strategies'*, viewed 12 January 2017, <http://www.stratcomcoe.org/social-medias-role-hybrid-strategies-author-thomas-elkjer-nissen>.

Ojala, H 2014, '*Lähi-idässä käytetyt kyberaseet'* ('Cyber weapons used in the middle east'), Thesis, National Defence University, Helsinki, FI.

Ottis, R 2015, 'Cyber warfare', *Cyber security: Analytics, technology and automation*, M Lehto & P Neittaanmäki (eds.), Springer-Verlag, Dordrecht, DE, pp. 89-96.

Paavola, J, Helo, T, Jalonen, H, Sartonen, M & Huhtinen, AM 2016, 'Understanding the trolling phenomenon: The automated detection of bots and cyborgs in the social media', *Journal of Information Warfare*, vol. 16, no. 1, pp. 100-15.

Pawluch, D & Neiterman, E 2010, 'What is grounded theory and where does is come from', *The Sage handbook of qualitative methods in health research*, A Bourgeault, R Dingwall & R De Vries (eds.), Sage Publications, London, UK, pp. 174-92.

Puttonen, H 2015, '*Informaatio-operaatiot ja niiden keskeiset vaikutusmenetelmät'* ('Information operations and their influencing methods'), Thesis, University of Jyväskylä, Jyväskylä, FI.

Rantapelkonen, J 2002, '*Psykologiset operaatiot: Propagandasta informaatio-operaatioihin'* ('Psychological operations: From propaganda to information operations'), National Defence University, Helsinki, FI.

Renz, B 2016, *Hybrid warfare' as a quasi-theory of Russian foreign policy*?, Aleksanteri insight-snapshots of Eurasia, viewed 15 January 2017, <http://www.helsinki.fi/aleksanteri/insight>.

Salminen, M 2018, '*Kyber-fyysinen sota 2030+. Yhteiskuntien kompleksisuus tuottaa yllätyksiä sodankäyntiin*' ('Cyber physical war 2030+. The complexity of societies creates surprises for warfare'), *Tulevaisuuden sota. Tulevaisuuden sodan tulevaisuus,* J Rantapelkonen (ed.), National Defence University, Otavan Kirjapaino, Keuruu, FI, pp. 198-226.

Saressalo, T 2012, *'Psykologinen vaikuttaminen CAST LEAD-Operaatiossa'* ('Psychological influence in CAST LEAD operation'), Thesis, National Defence University, Helsinki, FI.

Sartonen, M, Huhtinen, AM and Lehto, M 2015, 'From influence to influencer: The rhizomatic target audience of the cyber domain', *Proceedings of the 14th European Conference on Cyber Warfare & Security–ECCWS 2015,* Academic Conferences and Publishing International Limited, Hatfield, GB, pp. 249-56.

Secretariat of Security Committee 2018, '*The vocabulary of cyber security*', The National Emergency Supply Agency, Helsinki, FI.

Sigholm, J 2013, 'Non-state actors in cyberspace operations', *Cyber Warfare*, J Vankka (ed.), National Defence University, Juvenes Print, Tampere, FI, pp. 47–76.

Sirén, T, Huhtinen, A-M & Toivettula, M 2011, '*Informaatiosodankäynnistä kokonaisvaltaiseen strategiseen kommunikaatioon*' ('From information warfare to comprehensive strategic communication'), *Strateginen kommunikaatio ja informaatio-operaatiot 2030*, T Sirén (ed.), National Defence University, Juvenes Print, Helsinki, FI, pp. 3-21.

'Society' 2018, *Wikipedia,* viewed 18 May 2018, <https://en.wikipedia.org/wiki/Society>.

Tähtinen, J 2013, *'Georgian sodan tarkastelu strategisen iskun toteutusperiaatteiden ja torjunnan n*äkökulmasta*: suomalaisen uhkamallin analysointi Georgian sodan ja siitä saatavien oppien perusteella'* ('Review of the Georgian war from the point of view of the principles of implementation of the strategic attack and the fight against it: Analysis of the Finnish threat scenario based on the Georgian war and the lessons learned from it'), Thesis, National Defence University, Helsinki, FI.

Wolfswinkel, JF, Furtmueller, E & Wilderom, CPM 2013, 'Using grounded theory as a method for rigorously reviewing literature', *European Journal of Information Systems*, vol. 22, no. 1, pp. 45-55.

Yin, RK 2003, *Case study research: Design and methods*, Sage Publications, Thousand Oaks, CA, US.

Yin, RY 1994, *Applications of case study research*, Series 34, Sage Publications, Newbury Park, London, UK.