Author(s): Helfenstein, Sacha; Saariluoma, Pertti

Title: How cyber breeds crime and criminals

Year: 2014

Version:

Please cite the original version:

Helfenstein, S., & Saariluoma, P. (2014). How cyber breeds crime and criminals. In V. Snasel (Ed.), DigitalSec 2014 Proceedings : The International Conference on Digital Security and Forensics (pp. 76-90). The Society of Digital Information and Wireless Communications (SDIWC). http://sdiwc.net/digital-library/request.php?article=b2aba93ca73232d1cbd5ae79b05489b9

How Cyber Breeds Crime and Criminals

Sacha Helfenstein and Pertti Saariluoma
Department of Computer Science and Information Systems
University of Jyväskylä, Finland
PO Box 35, FIN-40014 Jyväskylä
sacha.helfenstein@jyu.fi, pertti.saariluoma@jyu.fi

ABSTRACT

Understanding how cyber breeds novel crime and new criminals is a contribution to criminological models with significant applied value. It is highly important for law enforcement and particularly pivotal for preventive intervention. In this paper we propose a human rights-based crime definition, present explanatory models for cybercrime, and outline future arenas and drivers to suggest to the stakeholder community prevention focuses and priorities. The presented work ultimately aims towards supporting two crime preventive design initiatives, one targeted at accounting for and narrowing the cybercriminal space of means, opportunities, and motives; the other aiming at augmenting early and proactive adaptation of crime legislation. Finally, life-based and agile design paradigms are briefly introduced as suitable methods to be pursued in future research and developmental projects.

KEYWORDS

Cybercrime, Cybersecurity, Future Crimes, Crime Prevention, Human Motives, Human Rights

1 INTRODUCTION

Technological artefacts have always had one persisting purpose, namely to enhance or ease human life and their goal-oriented actions. In this context, crime can be seen as a human intentional act with a particular goal orientation and therefore it—like many other human activities—makes use of various kinds of tools. This circumstance poses challenges to an organized society, particularly as humans and societal enterprises become increasingly dependent on various types of technological aids that then may be turned and (mis)used against them. Modern information and communication technology (ICT) devices and infrastructures are at the forefront rising attention due to the new kinds of possibilities emerging technologies open for traditional types of criminal activities, as well as radically new types of criminal activities. Forecasting of criminalization of technology—be this criminalization by design or by appropriation—is pivotal and urgent in order to find means to meet future crime and to develop policies and legislation in support of crime determent and prevention. A focus point in forecasting new crime today is in cybersecurity.

New information technology has had roughly two important evolution and impact branches. On one hand, the control mechanisms of traditional electromechanical tools have essentially improved, boosting the performance capacity of highly automatic and even autonomous systems. In this vein of development, we are about to witness cars that do not necessarily need human drivers to navigate. On the other hand, human use and dependence on information has grown dramatically – privately, socially, or industrially. For instance, in the United States, the number of people in information- and knowledge-intensive, non-routine type of professions has increased since 1960s by 30% to represent today more than half of the total labor market [1]. As an effect of this, the use of information to support criminal actions has also exponentially grown.

Indeed, cybersecurity concerns have become highly prominent and the phenomenon is continuously reaching new peaks in terms of statistical incidences and the hype generated around them. Norton estimates in its annual cybercrime report that in 2012 alone, every second user has fallen victim to some offensive online activity, effecting a global price tag of more than 100 billion US dollars [2]. In McAfee's freshest report this toll is even raised to over 445 billion US dollars [3]. While these figures are based on extrapolative projections rather than on actual reports, they do allow drawing a picture of the overall proportions of the issue.

In case the impression of cybercrime as a growing problem holds true, it is important to inquire about the drivers of this growth. It is reasonable to assume that offensive online activities would spread due to the increasing diffusion and adoption of enabling technology, both within the victim population as well as among offenders. On top of this there are also good indications that digital means and environments actually stimulate *novel forms of misconduct* and delinquency, as well as *new perpetrators* [4]. In short: Cyber breeds novel crimes and new criminals.

Understanding how cyber breeds novel crime and new criminals is a contribution to criminological models with significant applied value. It is highly important for law enforcement and particularly pivotal for preventive intervention. Such prevention comprises preemptive education, anticipation and early detection, regulative adaptations and resistance preparation, as well designing against cybercrime (for the Designing Against Crime (DAC) paradigm, see [5].

Considering the total sum of investment into buildup of cybersecurity and cybercrime countermeasures on top of the cost of cybercrime damages - estimated world-wide at over one trillion Euros per annum - it is vital to support cost-efficient, sustainable, and focused action. Prioritized, preventive work is most effective in this context and in order to propel this line of action, we need to pay closer attention and understand how cyber dimensions inspire crimes and motivate criminals, instead of just trying to repress cybercrime commission. This is also in response to the need for a better understanding of the *unique* characteristics of cybercrime, in addition to the various commonalities it shares with traditional illegal behaviors (e.g., [6]).

In this paper, we proceed from delineating cybercrime towards through explaining and towards approaches for forecasting and preventing it (see Figure 1). We start out from describing core characteristics of the cybercrime space to then draw attention to emerging and future crime opportunities and scenarios, as regards the technology-enabled planning and enactment of offenses, but also as regards the socio-psychological drivers that encourage their conception and enactment.

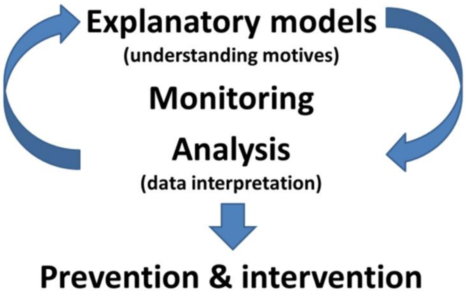

Figure 1. Crime Mitigation from Explaining to Preventing

2 DELINEATING CYBERCRIME

The ultimate aim of our research lies with supporting cybersecurity-relevant analytics and intervention. However, our intermediate aim must be with understanding and explaining current and forecasting future cyber-criminal activity based on interpretative observation and description (see Figure 1). To start, we first need to delineate what kind of criminal conduct we investigate and aim to provide explanations for. Our frame definition for cybercriminal activity will be composed of the following three core conditional constituents

1. Crime as violation of human rights
2. Crime as intentional and overt act
3. Crime planning and/or execution as technology-enabled

In standard sense, one can say that crime is any activity, which has been defined in the laws of a country or in international laws as a crime. Thus, crime is a deed that is defined by legislative social organizations and which has been coded in a system of laws. In this logic, spreading previously unknown drugs or doping substances may not necessarily be illegal although because they have not yet been classified as such.

Unfortunately, the idea of something being defined as a crime in a system of laws does not yet provide us with very fruitful foundations for our considerations. Cybercrime is in the history of legislation still a relatively new phenomenon, and with our added goal of studying future and emerging cybercrime, it is likely that many misdemeanors of interest are not yet encoded to any system of laws. In search for a more general definition ground for (cyber)crime we will therefore turn to universal, basic rights standards.

One of the most universal rights foundations is our shared belief and adherence to the principle that all individuals have equal rights. The general codex for the rights of an individual can be found perhaps best in The Universal Declaration of Human Rights [7] and the human rights legislation following this declaration. Crime, then, can be seen as a threat or disturbance to the human rights principles. Namely, one very firm property of a crime is that it always concerns how one person treats another, or more accurately, how one person intentionally impairs the rights and quality of another persons' life. And applied to cybercrime, we state that no new technology should be used in a way that intentionally limits the rights of other people in a manner or to the extent that is not mutually agreed and harmful.

The actual role and form of employing technology for criminal purposes may be manifold, and not merely focused on prototypical computer hacking, for instance, e.g., [8]. The misbehavior we are interested in encompasses all conduct involving digital means that targets (or at least tolerates) a violation of human rights – typically due to the harming of others, alongside the improper advancement of one's own benefits (material or immaterial).

Further, we share with standard crime-definitions the requirement of such malign actions (actus reus) to be *intentional* and *overt* in nature (e.g., [9]). But as argued above, we do not wish to constrain ourselves only to behavior that is judged as offensive from contemporary legal point of view. The thoughtful intent or motivation to bring about or accept others' harm or injustice in order to further one's own interests (mens rea) is a more primary concern and explanatory source for us. Finally, to classify a crime as "cyber", we simply add the condition that planning and/or execution of the criminal activity needs to be technology-enabled (see e.g., [10]). This technology or cyber element, so we argue, in turn influences back onto the scope of the *crime space*, due to type of violations that can be planned and committed, their intentional and motivational ground, as well as the opportunities and means to enact these intentions. In the next section we will unfold these core dimensions of the cybercrime space.

3 CYBERCRIME SPACE

Conceptual demarcation of the cybercrime space offers a good way to better understand its distinct drivers and cornerstone. In order to visualize this space of cybercrime, we apply adapt Detica's triangle concept with three interdependent factors: *means*, *opportunity,* and *motive* [11] (see Figure 2). Here through it is understandable that technological progress has probably always stimulated an enlargement of the (conventional) crime space by providing more (sophisticated) means, more opportunity and new action grounds and targets. This technology-driven progression has arguably been particularly accelerated in the cyber age.

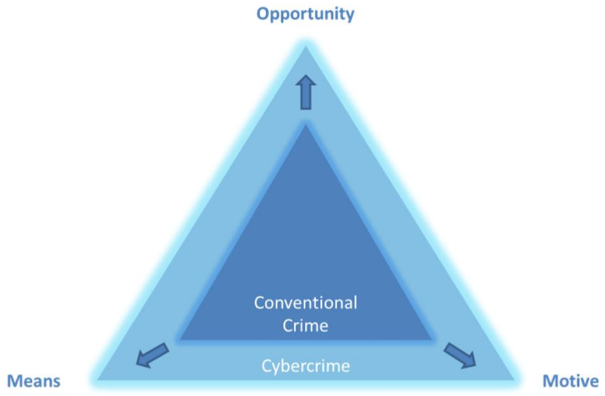

Figure 2: Crime Space demarcated by means, opportunity and motive (adapted from [11])

The question is therefore what the particular incremental means, opportunities and motives are in the cyber context.

3.1 Means

In terms of general means, the Internet and with it connected ICT offer naturally historically unparalleled criminal agencies regarding intelligence, speed, mass, reach, and concealment methods. We will look at specific means and concrete technologies further below in the context of outlining future cybercrime scenarios (Section 4.2).

3.2 Opportunities

Opportunity is often seen as another crucial element in the triggering of a criminal act – sometimes arguably even as a primary provoking agent (see e.g., [12] [13]). Hereby we find it important to differentiate two classes of opportunity influences, one being the opportunity to enact the criminal intention, the other being the recognition of an opportunity that generates a criminal intention. The latter we would like to discuss in the contexts of motive formation.

The Internet, per se is an opportunity-rich environment for criminal activities. In fact, the Internet is one of the best examples of feeble design against crime. As [14] emphasize: “The Internet is perhaps the most complex artificial system ever developed; what is worst: it was not designed with security in mind” (p. 5). And with daily more people, organizations, and information systems becoming connected to this colossal network, the gap between accelerating criminal opportunities versus diminishing control keeps growing [15].

Initially, the Internet as well as its hosted World Wide Web, were designed as small projects for an intimate group of trusted members. In the course of its following public popularization the Web has to date been carried by an implicit maxim of amity and anarchy - a space to live and realize cultural liberty. It is this openness spirit that has become itself part of the cause for why the Internet’s power and benefits are being so easily turned against itself and its users.

On top of this, the Internet is obviously an ideal facilitator, with its network bringing the digitally connected world at anyone’s fingertips, anytime-anywhere, including one’s own private premises. This circumstance provides pure cybercrime with a radically different opportunity constellation compared to traditional crime, namely one where the criminal objects come to the criminal, rather than the other way around. In addition to the increased availability of criminal targets, the Internet also amplifies opportunities to access information, tools and support to execute misdemeanors. And finally a cyber context provides ample opportunities to conceal ones wrongdoings from guardians and collateral audience due to the virtual nature of the criminal goods and methods [16], [17].

Victimization as opportunity

A particularly interesting driver of opportunity lies with cyber’s *victimization*-boosting impact. Here we identify 5 primary victimization factors:

1. User illiteracy
2. Deficient criminal cues
3. Emotional susceptibility
4. Limited attention
5. Inflated trust
6. Addiction potential

First, users are to date often unaware, ignorant, overconfident, uneducated or simply do not care about security issues. According to the most recent Norton Crime Report, two third do not use any security solution for their mobile phone, and almost half of the users do not even know such exist. One out of four Facebook users also does not bother to set any privacy control in their Facebook account [3]. In most cases, our personal information seems still immaterial compared to political or business intelligence. It seems that wide media coverage of social media data abuse has done little to change this situation. Recent court rulings such as in the case of Google search data [18], but also as in the open case against Facebook (first ruling expected for June 2014), may bring further change to public awareness and initiative taking. However, the latest news concerning Facebook's marketing-driven intention to open up their network to children will certainly jeopardize this evolution [19].

Second, virtual environments cause a lack of traditional cues to elicit human vigilance and caution. In contrast to cyber risks, human habituated risk cues are

- *visible*, i.e., crimes constitute of overt offensive action and physical crime artifacts;
- *contextually discomforting*, e.g., dark allies at night, strangers, physiognomy;
- *related to the holding of personally valuable goods*, e.g., carrying cash or jewelry. In contrast to this a small plastic credit card may feel less valuable than a 1'000€- bill in one's wallet.

Third, cybercrime often leverages on big human emotions and motivations. To highlight some of the major human affect-oriented tendencies:

- *Craving for love and affection*, e.g., "I LOVE YOU" worm's false affection with an estimated global damage of $15 Billion; online dating scams
- *Empathic inclination to help and reprocicate*, e.g., "Nigerian" Scam, Haiti relief donation scams
- *User anxiety, uncertainty, confusion*, e.g., Scareware—Selling of fake antivirus software
- *Fear and guilt*, e.g., Ransomware used to threaten and blackmail Internet users by exploiting logs of their illegal (e.g., illegal digital downloads are common among roughly 70% of youth aged 15-16, and 50% of the user cohort aged 15-24; compare [20]), immoral or stigmatized (e.g., visiting internet porn pages) online behavior.

Fourth, cybercriminal may leverage ICT users' cognitive attention limitations, or susceptibility to distractions. Much of everyday interaction with digital devices is governed by routines, such as the automatic opening of email attachments or the clicking on links and buttons. Also, especially mobile ICT usage is often embedded in contexts that compete for user attention, such as smartphone usage in public places. Both circumstances can be easily abused to lure users into making decision or providing information that has not been carefully verified. Further, the simple mass of online stimuli and interaction operations poses a favorable environment to disguise criminal content. Masking criminal content by imitating well-familiar stimuli is hereby a major criminal tactic, e.g., setting up phony websites whose visual design mimics that of familiar websites.

Fifth, cybersecurity is in many ways a victim of its own promises and activities. In principle, the whole success of emerging ICT depends on user adoption and trust-building regarding technological means that are in principle strange and intuitively non-trustworthy. Hence, a lot of effort is continuously put into convincing and promoting user adoption and trust of cyber means; a foundation that then can easily be abused. This happened for email (phishing), web-links (pharming), e-services and e-commerce (scams), social media (social engineering), and it is happening for the uptake of location-based tagging, mobile services etc. In this sense, Internet trust and crime evolution are tensely inter-dependent antipodes.

Finally, as sixth victimization driver, it is noteworthy that human ICT usage is often related to addictive, and dependency-colored behavior and cultures. This phenomenon is evident for many peoples' usage of mobile gadgets (e.g., problematic smartphone overuse; e.g., [21]) as well as for the use purposes and applications on these devices (e.g., digital gaming, social media). Excessive and compulsory digital gaming, for instance, was 2013 added as Internet Gaming Disorder to the Diagnostic and Statistical Manual of Mental Disorders (DSM) published by the American Psychiatric Association [22]. As in other domains addictions and crime do often go hand-in-hand. Crime can be a means to fund one's addiction, addiction-prone environments can heighten the likelihood to get involved with criminal networks, and, last but not least, addictive behavior can make people more vulnerable to become victims of hoaxes and scams, because the addict's intense need situation and motivational drive towards the addiction target competes with and overrides human innate attentiveness, caution, and suspicion.

3.3 Motivation & Intention

The final argument is that cyber environments have stimulated motivation and intention to enact a crime and thereby become criminal. Let us first look at cybercriminal intention, as it is a more proximate driver of criminal actions than underlying motives and motivation. In principle, criminal intention can be captured as the result of a basic 'value x expectancy' –calculation (see theory origins with Fishbein and Ajzen's work, [23]) coupled with a simple 'cost vs. benefit'-assessment. Hereby anticipated personal benefits (e.g., profits or other type of gratification) are weighed against undesirable personal disadvantages (e.g., the risk of being detained or unpleasant moral conflicts). In a formalized manner this can be expressed as criminal intention (CI) equaling the attainment likelihood (AL) for a projected benefit value (BV) minus the realization likelihood (RL) for an anticipated disadvantage value (DV) (1) (see also [24]).

$$\mathrm{CI} = (BV \times AL) - (DV \times \ RL) \qquad (1)$$

In our view, the advent of the Internet and related digital means may well have effected an increase in criminal intention based on enhanced means and enlarged opportunities to achieve a positive while avoiding a negative outcome of criminal action, which altogether have "positively" influenced the criminal intent as laid out above. This regards the prospect of

- greater variety and amount of BV and
- better success expectancy (AL), while
- introducing a new grey zone of legality and acceptability (DV), combined with a
- reduction of the perceived apprehension risks (RL).

We can also categorize the various intention-promoting factors of cyber contexts by distinguishing *behavioral facilitators* and *behavioral disinhibitors*.

Among the facilitators we mainly refer to an improved accessibility to crime-relevant information, tools and methods and the technological enhancement of criminal skills and illegal action (e.g., available intelligence and "how-to" instructions, recruitment and formation of an accomplice network, improved logistics, communication and coordination, heightened speed, reachable mass of victims, removal of time geographical, or other physical constraints).

The group of disinhibitors comprises amongst others the earlier argued "Online" cultural setting, which—so our claim—lightened the salience of experienced moral conflicts and regulatory constraints. The covert nature by which a hacker can work single-handedly over a package of potato chips from his cozy armchair reinforces with the perpetrator a deceptive or delusional mental representation of his or her action. On the one hand, this misapprehension is based on a set of immanent cues that suggest comfort, anonymity, tracelesness, weak controllability, and safety. On the other hand—analogue to the victim's side described earlier—the criminal actor is deprived of relevant action context and real-world feedback, i.e., traditional cues that can stimulate human sentiments such as responsibility, accountability, as well as—very importantly—empathy and compassion. On top of this, the amount of dubious content readily available on the Internet may imply a softening of social norms, legislative ambiguity and law-enforcement incapacity.

Altogether, we believe that these types of cyber effects—here denoted as *virtuality predicament or fallacy*—have far-reaching consequences. This regards for instance cyber's impairing effect on human empathy; an important antagonist to anti-social behavior (e.g., [25]. As empathy skills have been shown to be related to the recognition of facial emotion expression [26], it can be ventured that absence of such stimuli will undermine empathic response. Furthermore to the lack of social and physical cues, the depersonalized virtual context may actually be of heightened attractiveness to a user group with a weakened socio-emotional skillset to start with (e.g., [27]). Another virtuality predicament is that internet crime also invites misdemeanor on the basis of "harming many a little" or by legitimizing one's own illegal action by reference to many others, which allows for a moral diffusion. Yet another aspect of the virtuality predicament lies with the suggestiveness of cyber space as a deregulated space of anarchy, where disobedience and indiscretions seem socially acceptable, and where a user may easily adopt an unsound concept of "Freedom of Speech" or even a prophet of a higher-order moral code (e.g., [28]).

This brings us to the question about criminal motivation, especially such classes that seen rather exclusive to cybercrime. Neufeld's analysis of 113 US Department of Justice federal cybercrime cases 2008-09 revealed that financial gain and revenge-based motives still lead the list, together applicable to more than 80% of the studied cases [4]. However, we believe that the cyber setting also give rise to some motivations that have not been prevalent in the same way in the pre-cyber era.

One such a mega-trend concerns reputation as one of the most treasured and vulnerable personal goods, listed third in Neufeld's ranking [4], and particularly highlighted by the European Cybercrime Centre & International Cyber Security Protection Alliance: "Reputation will be everything, for governments, businesses and citizens alike. Damage will be instantaneous and increasingly difficult to repair." [29].

Another motivation trend indicated earlier concerns the circumstance that for many the advent of the Internet and Web may have marked a welcome door-opener to display inherent tendencies and drives towards righteousness, renegade, and rebelliousness against a dislike socio-economic and political systems or elites, e.g., piracy activists' "Robin Hood"-attitude in illegal downloading and spreading of media content.

Finally, there is one trait of the virtual world in favor of nurturing a new type of criminal motivation that we eye with particular concern: *Gamification of Cybercrime*. For instance, at pre-criminal or early illegality stages of misconduct a cybercriminal may be largely driven by the motives of challenge, thrill, or playfulness (hoax, prank) of the action and its intended outcome [30], [31]. This can be a trigger to a criminal career that at intermediate stages may be positively reinforced by (deceptive) social reputation and an evolving normality distortion, before pure criminal motives take over in terms of organized criminal behavior.

However, we also spot dangerous phenomena regarding a deliberate social blending of gameful concepts with harmful behavior. This may encourage a risky emotional and motivational transfer from the gaming domain to the criminal domain. One such an example is the TrackingPoint^{TM} smart rifle, a Linux-powered and WiFi-enabled gun that allows the shooter to track and lock his or her target via a tablet computer, and share the event online (http://tracking-point.com). In the voice of the developer company's president Jason Schauble: "''This kind of technology, in addition to making shooting more fun for them, also allows shooting to be something that they can share with others." Their latest “ShotView”-invention will in combination with Google Glass even allow to aim and pull the trigger without any physical sight contact. Another example is Watch Dogs^{TM}, a new action-adventure video game developed by Ubisoft due to be released at the end of May 2014, promoting hacking culture, particularly the scenario of taking over of a whole city’s information control infrastructure (http://watchdogs.ubi.com/). Finally, there is a wide range of originally playful technology that can be instantly or gradually turned into cybercriminal weapons, such as remote-controlled Quadcopter drones.

The point of these examples is not with alarming or banning such technology, but with raising attention to their criminal potential, especially as where boundary between gameful and somber application motives can become very blurred, encourage negative-type of (emotional) transfer [32], or foster emotional desensitization [33].

4 FORECASTING CYBERCRIME

Following the demarcation of the cybercrime space in the previous section, we next wish to project and speculate on emerging crime arenas and future scenarios that will populate this space. Our projections are a result of a wide investigation of the evolution of cybercrime based on popular and research literature review, the study of recent cybercrime statistics and current trends, discussion with leading representatives from the Finnish National Bureau of Investigation, as well as a scrutiny of future emerging technologies, for instance as the 2013 report devised by the Finnish parliament’s Committee of the Future [34].

4.1 Evolution of Cybercrime

Cybercrime has come a long way since the advent and early build-up of computing technology in the 1960s (where cybercrime concerned mainly physical damage to electronic data processing infrastructures) and 1970s (early data manipulation cases). It was further propelled by the public spreading of personal computers in the 1980s (onset of software piracy), and has been finally boosted by the launch of the Internet and its cultural phases pertaining to the Web 1.0 and 2.0 in the 1990s (rise of hacking), and on into the 21st century with the explosion of the social web (expansion of social attacks, such as phishing, identity theft, social engineering).

Some core themes in this overall cybercrime evolution have naturally been a progressing disentanglement of crime scene and crime act, growing criminal creativity and sophistication, as well as cybercrime’s mounting social dimension and societal impact. Projecting from current digital trends crime evolution into the future it is possible to highlight a few characteristics that will most probably define the face of cybercrime for the years to come. Among these three core themes rise above others:

- Cybercrime becomes further *socially networked* and *mobile*
- Cybercrime becomes increasingly *professional* and *industrialized*
- Cybercrime means become *easily accessible* and adoptable by everyone

4.2 Outline of Future Cybercrime Arenas and Drivers

In the following we will in cursory manner through the main arenas and drivers of future cybercrime.

Social Media

- An increasing amount of human communication, identity and social status formation, as well as leisure, professional and commercial interaction takes place in virtual environments of social networks. This means that these environments not only allow for the perpetration of crime activities inside these cyber contexts, but the information available in social media—including their storability and processability—essentially motivates and augments crime planning and enactment in real-world environments. As crime concerns in core a hostile act of one individual, negatively affecting another individual, social media is the new natural habitat for it to blossom.

- Besides the leveraging of social media to intimidate and discriminate others (e.g., cyber mobbing) it is mainly social engineering, identity theft, and particularly reputation manipulation that will remain at the forefront of future cybercrime.

e-Life

- Alongside social life going increasingly online, official correspondences and relations in general are growingly digitalized. E-citizenship is becoming a vast phenomenon encompassing, e.g., our dealings on eGovernment, eCommerce, eEducation platforms and the increasing uptake of electronic banking and payment. In principle, this all means that the amount of privacy delicate information and goods available in digital format, for cyber-criminal exploitive purposes of interception, manipulation, or fakery is exponentially growing.
- eBusiness seems particularly vulnerable in this context. Most businesses are to date awfully under-protected, and attacking those financially or intel-wise attractive enterprises yields extraordinary reward at minimal risk and cost.

Online Gaming/Gambling

- The (real world) gambling scene has historically always been crowded by crooks and organized crime, due to the prominence of capital involved as well as the vulnerability of the clientele. The virtual added benefits such as anonymity and disguise, global reach, social engineering, and legislative avoidance are only providing upwind to criminal exploitation. A fresh whitepaper published by McAfee estimates online gambling growth rate at over 7% yearly, much of it driven by criminal activity itself, or exploitable by such [35].
- Cyber-gambling fraud as well as money laundering activities via online gambling mechanisms and network will be key driver of this criminal domain.

Autonomous systems/Internet of Things

- The Internet of connected Things (IoT) and cyber-physical systems will in future be much bigger than the current social web. Cisco estimates that IoT will grow from 15 billion connections in 2014 to over 50 billion in 2020 (see http://newsroom.cisco.com). These smart things and environments (such as smart homes appliances, cyber-cars, and robots) will be provider and customers of various virtual services. And because, as per definition, they will be much less under direct control of human beings—or even unnoticeable to its users—their attractiveness and vulnerability for criminal purposes is huge.
- Interpol's Project2020 forecasts "interference with, and criminal misuse of, unmanned vehicles and robotic devices" as well as "hacks against connected devices with direct physical impact (car-to-car communications, heads-up display and other wearable technology, etc.)" as major threat [29]. And with military warfare becoming increasingly autonomous and Internet-based itself, one of the scariest scenario is of course criminal exploitation of sophisticated weapons of mass destruction.

3D Printing

- 3D printing is another interesting case of how virtual (planning) and physical (enactment) constituents of cybercrime become increasingly blended. The easy, location-independent mass-production of physical artefact based on digital information will be an important accessory for criminals, and especially for crime-relevant service providers.
- Recent mediatized cases demonstrated the copying of lock keys or fake Point-of-Sale's terminals and related ATM skimmer devices.

Biometrics, Genomics & eHealth

- Biometric technology purports to collect and retain personal information and is therefore innately prone for privacy compromization and misuse of this same technology. The recent uptake of biometric identification or authentication solutions (e.g., Apple's iPhone 5S and Samsung's Galaxy S5) carries in their design still too often a tradeoff between security and convenience. The acceptance of this tradeoff is probably also driven by the illusion of biometrics as a marvel futuristic technology; an image that was built up over the last half a century in Science Fiction conceptions. The extension of this domain into the areas of genomics and eHealth, is maybe one of the most scary as it not merely blends the digital world with the physical, but actually provides invasive access into the very natural core of individual life and existence. Just as hackers can intrude and manipulate computer digital code, it is possible that in future they can access and manipulate human genetic code.
- Bio-hacking will become a new prolific case of transfer of scientific to criminal excellence. Due to the increasing implantation practices of digital sensors and control devices into the living organism, eHealth attacks are becoming a major threat; either for direct manipulation or for crime-instrumental menacing acts.

Cloud & Big Data

- Cloud computing and Big Data have major impact on amplifying the means for cybercrime. First, cloud computing furthers the geographical and physical dissociation of the criminal actors and victim networks. But they also empower the generation of a criminal intelligence and facilitate virtual crime enactment (e.g., processing and information mining power) that allows for increased scalability and automatization. This includes the vision of "automated crime" where the whole criminal process is scripted, from victim identification, via intelligence gathering and means arrangement, to its covert execution and the erasing of traces. In general, with more data being handled in outsourced manner, the liability and vulnerability to fall victim to data leakage or abuse also grows.
- Examples of emerging threats: Cloud-based botnets and highly distributed denial of service-attacks; sophisticated and automated victim target screening and cyber-casing, identity theft and social engineering, and, finally information espionage on all levels from individuals to business enterprises and critical institutions.

Augmented reality, Location tagging

- Location-tagging has evolved into a megatrend recently, with geographical metadata being directly embedded into information transmitted across and stored on the internet. Mobile applications have been a major driver in this trend, also because a vast amount of apps nowadays require the acceptance of location sharing, often for no particularly legitimized reason.
- Location information is particularly valuable for cyber-casing purposes, meaning the fusion of information about a person, her interest and belongings, and here real-time or periodical whereabouts (often especially her absence from specific places, such as for instance her home residence). But they also allow for enhanced coordination among criminals for planning and execution purposes, just as the can facilitate for instance the transaction of drugs between traffickers, dealers, and users. Finally, the GPS- and navigational systems behind the location-based services will become a major incentive for manipulative actions with manifold criminal payoff.

Mobile technology ("anytime-anywhere")

- The rapid spread and staggering adoption of mobile technology is obviously to the advance of cybercrime on many levels. According to current projections, 2015 will be the year where total mobile connections will surpass the size of the world population, two third of which will be through smartphones, and one third of which through high-speed LTE networks. This evolution translates into an inflation of the victim population as well as devices ownership, including boosted accessibility and attackability of the entailed crime-sensitive information. Mobile networks have also heightened the means for malignant interception and interference compared to line-based networks. Simultaneously the use culture has evolved unfortunately into the opposite direction, where devices, their maintenance, and access are—paradoxically so—treated with less care in more public space contexts. Also, mobile phones, being experienced as a much more personal companion than PCs used to be, are stacked with privacy insight like never before.

- Exploiting users' deficient device protection, their willingness to install unfamiliar apps and software updates—with often intransparent and inflated privacy access requirements—and leveraging the privacy-rich information stored and transmitted by mobile devices will be a core driver for future crime. A 2012 Bit9 reports suggests one quarter of Google Play apps to pose a security risk [35]. In addition, criminals themselves benefit from the mobile device as sophisticated crime tool in action, as had been tragically witnessed in the 2008 Mumbai terrorist attack.

Cyber diffusion

- Growing digital, internet, and mobile penetration rates, particularly in politically instable, economically frail regions with weary legal systems and a high criminal cultural base rate will be an obvious sociological driver of future cybercrime. Simply speaking, it means that it spreads cybercrime means and opportunities to people prone to use it against victims that have so far been out of their (geographical or network) reach. And it also means that more inexperienced, prospective victims (private, public, and commercial) are getting online and accessible by attackers.

Organized Crime

- The move from the teenage hacker model cybercriminal to the professional trans-national cybercriminal organization is widely proclaimed as sea change in cybercrime evolution. In our assessment crime organization profits from and leveraged cyber environments in three ways. For once, cybercriminals become more organized just as incumbent criminal networks are going increasingly online. Alongside systematized cybercriminal organization, the online social networks also facilitate spontaneous organization of criminal activities or originally legal activities that spill over into illegal forms such as when flash mobs become crime mobs. Finally, the cyber landscape has cultivated Crime as a Service in a completely new dimension. Tools, expertise, connections necessary for criminal execution are all easily findable through popular search engines, available for online consumption or offline purchase at a click of a mouse button.

Attack against critical infrastructures

- Attacks against critical infrastructures as glorified in the new adventure video game Watch Dogs^{TM}, are highly attractive due to their immense impact scope and are facilitated by increasing connectivity and internet-dependency of the targeted systems as well as the modern ICT tools at hand. This concerns interruptions of energy or water supply and distribution, but increasingly interesting so for cyber ages' own infrastructures, such as data centers, internet servers and gateways, telecommunication operators' networks, and satellite systems.
- A particularly bleak outlook on infrastructural criminal attacks relates to interference and manipulation targeted at law enforcement and military infrastructures themselves, who themselves develop and rely increasingly on cyber-systems and cyber-enhanced armament and warfare. Hijacks of military drones or hacks into a countries missile defense

system are certainly not among the mind-soothing future crime scenarios.

Legislative lag

- In many senses, the legislative loopholes as developmental lag, including international inconsistencies, and local enforcement incapacities must be seen as substantial driver of cybercrime. As laid out in Section 3.3 crime will always gravitate towards paths of least resistance. Cybercrime does not obey and is not constrained by the same boundaries that motivated the evolution of crime fighting and containment. Cybercrime evolution typically also outpaces cybersecurity and legislative evolution, which is why efforts such as the one represented by this paper are pivotal. International law enforcement bodies Europol or the International Cyber Security Protection Alliance (ICSPA) emphasized the topics of deficient international coordination, harmonization and joint Internet governance, alongside insufficient resources to impose existing laws.

Common People

- Finally, as already indicated earlier, we sense that cybercrime has lowered the barrier for common people criminal involvement for manifold reasons; something we could call a "democratization of crime". First, small cybercriminal acts are often romanticized or belittled by both the perpetrator as well as society, which works as seed for criminal "careers". Second, there are plenty of mediatizes inspirational reference models of other "ordinary" people-turned-outlaw cases, e.g., by breaking behavioral codes or law on and through the internet. Further, the general user mass has quickly grown more tech savvy in terms of mastering techniques to enact something illegal on the internet, as well as to be able to rapidly gather the necessary know-how and tools to do so: "Crime-crowdsourcing" comes in handy not only to be able to perform ones action, but also to diffuse the moral barriers that are naturally associated with its planning and enacting. Also, because much of cybercrime or misconduct concerns an ambiguous legislative space and lenient law-enforcement stance, common people may not be conscious of their wrongdoing or their misdemeanor may fall into a legislative void-zone.

5 IMPLICATIONS FOR PREVENTION

The purpose of our present paper is to contribute to the foundations of preventing future crimes in cyber environments or by cyber means. Because criminal actions are crimes in a juridical sense only when they are coded in laws, our focus is not on crimes as an unlawful act but as an act of human rights injustice. This approach allows us to early forecasts types of crimes and to support the buildup of counter-measures including creating agile legislative practices to prevent crimes. The more time criminals have to harm other people without being detected, deprived of means, or prevented by laws and law enforcement, the more vulnerable our society becomes. We live in a risky world and crime is one important risk for smooth development of social welfare.

Prevention needs to look at underlying causes and drivers (means, opportunities, motives) of crime as well as specific arenas and scenarios of crime execution. And because prevention constitutes be an enormously wide social influence space, criminal prevention also needs to be able to set priorities. The primary preventive focus pursued in this paper adds on to the more generic criminal prevention that concentrates on underlying social and individual causes for criminal behavior in general. In our exposition, we focused specifically on the added value and levers of cyber environments for motivating and facilitating criminal intention and engagement, and we highlighted a set of arenas that should receive special attention.

In a sense, criminal intention can be reduced or its enactment discouraged by reducing the expected reward and increasing the risk involved for the criminal. One of the most important initial steps, nevertheless, is to become aware and legislatively represent the relevant technology and related misdemeanor. Our list of likely future crime arenas aims to improve possibilities of law making by means of agile design. Agile design has traditionally been seen as a paradigm of developing software fast and in a reliable way [37]. However, there is no obstacle for extending it to solve design problems in any field of human affairs, and in the case of cybercrime we are actually dealing with nothing else than negative implications of human technology interaction.

Mitigating technology victimization is one important approach to deal with the conundrum of negative impact of technology adoption. This can be achieved both on technology usage as well as on design level to address the victimization factors laid out in Section 3.2, and the foresee and cope with criminal-minded exploitation. User education and guidance are crucial preventive mechanisms that can be furthered through training and support powered by official institutional bodies, based on technology service providers' corporate social responsibility engagement, or generated by crowd initiatives such as the "Reset the Net"-action (https://www.resetthenet.org/). Criminal behavior, in turn, can be predicted not only based on scenario forecasting, but increasingly, law enforcement will itself utilize the analytical and predictive power of big data to identify potential crimes and criminals (e.g., [38]).

Design is another important preventive approach. Human technology interaction must be seen in the context of human life and in this wide perspective to technology design we are speaking of so-called *life-based design* or designing for life [39], [40]. In life-based design, the focus is in designing how people live instead of merely concentrating on engineering technical artefacts and their interaction properties. Of course, the laws proposed and emerging from the development and offence use of new technologies belong to the scope of life-based design. Hereby the main life-focus to design for would be on protecting and sustaining human rights and citizens' quality of life.

Hence, developing laws to regulate human behavior and life around the new (hostile) capacities opened by technical tools is an important form of designing for life. The second form or application arm of life-based design in the service of cybercrime prevention and cybersecurity enhancement would be to address directly the design of technological environments in order to contain the extent to which these offer crime-friendly or crime-stimulating conditions. Hence, we argue that life-based design shall be introduced to strengthen design against crime, [4], along the dimensions of means, opportunities, and motives (see Section 4). Both forms can be constructed by adapting important technology design paradigms. In case of future crime prevention, speed will be a vital factor and this is why agile design practices should be considered.

6 DISCUSSION

This paper reinforces criminologists' call for policy makers to go beyond legislation and law enforcement to tackle the underlying causes of crime as this more efficient and effective path to social benefit than conventional repressive responses [41]. In the case of cybercrime, prevention as silver bullet needs to time travel at the speed of light, because technology development and criminal appropriation is certainly outpacing traditional legislative sense-making and codification.

For this reason we first need to introduce a more foundational frame to crime definition, which we proposed in the form of characterizing crimes as acts that directly or indirectly harm other individuals' human rights. Human rights are a good guiding light to detect emerging fields of cyber-offenses. In the case of human basic rights on privacy we are currently for instance witnessing a cultural quarrel that is symptomatic and has significant impact on cybercrime context. The recent European Union Court ruling on user rights for personal data removal and deletion [26] is part of a series of jurisdictive assessments and a kind of a cultural background dispute between US and European stances on privacy. And it shows not only how the legislative system needs to catch up and adapt to new social implications of technology in terms of issuing new, internationally harmonized laws, but also in terms of applying existing ones.

In addition, we then need to understand the main properties of future emerging technologies for facilitating and stimulating crimes. New technologies create new capacities, possibilities and incentives to develop new kinds of violations to other human rights. In response to this future challenge, we need to trigger design measures that cope and counter cybercriminal evolution as regards narrowing the cybercriminal space and extending the cyber-legislative space.

Technology forecasting and outlining of priority cybercrime arenas is pivotal to support the task of diminishing and eliminate cybercrimes by giving by creating consciousness of the consequences of criminal action among the public, and by improving means of law enforcement for primary and secondary prevention through more apt legislation and, ironically, design and exploitation of technology to counteract cybercrime. In addition, user groups themselves and especially the big Internet players must be taking their social responsibilities more serious on the technology adoption end. Facebook's latest cyber safety initiative in collaboration with the Yale Center for Emotional Intelligence is welcome examples of this (see e.g., https://www.facebook.com/safety/ bullying/).

The principles of life-based design and agile development open hope to improve our capacity to design criminally defused technological environments and effective legislation in such a time frame that keeps pace or overtakes technology development and appropriation by criminals.

ACKNOWLEDGEMENTS

This paper is a result of the MineSocMed-project, funded by the Academy of Finland.

REFERENCES

[1] D. H. Autor, F. Levy, and R. J. Murnane "The skill content of recent technological change: an empirical exploration". The Quarterly Journal of Economics, vol. 118, iss. 4, 2003, 1279-1333.

[2] Norton, "2012 Norton Cyber Crime Report", Symantec, 2012, Available at: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[3] McAfee Center for Strategic and International Studies "Net Losses: Estimating the Global Cost of Cybercrime", Intel Security Report, June 2014. Available from: http://www.mcafee.com/

[4] D. J. Neufeld "Understanding Cybercrime2, Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010, pp. 1-10.

[5] L. Gamman and A. Thorpe, A. "Less is More: What Design Against Crime can Contribute to Sustainability", in: Sustainability via Security: A New Look, Built Environment, vol 35, iss. 3, A. Armitage and L. Gamman, Eds, 2008, Alexandrine Press, pp. 403-418.

[6] M. Rogers "A social learning theory and moral disengagement analysis of criminal behavior: An exploratory study. PhD thesis, Department of Psychology, 2001, University of Manitoba, Winnipeg.

[7] Universal Declaration of Human Rights. UN General Assembly. December 10, 1948.

[8] R. Young, L. Zhang and V.R. Prybutok "Hacking into the minds of hackers," Information Systems Management, vol. 24, iss. 4, 2007, pp. 281-287.

[9] E. A. Martin "Oxford Dictionary of Law", 7 ed., 2003, Oxford: Oxford University Press.

[10] S. Gordon "Technologically enabled crime: shifting paradigms for the year 2000. Computer and Security vol 14, iss. 5, 2000, 391-402.

[11] Detica "The cost of cybercrime", 2011, Report retrieved January 5 2013 from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

[12] M. Felson, and R. V. Clarke "Opportunity Makes the Thief: Practical Theory for Crime Prevention", Police Research Series, Paper 98, 1998, Home Office, London.

[13] P. M. Mayhew, R. V. G. Clarke, A. Sturman, and J.M. Hough "Crime as Opportunity. Home Office Research Study, no. 34, 1976, H.M.S.O, London.

[14] D. Andersen, A. P. Moore, J. M. Stanton, E. Rich, E. A. Weaver, J. J. Gonzalez, J. M. Sarriegui, P. M. De, A. Zagonel and M. Mojtahedzadeh "Preliminary System Dynamics Maps of the Insider Cyber-threat Problem", in Proceedings of the 22nd Conference on System Dynamics Modelling for Information Security. An Invitational Group Modeling Workshop at the

Software Engineering Institute, Carnegie Mellon University, 2004.

[15] K. D. Loch, H. H.Carr, and M.E. Warkentin "Threats to information systems: today's reality, yesterday's understanding", MIS Quarterly, vol. 16, iss. 2, 2012, 173-185.

[16] R. Willison "Understanding the offender/environment dynamic for computer crimes," Information Technology & People, vol. 19, iss. 2, 2006, pp. 170-186.

[17] R. Willison and J. Backhouse "Opportunities for computer crime: considering systems risk from a criminological perspective," European Journal of Information Systems, vol. 15, iss. 4, 2006, pp. 403-414.

[18] Court of Justice of the European Union "Judgment in Case C-131/12". Press Release no. 70/14, 2014, Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

[19] Facebook Inc. "Managing Social Network Accessibility Based On Age", United States Patent Application, no. 13/687867, May 29, 2014. Available from http://appft.uspto.gov.

[20] Taloustutkimus Oy "Copyright barometer 2012 [Tekijänoikeusbarometri 2012]", 2012, Available at: http://www.kulttuuriuutiset.net/easydata/customers/kulttuuriuutiset/files/pdf/tekijanoikeusbarometri_2012_piratismi.pdf

[21] E. Gibson "Smartphone dependency: a growing obsession with gadgets", 2011, Available at: http://usatoday30.usatoday.com/news/health/medical/health/medical/mentalhealth/story/2011/07/Smartphone-dependency-a-growing-obsession-to-gadgets/49661286/1

[22] American Psychiatric Association "Diagnostic and Statistical Manual of Mental Disorders (Fifth ed.).", 2013, Arlington, VA: American Psychiatric Publishing.

[23] M. Fishbein and I. Ajzen "Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research", 1975, Reading, MA: Addison-Wesley.

[24] C. Hollin "Psychology and crime: An introduction to criminological psychology", 1989, New York: Routledge.

[25] P. A. Miller and N. Eisenberg "The relation of empathy to aggressive and externalizing/antisocial behavior." Psychological Bulletin, vol. 103, iss. 3, 1988, pp. 324–344.

[26] R.A. Martin, G.E. Berry, T. Dobranski, M. van Horne "Emotion perception threshold: Individual differences in emotional sensitivity", Journal of Research in Personality, vol. 30, iss. 2, 1996, pp. 290–305

[27] J. Post "The dangerous information system insider: Psychological perspectives.", 2006, Available from http://www.infowar.com

[28] R. Blackburn "The psychology of criminal conduct: Theory, research and practice, 2003, Toronto: John Wiley & Sons.

[29] European Cybercrime Centre (EC3) & International Cyber Security Protection Alliance (ICSPA) "Project 2020. Scenarios for the Future of Cybercrime - White Paper for Decision Makers." Europol. 2013, Retrieved 29.10.2013 from https://www.europol.europa.eu/latest_publications/85.

[30] A. Chandler "The changing definition and image of hackers in popular discourse", International Journal of the Sociology of Law, vol. 24, iss. 2, 1996, pp. 229-251.

[31] K. Hafner and J. Markoff "Cyberpunks: Outlaws and hackers on the computer frontier", 1995, Toronto: Simon and Schuster.

[32] S. Helfenstein "Product Meaning, Affective Use Evaluation, and Transfer: A Preliminary Study", Human Technology, vol. 1, iss. 1, 2005, pp. 76-100.

[33] C. A. Anderson, A. Shibuya, N. Ihori, E. L. Swing, B. J. Bushman, A. Sakamoto, H. R. Rothstein, M. Saleem "Violent video game effects on aggression, empathy, and prosocial behavior in eastern and western countries: A meta-analytic review", Psychological Bulletin, vol. 136, iss. 2, 2010, pp. 151–173.

[34] R. Linturi, O. Kuusi, and T. Ahlqvist (Eds) "Suomen sata uutta mahdollisuutta: radikaalit teknologiset ratkaisut" [Finland's onehundred opportunities: radical technological solutions]. Publication of the Finnish Parliament's Committee for the Future, 6/2013.

[35] C. McFarland, F. Paget, and R. Samani R "Jackpot! Money Laundering Through Online Gambling", McAffee labs report, 2014, Available at: http://www.mcafee.com/ca/resources/white-papers/wp-jackpot-money-laundering-gambling.pdf

[36] H. Sverdlove and J. Cilley "Pausing Google Play: More Than 100,000 Android Apps May Pose Security Risks", Bit9 report, 2012.

[37] K. Beck, M. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Grenning, J. Highsmith, A. Hunt, R. Jeffries, J. Kern, B. Marick, R. C. Martin, S. Mellor, K. Schwaber, J. Sutherland and D. Thomas "Manifesto for Agile Software Development". Agile Alliance, 2010. Available at: http://agilemanifesto.org/

[38] R. Berk and J. Bleich "Statistical Procedures for Forecasting Criminal Behavior: A Comparative Assessment", Criminology & Public Policy, vol. 12, iss. 3, 2013, pp. 513-544.

[39] J. Leikas "Life-Based Design – A holistic approach to designing human-technology interaction", VTT Publications 726, 2009, Helsinki: Edita Prima Oy. Available at: http://www.vtt.fi/inf/pdf/publications/2009/P726.pdf

[40] P. Saariluoma and J. Leikas "Life-Based Design – an approach to design for life", GlobalJournal of Management and Business Research, vol. 10, iss. 5, 2010, pp. 17-23.

[41] L. W. Sherman, D. C. Gottfredson, D. L. MacKenzie, J. Eck, P. Reuter, and S. D. Bushway "Preventing Crime: What Works, What Doesn't, What's Promising", U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 1998. Available at: https://www.ncjrs.gov/pdffiles/171676.pdf