TAL TECH

DOCTORAL THESIS

Modelling Financially Motivated Cyber Crime

Tiia Sõmer

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2022

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
10/2022

Modelling Financially Motivated Cyber Crime

TIIA SÕMER

TAL TECH PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science
This dissertation was accepted for the defence of the degree of Doctor of Philosophy (cyber security) 02/03/2022

Supervisor: Dr Rain Ottis
School of Information Technologies
Tallinn University of Technology
Tallinn, Estonia

Co-supervisor: Dr Patrick Voss de Haan
Bundeskriminalamt
Germany

Opponents: Dr Hervé Borrion
Associate Professor - Deputy Head of Department
University College London
UCL Department of Security and Crime Science
UCL Jill Dando Institute of Security and Crime Science

Dr Matti Näsi
University Lecturer, Criminology
Institute of Criminology and Legal Policy
University of Helsinki

Defence of the thesis: 03/05/2022, Tallinn

Declaration:
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology has not been submitted for doctoral or equivalent academic degree.

Tiia Sõmer

---
signature

ISSN 2585-6898 (publication)
ISBN 978-9949-83-800-4 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9949-83-801-1 (PDF)
Printed by Koopia Niini & Rauam

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
10/2022

Finantsiliselt motiveeritud küberkuritegevuse modelleerimine

TIIA SÕMER

TAL TECH
KIRJASTUS

Contents

List of publications

The list of the author's publications[1], from which this thesis has been prepared:

I Somer, Tiia; Hallaq, Bil; Watson, Tim (2016). Utilising journey mapping and crime scripting to combat cyber crime. Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS 2016: Universität der Bundeswehr, Munich, Germany, 7-8 July 2016. Ed. Koch, Robert; Rodosek, Gabi. Reading,UK: Academic Conferences and Publishing International, 276−281.

II Somer, Tiia; Hallaq, Bil; Watson, Tim (2016). Utilising journey mapping and crime scripting to combat cyber crime and cyber warfare attacks. Journal of Information Warfare, 15 (4), 39−49.

III Somer, Tiia; Tiido, Anna; Sample, Char; Mitchener-Nissen, Timothy (2018). Application of journey mapping and crime scripting to the phenomenon of trolling. In: Hurley, John S.; Chen, Jim Q. (Ed.). Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018: National Defence University, Washington DC, USA, 6-9 March 2018 (465−473). Reading, UK: Academic Conference and Publishing International Limited.

IV Somer, Tiia (2019). Taxonomies of cyber crime: an overview and proposal to be used in mapping cyber criminal journeys. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019: University of Coimbra, Portugal, 4-5 July 2019. Ed. Cruz, Tiago; Simoes, Paulo. Reading, UK: ACPI, 475−483.

V Somer, Tiia (2021). Modelling financially motivated cyber crime. Proceedings of the 16th International Conference on Cyber Warfare and Security, ICCWS 2021: Tennessee Tech University and the Oak Ridge National Laboratory, USA, 25-26 February 2021.

[1] All publications have been published in international peer-reviewed journals or conference proceedings, which are considered suitable for inclusion in a TalTech PhD thesis.

Author's contribution to the publications

I In **Publication I**, as the main and leading author of this publication, the author analysed ways in which utilising methods from typically non-cyber disciplines, social sciences and criminology, can successfully be applied to the cyber domain to aid the fight against and the prevention of cyber crime. The publication proposed a journey mapping methodology to deconstruct cyber criminal acts and find ways to use the methodology in order to investigate crimes, fight against them, or find countermeasures.

II In **Publication II**, as the main and leading author of this publication, and as a further development from **Publication I**, the author analysed mapping cyber criminal processes in more detail. In addition to crime, the application of the model to cyber warfare was discussed. The publication explained how to best deconstruct the attacks: tactics, methodologies, and techniques used; targets and consequences – regardless of attribution (cyber crime or cyber warfare). The publication concluded that even though intent and end goals are different in cases of cyber crime and cyber warfare, the underlying attack cycle remains the same in both: preparing for the attack, executing the attack, and following an exit strategy.

III In **Publication III**, as the main and leading author of this publication, the author proposed ways in which journey mapping methodology can be applied to the phenomenon of trolling. The journey mapping methodology, developed earlier in **Publications I and II**, was taken further and used for analysing the phenomenon of trolling. The article concluded that the methodology of journey mapping and crime scripting can be successfully utilised to explain cyber attacks other than crime, including trolling.

IV In **Publication IV**, as the main and the only author for this publication, the author analysed the definitions and taxonomies currently used for cyber crime and discussed their potential application for modelling cyber crime. The author concluded that the current definitions and taxonomies cannot be applied without adaptation to model cyber crime, and proposed a new taxonomy to use for mapping cyber criminal journeys.

V In **Publication V**, as the main and only author for this publication, the author proposed a process model for financially motivated cyber crime. This is a practical mechanism that can be used by various stakeholders in the cyber crime investigation and prevention process. The article concluded, that the model provides a step-by-step account of actions taken by the criminals throughout the cyber crime process, allowing the identification of the major decision points criminals pass through.

Abbreviations

APT/APA	Advanced Persistent Threat/ Advanced Persistent Attack
CaaS	Crime-as-a-Service
CEO	Chief Executive Officer
CEO fraud	Chief Executive Officer fraud
DDoS	Distributed Denial-of-Service
DRM	Digital Rights Management
E-CRIME	EU FP 7 project Economic Impacts of Cyber Crime
GT	Grounded Theory
GTM	Grounded Theory Methodology
ICT	Information- and Communication Technology
LEA	Law Enforcement Agencies
VoIP	Voice over Internet Protocol

Terms

Attack vector	Means or path by which a criminal can gain access to a computer or network
Crime scripting	Deconstructing a crime into its smallest component actions
Criminal journey	End-to-end process of a criminal in committing crime
(Customer) journey mapping	Visualisation of customer experience, mapping out the overall end-to-end process, from the first to final touchpoint
Cyber criminal cycle	Process of commissioning a cyber crime
Cyber crime	Activity that involves the use of information technology for criminal purposes at any stage of the process
Cyber range	Cyber-synthetic virtual environment in which organisations can test critical capabilities
Information age	Historical period that began in the mid-20th century, to an economy primarily based upon information technology
Law Enforcement Agencies	Government agencies responsible for the enforcement of law (e.g. police, prosecution)
Macroeconomics	Study of how the economy and the market system function
Microeconomics	Study of the economic activities of individuals and enterprises
Victimisation	The process of being victimised or becoming a victim
Victimology	Study of victimisation

"To perfectly understand a problem, omit every superfluous conception, reduce it to its simplest terms, and divide it into its smallest possible parts."

Rene Descartes (1596-1650), *Rules for the Direction of the Mind*

1 Introduction

> *"At each stage of the evolution of society a particular form of crime occurs. When the primary sector used to dominate, crimes against people (murders, assassinations, assaults, slavery, prostitution, etc.) accounted for most reprehensible acts. With the development of the secondary sector, the production of manufactured goods created damages to property (theft, concealment, destruction, damage, etc.). With the emergence of service sector, "smart" white-collar delinquency emerged. Services rely on often complex, legal and financial structures, exploited by fake authors, frauds, embezzlements, money launderers, etc. Our century sees the consecration of digital technologies. These are now ubiquitous in the spectrum of human activities (information, culture, education, administration, commerce, industry, services, health, justice, security, defence, etc.). They are a source of progress, of growth if they are mastered, but they also offer risks of fragility. This is not an evolution but a true revolution, which we do not yet measure all the effects."*
>
> *General Marc Watin-Augouard, French Gendarmerie* [1]*. (author's translation)*

The past decades have seen the rapid development of internet, and information and communications technologies. The transformations these have brought have a great impact on the way societies, economies and people operate. Worldwide internet usage has increased from 1.7 billion users in 2009 to more than 4.1 billion users as of July 2019 [2]. In addition to people, the number of digital devices connected to the internet is increasing, with more things connected to the internet than people. According to reports, the number of internet connected devices reached 18 billion in 2018, and will be close to 50 billion in 2030. However, the rapid developments of internet and related ICTs are not only a source for progress, but have also made everyone and everything vulnerable to various risks. Cyber crime is a major public concern. Lone criminals and criminal organisations worldwide have access to powerful and evolving capabilities, which they use to commit cyber crimes. Cyber crime is a global problem.

The reasons for risks and our vulnerability are two-fold with the first being that governments, societies, businesses and people are ever more dependent on cyberspace. Secondly, cyber criminals continually adapt to new technologies and develop new methods to compromise systems and their users. Mitigating this threat requires those working in cyber security to constantly monitor the cyber environment to identify how criminals operate and what measures can be taken to counter their activities.

Financial gain has been a strong motivating factor in criminal activity and as more personal and commercial activity takes place online, this has increasingly attracted those with malicious intent. There are frequent reports of ransomware attacks in which computer files have been encrypted and payment is demanded to regain access. There is CEO fraud, when a senior member of an organisation is fraudulently asked to approve the transfer of funds to an account controlled by criminal elements. Consumers are duped into investing in online investment frauds that promise quick wins, but result in the loss of their deposit. Sophisticated malware is being installed into a computer or computer system, which steals sensitive information, trade secrets or intellectual property. Computers become part of botnets that take part in widespread cyber criminal

attacks. What we don't hear about that much is how crimes happen, what effort goes into the preparation and execution of crimes, and how they are monetised.

Cyber criminals use human, social or technical weaknesses involving a range of technical methods, but also employ new business models to commit crimes. Research to date has tended to focus on technical and human aspects of cyber crime, but understanding the lifecycle, and process of a crime has not received as much attention. Computer scientists have researched primarily the "hard" aspects of cyber security, while social scientists discuss the human "soft" aspects, with each lacking an understanding of the other. Analysis of cyber crime processes has been a challenge and the need to develop such an understanding has been identified by law enforcement, academia, governments, [3] [4] [5] and in interviews with Law Enforcement Agencies conducted for this thesis [6] [7] [8] [9] [10] [11] [12]. This indicates the need to recognise the various perceptions of cyber crime that exist among academic disciplines. Cyber crime is a complex system, which cannot be understood by computer science alone. Toomas Hendrik Ilves, in his address to 2014 Munich Security Conference, concluded that the problem in cyber security we face today represents the culmination of a problem diagnosed 55 years ago in C.P. Snow's famous essay "The Two Cultures". This highlights the absence of dialogue between the scientific-technological and the humanist traditions [13]. The aim of this dissertation is to shine a new light on these debates through an interdisciplinary view. It combines computer science with social sciences, utilising traditionally non-computer science methods to understand the current technical view of cyber crime. In particular, this dissertation will examine how cyber crimes are conducted from a criminal's point of view and will provide a model to assist in developing a better understanding of the issues involved. Bridging the gap between the "two cultures" can be a basis for better decisions in our attempts to fight against and prevent cyber crime.

Cyber criminals are increasingly using new technologies, but also developing innovative techniques, procedures and business models for their criminal purposes. Cyber crime is a mirror of our contemporary economic system, often not only mirroring, but out-innovating legitimate economies [14]. Cyber criminals operate in the same manner as legitimate commercial networks with clearly established business objectives and trusted supply chains for services or products that require outsourcing or development. Cyber criminals know what they are looking for, have clear objectives they want to achieve, meticulously plan how to achieve these goals, and are willing to spend time to research and plan the necessary actions. Crimes can be seen as a process where resources are required and decisions are made that together constitute the modus operandi of a crime. Cyber crimes usually, but not always, require preparation, planning and making rational choices and decisions along the way. Organised cyber crime, in particular, relies heavily on coordination and established processes. Contrary to legitimate business corporations, the choices and decisions of criminals are not explicitly written down as policies or procedures, rather they happen on an ad-hoc basis. Yet analysing the complete processes of different cyber criminal acts provides a pattern of underlying associated decision points and processes, which provides a different view of cyber crime. Unless we understand the complex process of cyber crime, we cannot see the wider picture and will be reactive, rather than proactive in countering this threat.

Cyber crime research is a new discipline, where the development of precise or comprehensive theories and theoretical frameworks has only recently started to emerge. Only a limited amount of research has used an interdisciplinary approach. Much of the current literature on cyber crime within the computer science discipline has focussed on

technical cyber security, the economics of the cost of cyber crime, or within social science studying the human aspects and victimology. However, research of cyber crime as a process that involves a complex system of interconnected actions from preparation to completion, and interconnected actors of criminals, criminal ecosystem and victims has been limited.

Central to the work of this dissertation is the construction of a financially motivated cyber crime process model, the Cyber Criminal Journey Mapping (JMAP) model. This dissertation has used Grounded Theory Methodology (GTM) [15] to generate a model for financially motivated cyber crime. GTM is one of the more practical methods to use in cases of incomplete data, with analysis commencing with the first available pieces of data. Through several reiterations and validation rounds more data is included, thereby grounding the developed model in more data. In line with the methodology, the process of data collection, and updating and validating the model was reiterated five times.

The Criminal JMAP model developed by the author is an explanatory and practical tool that can be used by various stakeholders in the cyber crime investigation and prevention process. It provides a step-by-step account of actions taken by the criminals throughout the crime. This has important implications in that it provides the potential to overcome challenges in understanding cyber crime. It is not intended to be a rigid or linear process but a flexible tool to understand the key steps within the cyber crime process, allowing the identification of pinch points the criminals have to pass through. The aim is to allow those investigating cyber crimes or developing countermeasures to quickly apply new crimes to the model (or quickly apply the model to new crimes) and focus on the specific known (and unknown) pinch points in order to conduct their work more effectively.

One of the most developed skills commonly used is dissection [16]. This involves dismantling problems into small components, yet we often do not put these components together again. We are more skilled as analysts, not synthesists [17]. The JMAP model developed as a result of the current dissertation aims to develop a general process model of cyber crime, in order to both dismantle the cyber crime process, and to enable us to put the pieces back together. Developing the JMAP model drew inspiration from crime scripting used in criminology, the phase-based approach used by the military, and customer journey mapping used in economics. By visually presenting the sequence of steps constituting a cyber crime, those working on preventing, investigating or fighting these activities will be able to identify the specific phases and steps that cyber criminals pass through in committing their crimes. By modelling and understanding both general and specific cyber crimes, a better oversight of existing countermeasures and potential development of new innovative countermeasures or disruption techniques can be formulated. The model can provide a sense of processes and practices through which cyber crime occurs (including both technological and organisational pathways), and has the flexibility for use in wide range of cyber crimes.

The author is fully aware of the ethical issues that this dissertation may raise, in the sense of serving as a manual for criminals, by enabling them to “know what we know” about them. However, as can be seen from history, there are certainly some criminals who will benefit from such knowledge. As Professor Anderson, discussing a similar question on cryptography, commented [18]: “While some bad guys will benefit from [a book such as] this, they mostly know the tricks already, and the good guys will benefit much more” [18] (as quoted in [19]). As pointed out throughout this dissertation,

an increased understanding of cyber crime processes together with a better developed specific knowledge and skills of law enforcement agencies will increase the effectiveness of investigations. In conclusion, the developed JMAP model for financially motivated cyber crime serves as a description of the underlying principles of cyber criminal processes, leading to the identification of pinch points. This provides opportunities to conduct more effective investigations, find better countermeasures, and develop novel policy, investigative, or technical approaches in the fight against cyber crime.

1.1 Problem statement

Much of the current literature on cyber crime pays particular attention to the mechanisms of the activity [20] [21] [22] – that is, how it happens. This has resulted in technical factors such as malware types, security vulnerabilities and the prevention of certain types of attack being discussed most frequently. In recent years, there has been an increasing amount of literature on the human factor and economic aspects of cyber crime. However, there has been less discussion about the dynamic and constantly changing nature of cyber crime as a (business) process and it is not clear what are the factors influencing this overall process. The ability to write a piece of malware alone does not mean a person will be a successful cyber criminal. A successful financially motivated cyber crime means the criminal has to take a series of consecutive steps [23]. Criminals prepare and plan crimes, execute them and finally generate income for themselves. The need to understanding cyber crime as a whole process, in order to more effectively fight and prevent it, has been identified by law enforcement agencies, international organisations and academia [3] [4] [5] [6] [7] [8] [9] [11] [12]. The requirement for such an understanding was also emphasised during validation events and interviews conducted for the current dissertation [12] [9] [7] [11] [8] [24] [20] [10].

The motivation, or intent, of cyber criminals can vary from the purely financial to political, ideological, entertainment, or credibility amongst their peers. It is beyond the scope of this dissertation to examine criminal intent – a big area of research in itself – but will instead focus on crimes committed for financial gain. However, it must be said that the processes of cyber crime, as well as the tools and techniques used by criminals remain similar, regardless of their motivation. Similar attempts at modelling are provided in literature on cyber warfare, e.g. [25]. It has been noted, that many techniques and approaches are common across a range of criminal or terrorist activities [26]. In the case of financially motivated cyber crime, monetization is an important part – even enabler – of the criminal journey.

The aim of the research is to develop a theoretical/ conceptual framework model of analysis that enables a better understanding of financially motivated cyber crime as a complex system, in order to fight against it in a dynamic environment.

The main contribution of this doctoral dissertation is to present a structured, systematic and multidisciplinary study on cyber crime as a complex system. The final result is a Criminal JMAP model that has explanatory power, flexibility and potential usability across different cyber crimes. In addressing these objectives the thesis further makes novel contributions in proposing a definition for financially motivated cyber crime and a taxonomy for use in mapping cyber criminal journeys.

1.2 Research questions

The main research question of this dissertation is: **how to model the process of financially motivated cyber crime**? In answering the main umbrella research question and addressing mapping of cyber criminal journeys, the study will examine three research questions. Starting from defining cyber crime, taxonomies used to explain and classify cyber crime, leading to how to analyse cyber crime. To further clarify these research questions, they are split into sub-questions aimed at seeking more precise answers and addressing more particular nuances of the subject. The question is addressed by providing answers to each sub-question. The mapping of research questions to the corresponding publication(s) and thesis chapter is presented in Table 1.

Q 1. What is financially motivated cyber crime?
- 1.1. What is cyber crime and how do we understand it?
- 1.2. How does our understanding shape or affect the way financially motivated cyber crime is being analysed and approached?

Q 2. What is the most suitable taxonomy for appreciating financially motivated cyber crime?
- 2.1. Which taxonomies are currently used for classifying cyber crime?
- 2.2. How appropriate are these taxonomies for classifying financially motivated cyber crime?

Q 3. Which model can be adapted for modelling financially motivated cyber crime?
- 3.1. Which models have been used for modelling cyber crime?
- 3.2. Which existing models are available or can be adapted to model the process of financially motivated cyber crime?
- 3.3. Can existing models be adapted for financially motivated cyber crime?

Table 1. Mapping research questions to publications and thesis chapters

Q 1. What is financially motivated cyber crime?		
1.1. What is cyber crime and how do we understand it?	**Publication IV**	Chapter 2
1.2. How does our understanding shape or affect the way financially motivated cyber crime is being analysed and approached?	**Publication IV**	Chapter 4
Q 2. What is the most suitable taxonomy for appreciating financially motivated cyber crime?		
2.1 Which taxonomies are currently used for classifying cyber crime?	**Publication IV**	Chapter 2
2.2. How appropriate are these taxonomies for classifying financially motivated cyber crime?	**Publication IV**	Chapter 4
Q 3. Which model can be adapted for modelling financially motivated cyber crime?		
3.1. Which models have been used for modelling cyber crime?	**Publication I, II, III**	Chapter 5
3.2. Which existing models are available or can be adapted to model the process of financially motivated cyber crime?	**Publication I, II, III, V**	Chapter 5
3.3. Can existing models be adapted for financially motivated cyber crime?	**Publication I, II, III, IV, V**	Chapter 5

1.3 Contribution

This thesis is based on a collection of peer-reviewed publications in conference proceedings and journals[2]. **Publication I** analysed how utilising methods from typically non-cyber disciplines can successfully be applied to cyber crime. In it, the author proposed a journey mapping methodology to deconstruct cyber criminal acts and find ways to use the methodology in order to investigate crimes, fight against them, or find countermeasures. **Publication II** built on previous work and analysed mapping cyber

[2] Publications which have been included are considered suitable for inclusion in a TalTech PhD thesis.

criminal processes in more detail, and investigated the potential use of journey mapping methodology to cyber warfare. The publication concluded that underlying attack mechanics are similar, whether in crime or warfare. **Publication III** further proposed ways in which the methodology can be applied to the phenomenon of trolling. **Publication IV** analysed definitions and taxonomies currently used for cyber crime and discussed their potential application for modelling cyber crime. This analysis concluded that current definitions and taxonomies cannot be applied without adaptation to model cyber crime, and proposed a new taxonomy to use for mapping cyber criminal processes. **Publication V** proposed a process model for financially motivated cyber crime, a practical solution that can be used in the cyber crime investigation and prevention process. The proposed model provides a generic step-by-step account of actions taken by the criminals throughout the cyber crime process, enabling the identification of major decision points the criminals pass through.

The main contribution of this dissertation is to present a structured, systematic and interdisciplinary study on cyber crime as a process. The JMAP model for financially motivated cyber crime developed as a result of this thesis is a model that is explanatory and has flexibility. By graphically presenting the sequence of events constituting a cyber crime, those tasked with investigating, countering or preventing it, will be able to identify the specific phases and steps that cyber criminals pass through when committing their crimes. By mapping and understanding both general and specific crime journeys, a better oversight on existing countermeasures and current prevention strategies can be formulated. This can be used for a range of purposes including developing training programs for law enforcement. In addition, such mapping could provide a basis for the development of new novel countermeasures, prevention strategies and disruption techniques.

As explained in **Publication I**, the benefits of producing this visual representation are that;

a. By identifying the commonalities in different cyber crimes, we can provide a cognitive picture of the sequence of events that underpin the majority of these,
b. By comparing detailed models of different types of cyber crime against a general model, those tasked with preventing and/ or defending against such crimes can see where to focus their resources for maximum effect,
c. Modelling can provide a basis to experiment via cyber range based exercises. The application of countermeasures at various points along the pathway can inform the selection of the most effective ones for application in real world scenarios,
d. Improving the general understanding of modus operandi and identifying pinch points in the overall cyber criminal processes can help law enforcement authorities in investigations,
e. By mapping the pinch points and decision processes of cyber crime, we can fight organised crime, which is heavily reliant on such processes,
f. By mapping pinch points and decision processes, new legislative measures can be adopted to target specifically these points in the cyber criminal processes.

Researching cyber crime poses several methodological challenges [19]. While studying which qualitative method would best fit to construct a model on cyber crime as a system, Grounded Theory Methodology [27] [28] was selected. This methodology was deemed most suitable as current research on cyber crime is limited and no precise or

comprehensive frameworks to analyse cyber crime processes have emerged. Since being introduced, Grounded Theory has proved to be a useful approach in various disciplines [29] and is also becoming increasingly popular research method in computer science [29]. It does not focus on testing hypotheses taken from existing theoretical frameworks, but instead promotes the development of a theory of an action, process or interaction grounded in data collected [29]. A central characteristic of Grounded Theory is simultaneous data collection, analysis and writing which are considered interrelated processes [27].

1.4 Thesis structure

This thesis is divided into six chapters. The introduction chapter examines the cyber crime problem, presents research questions and contribution of the thesis.

Chapter two begins by providing an overview of related work and background in research of cyber crime and financially motivated cyber crime. It will then move on and look at how cyber crime and financially motivated cyber crime have been defined, as well as which taxonomies have been proposed.

The third chapter is concerned with the methodology used for this dissertation. It provides an overview of the methodology used and the way it was used in the thesis. The chapter further analyses the results of validation events, focus group discussions and interviews (expert assessment) undertaken for validation of the model.

Chapter four presents a definition for financially motivated cyber crime and proposes a taxonomy for use in modelling financially motivated cyber criminal processes. The chapter also includes an overview of economic perspectives and the cyber criminal ecosystem.

Chapter five explores existing models for modelling cyber crime and looks at how these existing models can be adapted to model the process of financially motivated cyber crime. As the main result of the current thesis, this chapter presents a Criminal JMAP model for financially motivated cyber crime.

Finally, Chapter six concludes this thesis and presents ideas for future work.

2 Background and related work

Modern life, governance, economic activities and society in general are more and more reliant on cyberspace. While the internet is providing ever more benefits to individuals, organisations and governments, it has also given rise to a new type of crime: cyber crime. Cyber crime is a vast and growing problem internationally, and its impacts – social, economic, or political – have gained substantial attention within the past years [30], with some estimates of cyber criminal revenues reaching 1,5 trillion USD annually in 2018 [14]. While it is beyond the scope of this thesis to examine the financial loss of damages or revenues from cyber crime, as there are no reliable metrics for estimating such costs, it is clear that the numbers are high.

This chapter will focus on research question 1: "What is financially motivated cyber crime?". In answering this question, section 2.1 will answer sub-question 1.1. "What is cyber crime and how do we understand it?".

Is cyber crime different from „traditional crime"? Is there such a thing as cyber crime? In order to better understand cyber crime and the processes, tactics, techniques and procedures used by cyber criminals, it will be useful to have a robust framework. This chapter reviews a number of well-known taxonomies and approaches used currently, and analyses whether these can be used to understand cyber criminal processes. The current chapter is based on **Publication IV**, which analysed a number of definitions and taxonomies used for (financially motivated) cyber crime.

Cyber crime, computer crime, digital crime, and high-tech crime are all words that have come into everyday use around the world. But what is cyber crime? Cyber crime can cover a wide range of actions, with a common denominator of using information technology for criminal purposes [31]. The issue has grown in importance and the rapid adoption of information technology use has led to a major growth in financially-motivated cyber crime [32]. Modern society is relying on information technology for ever more tasks, from simple personal use of IT to critical tasks of governance and national security. Every person, enterprise or government who conducts any activity online, can fall victim to cyber crime.

Publication IV has analysed the existing taxonomies and definitions for cyber crime. As a result, and as has been identified by previous research by [30], it became apparent that there is currently little agreement on what cyber crime is and how to define it. Several attempts have been made by either legal, technological, criminological or law enforcement practitioners. Some scholars have also looked at cyber crime from economical, cultural or psychological aspects. One of the reasons for not having a commonly accepted definition for cyber crime could be that our understanding of the rapid growth and flexible nature of cyber crime does not follow its pace and is therefore limited. The currently developed definitions and taxonomies focus on different aspects of cyber crime, classifying cyber crimes by using typologies [33]. In an attempt to conceptualise the cyber criminal processes, the underlying question after the review of literature is: how to provide a taxonomy, which would give better insight into an understanding of cyber criminal processes from a criminal's perspective, reflecting all possible steps they pass through and the decision points within that process?

2.1 Cyber crime and financially motivated cyber crime

The term "cyber crime" embodies a multitude of concepts and a generally accepted overarching definition is lacking. Drawing on existing literature, the current definitions for defining cyber crime differ based on criminals, victims, attack vectors, or implications. Brenner asks if there is such a thing as cyber crime, and argues that cyber crime is "nothing more than the migration of real-world crimes into cyberspace" [34]. The European Commission refers to cyber crime as "criminal acts using electronic communications networks and information systems or against such networks and systems" [35]. The Council of Europe Convention on Cybercrime [36] defines cyber crime as "offences against confidentiality, integrity and availability of computer systems and data; computer related offences; content related offences; or offences related to infringements of copyright and related rights". The United Nations Manual on the Prevention and Control of Computer Related Crime [37] covers five common types of crimes that use computers: fraud by computer manipulation; computer forgery; damage to or modification of computer data or programs; and unauthorised access to computer systems and services. The INTERPOL defines pure cyber crime as "crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user" [38].

Some proposals are based on the well-established traditions of criminal justice, stating that information technology is a tool with which existing crimes are facilitated, and view cyber crime as development and innovation in traditional crimes. Wall [39] discusses the rise and rapid increase of cyber crime from the perspective of criminal justice, and concludes that the internet is just an additional tool to commit old or new crimes. He proposes there are three types of crimes: traditional crimes, partially new crimes and new crimes [39]. A practical definition is proposed by Kshetri [30] "cyber crime is a criminal activity in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations".

The German Federal Criminal Police Office has established a special "Service Centre for Information and Communications" designed to combat cyber crime. On its website [40] they give a working definition of cyber crime: "High tech and computer crime" means offences which are committed using information and communication technology or crimes which are targeted at these technologies [40].

The Estonian police [41] define cyber crime as "crimes committed against confidentiality, availability and integrity of computer data and computer systems". They also note that it is difficult to draw a line between cyber crime and other, traditional crimes.

The UK Cyber Crime Strategy defines cyber crime as "falling into one of two categories: new offences committed using new technologies, and old offences committed using new technology" [42], where the former means e.g. crimes against computer systems and data, and the latter means crimes where computers and other devices are used to facilitate the commission of an offence.

2.2 Taxonomies of cyber crime and financially motivated cyber crime

As presented in **Publication IV**, there is currently no single, universally accepted taxonomy which could be applied to cyber crime. Section 2.2 will answer research question 2.1. "Which taxonomies are currently used for classifying cyber crime?".

A number of the taxonomies follow the logic used for "traditional crimes" (e.g. [34] [39]), others use approaches based on technology, adversaries or threats (e.g. [43] [44]

[45] [46] [47] [48] [49] [50]), yet others base it on law (e.g. [36] [37]). Common points do exist among these taxonomies, but there are differences in structure and content. There is a clear distinction between comparing the approaches using the technical nature of cyber crime, with those using the impacts of crime. Researchers have studied different aspects of crime, such as the technical aspects (e.g. malware types and prevention of these) of executing crimes, or the human aspects (human error, victimisation, culture, etc.), but understanding cyber crime as a process and system remains less developed [10]. The following sections provide an overview of current taxonomies and approaches of cyber crime as concluded in **Publication IV**. The taxonomies and proposals which are being used today can be categorised as follows:

- Approaches based on criminology
- Approaches based on technologies, adversaries and threats
- Two dimension taxonomies
- Three dimension taxonomies
- Proposals by international bodies

2.2.1 Approaches based on criminology

Taxonomies based on criminology are built on approaches used in criminal justice. Such taxonomies see cyber crime as regular crime, where computers are enablers for "traditional" crimes. Brenner [34] states that the definition of cyber crime as "a crime committed on a computer network" should reflect existing national and international legal frameworks. According to her, this basic definition can cover most "traditional" crimes (e.g. theft, extortion, harassment) enabled by ICT, and she notes that there are also new crimes (such as DDoS). Brenner further discusses the difference between cyber crimes and cyber terrorism, and concludes that the methods used are largely the same, but motives differ: the intent in committing crimes in general is to reach some kind of personal gain; but in the case of terrorism it is different [34].

Wall [39] follows similar logic: the internet is just an additional, new tool to commit old and new crimes. Wall's work is primarily based on criminal justice. In addition to "old" and "new" crimes, he introduces a further category of "partially new crimes". As can be seen in Table 2, he proposes there are three types of crimes: traditional crimes, partially new crimes and new crimes.

*Table 2. Taxonomies of cyber crime based on criminological aspects (Adapted from **Publication IV**)*

Wall (2007)	Three different types of crime	- Traditional crimes, committed through use of ICT - Partially new crimes, modified crimes - New crimes, enabled by ICTs
Brenner (2001)	Two types of crime	- Traditional crimes, enabled by the use of ICT - New crimes, enabled by ICTs

2.2.2 Approaches based on technologies, adversaries and threats

Other proposals focus primarily on the technological aspects of crimes being committed or the nature of the cyber adversaries. These approaches distinguish between crimes based on how they are carried out and which aspects of computer and network infrastructure are the targets or vectors of attack. Table 3 below presents a number of different approaches in chronological order:

*Table 3. Taxonomies of cyber crime based on technical aspects (adapted from **Publication IV**)*

Landwehr et al [43]	The nature of computer security flaws as a basis	- Flaws by genesis (how the flaw arises) - Flaws by time of introduction - Flaws by location (hardware and software)
Howard [44]; Howard and Longstaff [45]	Based on existing data on security incidents	- Attackers (hackers, criminals, terrorists, vandals) - Tools (scripts, toolkits, user commands) - Access (implementation or design vulnerabilities, access permissions) - Results (corruption, deletion or disclosure of data, theft of resources, denial of service) - Objectives (intellectual challenge, peer status, financial gain, damage)
Hansman and Hunt [46]	Four-category model	- Attack vectors (the means by which the target is reached) - Targets (hardware, software, network, data) - Specific vulnerabilities and exploits (security flaws) - Payload (the outcome and effects)
Kjaerland [47] [51]	Built on earlier work and added a quantitative component	- Source sectors (top level domains) - Method of operation (resource theft, social engineering, malware, denial of service) - Impact (disruption, distortion, destruction, disclosure) - Target services (commercial or governmental)
Meyers et al. [48]	Based on attack vectors	- Viruses; - Worms; - Trojans; - Buffer overflows; - Denial of service; - Network attacks; - Physical attacks; - Password attacks/user compromise; and - Information gathering
Simmons et al. [49]	AVOIDIT taxonomy	- Attack Vector - Operational Impact - Defence - Information Impact - Target

Rogers [50] [52] [53]	Adversaries	- Script kiddies, newbies, novices; - Hacktivists, political activists; - Cyberpunks, crashers, thugs; - Insiders, user malcontents; - Coders, writers; - White hat hackers, old guard, sneakers; - Black hat hackers, professionals, elite; - Cyberterrorists

2.2.3 Two-dimension taxonomies

A number of two-dimensional classifications of cyber crime has been proposed, approached by different angles (see Table 4). Alkaabi et al. [54] propose a Type I and Type II taxonomy of cyber crime. Type I crimes "include crimes where the computer, computer network, or electronic device is the target of the criminal activity" [54]. This category is divided into four sub-categories:

- Unauthorized access offences
- Malicious codes offences
- Interruption of services offences
- Theft or misuse of services.

Type II crimes "include crimes where the computer, computer network, or electronic device is the tool used to commit or facilitate the crime" [54]. This is divided into three sub-categories:

- Content violation offences;
- Unauthorised alteration of data, or software for personal or organisational gain;
- Improper use of telecommunications.

Several authors [55] [56] [57] [58] have proposed a different two-level classification of cyber crimes, distinguishing between crimes committed using or those targeting computers and networks (hacking, viruses); and traditional crimes that are facilitated by the use of computers (illegal pornography, online fraud).

Similarly, the UK Home Office has proposed classifying crimes as being either cyber-dependent or cyber-enabled crimes [59]. Cyber-dependent in this classifications means new crimes, made possible by information technology (malware, hacking, viruses, DDoS, etc.); cyber-enabled are old crimes using new technologies (extortion, fraud, theft, etc.).

Gordon and Ford also propose a two-dimension approach of cyber crime saying that cyber crime "presents a continuum (Figure 1) ranging from crime which is almost entirely technological in nature and crime which is really, at its core, entirely people-related" [60]. The technology-centric crimes are similar to cyber-dependent crimes with people-centric crimes exploiting the human factor.

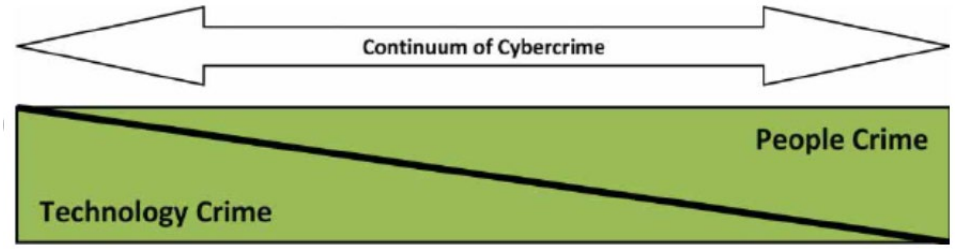

Figure 1. Continuum of cyber crime, as presented in [60]

*Table 4. Two-dimensional classification of cyber crimes (Adapted from **Publication IV**)*

Furnell [55], the Australian High Tech Crime Centre [56], Wilson [57], Foreign Affairs and International Trade of Canada [58]	Two-dimensional classification of crimes	- crimes committed using computers and networks (hacking, viruses); - traditional crimes that are facilitated by the use of computers (illegal pornography, online fraud)
Alkaabi et al. [54]	Two-dimensional classification of crimes	- Type I crimes, where the computer, computer network, or electronic device is the target of the criminal activity - Type II crimes, where the computer, computer network, or electronic device is the tool used to commit or facilitate the crime
UK Home Office [59]	Two-dimensional classification of crimes	- cyber-dependent crimes, and - cyber enabled crimes
Gordon and Ford [60]	Two-dimensional classification of crimes	- technology-centric crimes, and - people-centric crimes

2.2.4 Three-dimension taxonomies

A number of authors have proposed three-dimensional taxonomies of cyber crime, with variations on the nature and degree of specificity of these dimensions. As referred to in section 2.1 above, the European Commission's definition [35] proposes the publication of illegal content as a specific category, accompanying two categories familiar from the review of two-dimension taxonomies in section 2.2.3, namely traditional forms of crime committed over or using electronic technologies, and crimes unique to computer networks.

Wall [39] highlights that "value in cyberspace is attached mainly to the expression of informational ideas rather than things. The focus of cyber crime, therefore, is to acquire information in order to extract its value". Against this background, he distinguishes three typologies of cyber crime:

- Computer integrity crimes, which include hacking, cracking and denial of service attacks, activities that prevent access to systems by legitimate users or modify, corrupt or delete software and data;
- Computer-assisted crimes, which include virtual robberies, scams and thefts;
- Computer content crimes, which include the digital storage and communication of pornography, violence and offensive materials.

A considerable amount of research has been conducted on crimes made possible because of the internet. These include spamming, spreading viruses, trojans, botnets and worms. Wall identifies such crimes as a new generation of cyber crime, one in which massive automation is being employed to commit large numbers of individually low value crimes [39]. He also discusses the human factor behind cyber crimes, the links with old-fashioned crimes and the various motivations that cyber criminals might have, without drawing these into a formal taxonomy [39].

Goodman [61] categorised cyber crime into three types: crimes in which the computer is the end target; crimes where the computer is the tool to commit crimes; and crimes where there is an incidental presence of computer equipment.

Ghernaouti [62] emphasises that in such taxonomies the starting point for analysis should rely on motivations and intent, because the techniques and methods used by cyber criminals attacking different categories of targets are very similar and not easily distinguishable. She proposes a three dimension categorisation of cyber crime, differentiating crime from conflicts, wars and terrorism:

- Cyber crimes against people, including activities affecting their dignity and integrity, swindles and frauds, identity crimes and privacy related offences;
- Cyber crimes against assets, including the theft of data, the theft of services and resources, counterfeiting, software piracy, surveillance and espionage, the manipulation of information, and the fraudulent acquisition of intellectual property; and
- Cyber crimes against states, including destabilization, information warfare, and attacks on critical infrastructures.

Moitra [63] proposes a three-dimension classification for cyber crimes: based on motivation, opportunities, and skills. Additionally he proposes a different classification based on the victims, which can be segmented as individuals, organizations, systems and information types. Table 5 below provides an overview of three-dimensional taxonomies proposed.

*Table 5. Three-dimensional taxonomies of cyber crime (adapted from **Publication IV**)*

Wall [39]	Three- dimensional classification of crimes	- Computer integrity crimes (hacking, cracking and denial of service attacks, preventing legitimate access to systems or modifying, corrupting or deleting software and data); - Computer-assisted crimes (virtual robberies, scams and thefts); - Computer content crimes (digital storage and communication of pornography, violence and offensive materials).
Goodman [61]	Three types of cyber crime	- crimes in which the computer is the end target; - crimes where the computer is the tool; - crimes where there is an incidental presence of computer equipment.
Ghernaouti [62]	Distinguished cyber crime from cyber conflicts, wars and terrorism	- Cyber crimes against people (activities affecting their dignity and integrity, frauds, identity crimes and privacy related offences); - Cyber crimes against assets (theft of data, theft of services and resources, counterfeiting, software piracy, surveillance and espionage, manipulation of information, theft of intellectual property); and - Cyber crimes against states (destabilization, information warfare, attacks on critical infrastructures)
Moitra [63]	Three- dimensional classification of crimes	- Motivation for crime; - Opportunities to commit a crime; - and skills to commit a crime
Moitra [63]	Three- dimensional classification of crimes	Based on the victims: - individuals; - organizations; - systems; and - information types.

2.2.5 Proposals by international organisations

The taxonomies proposed through international organisations are significant because of their visibility and influence in shaping opinion, promoting research, and providing a framework for legislation aimed at combatting cyber crime. Such proposals also promote acceptance and common understanding between states, as well as giving direction to national policies and diplomacy. It must be noted, that globally nothing is agreed and Table 6 below provides a non-exhaustive overview of the proposals that have most influenced international understanding.

The best-known legal document proposing definitions and classifications at an international level is the **2001 Budapest Convention of the Council of Europe** [36]. This convention is well-known and widely recognised as one of the more comprehensive

international approaches to cyber crime. The Budapest Convention defined cyber crime as a set of instances, actors and objects. It gives definitions for “computer system”, “computer data”, “service provider” and “traffic data” for its own purposes and then puts forward the following classification of cyber crime:

- Offences against the confidentiality, integrity and availability of computer systems and data;
- Computer related offences (forgery, fraud);
- Content related offences;
- Offences related to infringements of copyright and related rights.

The total number of ratifications/accessions to the Convention is sixty-five states as of August 2020 [64]. However, the convention does not cover some types of crimes, which are widely considered as cyber crimes, or enablers for it: money laundering, identity theft or storing illegal contents.

The UN Manual on the prevention and control of computer related crime [37] acknowledged that there is a lack of global consensus on what constitutes cyber crime, and what is the legal definition for it. It further acknowledged that computer crimes are transnational in nature, but at the same time, there is a lack of harmonisation between different national legislations in investigating these crimes. The UN Manual [37] provides common terms and frameworks, but does not have any legal force or obligation for compliance. The manual covers five common types of crimes that use computers:

- Fraud by computer manipulation;
- Computer forgery;
- Damage to or modification of computer data or programs;
- Unauthorised access to computer systems and services;
- Unauthorized reproduction of legally protected computer programs.

Similar to the Budapest Convention, the UN Manual does not cover other types of offences using computers, i.e. identity theft, money laundering or storing illegal contents. Contrary to the Budapest Convention, the UN manual does not discuss content-related crimes.

Interpol, according to its web page, divides cyber crime to attacks against computer hardware and software (botnets, malware and network intrusion); financial crimes (online fraud, penetration of online financial services and phishing); and abuse (especially of young people, in the form of grooming or “sexploitation”) [38]. “Pure cyber crime refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user. Traditional forms of crime have also evolved as criminal organizations turn increasingly to the internet to facilitate their activities and maximize their profit in the shortest time. These ‘cyber-enabled’ crimes are not necessarily new – such as theft, fraud, illegal gambling, the sale of fake medicines – but they have taken on a new online dimension” [38].

The European Commission distinguishes between cyber crime as new crimes specific to the internet, and computer-assisted crimes, or internet-facilitated crimes where computers are used as tools to commit more traditional crimes. The EU Commission has defined cyber crime as follows: “criminal acts committed using electronic communications, networks and information systems or against such networks and systems” [35].

Table 6. Proposals for classification of cyber crime by international bodies

Budapest Convention [36]	Cyber crime as a set of instances, actors and objects	- Offences against the confidentiality, integrity and availability of computer systems and data; - Computer related offences (forgery, fraud); - Content related offences; - Offences related to infringements of copyright and related rights
UN [37]	Provides common terms and frameworks	- Fraud by computer manipulation; - Computer forgery; - Damage to or modification of computer data or programs; - Unauthorised access to computer systems and services;
INTERPOL [38]	Pure cyber crime and traditional crime enabled by cyber	- attacks against computer hardware and software (botnets, malware and network intrusion); - financial crimes (online fraud, penetration of online financial services and phishing); - abuse (especially of young people, in the form of grooming or 'sexploitation')
European Commission [35]	Cyber crime and computer-assisted crime	- cyber crime (new crimes specific to internet) - computer assisted crimes, where computers are tool to conduct more traditional crimes

3 Methodology and validation

Stol et al have noted that "there is growing awareness that Software Engineering research must consider social, cultural and human aspects", and that "Grounded Theory is an increasingly popular research method in software engineering" [29]. Use of multiple methods allows the subject to be understood more deeply, and different models help to reveal different facets of reality [27]. The current research is focussed on a subject made possible by information technology – cyber crime – and not information technology itself, or the underlying causes of cyber crime. This thesis has utilised methodologies from traditionally non-cyber disciplines to explain the key steps and experiences that cyber criminals go through during the process of committing a cyber crime. This has been completed by combining crime scripting techniques from criminology, phase-based approach from military, and customer journey mapping from economics.

Cyber criminals are an unwilling population for research as they do not want to reveal their identities, income or modus operandi [19]. Therefore, most of the current work is based on secondary data sources: academic and publicly available data as well as practitioners within the law enforcement and cyber security community who have been working on the cyber crime arena.

In choosing which method would provide the best means to construct a model on cyber crime as a process, Grounded Theory Methodology [65] was selected. This methodology was deemed most suitable as no theoretical frameworks to analyse cyber crime processes was identified in literature. Grounded Theory is considered relevant when not much detail is known about a phenomena [28]. One advantage of Grounded Theory is that it is a flexible methodology, while still being structured. Grounded Theory does not focus on testing hypotheses taken from existing theoretical frameworks, but instead promotes the development of a theory of an action, process or interaction grounded in data collected [28]. A central characteristic of Grounded Theory is simultaneous data collection, analysis and writing which are considered interrelated processes [15].

Grounded Theory Methodology was used to generate high abstract categories of cyber crimes, and customer journey mapping was used to explain criminal intent and actions within a crime cycle. Grounded Theory was also used to look at the potential application of the JMAP model in answering the main research question: how to model the process of financially motivated cyber crime. This emphasises the most important point identified in interviews with policy-makers, law enforcement officers and technical cyber security experts: the need for understanding the complete cyber criminal process, and it shows the value of interdisciplinarity in modelling cyber crime. In other words, the current thesis uses social science methods and techniques to research the computer science understanding of cyber crime.

Historically, researchers have not treated cyber crime as a process in much detail, considering cyber crime as a system of interconnected "parties": criminals, victims, law enforcement, security providers, etc. [14]. While different disciplines analyse cyber crime from varying perspectives, they also use different methods. An interdisciplinary approach means applying methods from one discipline to study a problem in another discipline, or using a mixed-method approach.

3.1 Grounded Theory Methodology

The body of this thesis relies on Grounded Theory (GT), a social science methodology, to conduct research in understanding cyber crime. Grounded Theory has been used and is increasingly being used in computer science [29]. Grounded Theory is "an iterative process by which the analyst becomes more and more grounded in the data and develops increasingly rich concepts and models of how the phenomenon being analysed works" [27]. The goal of Grounded Theory is to generate theory rather than test or validate existing theory [29], it does not focus on testing hypothesis, but allows the development of a theory grounded in data [19].

Grounded Theory is a complex method, and there are many different versions of it [29]. It is acknowledged that there are three main versions of GT: classic GT developed originally by Glaser and Strauss in 1967 [28]; Straussian GT, a further development of classic GT, developed by Strauss and Corbin [15]; and constructivist GT developed by Charmaz [66]. Stol et al have summarised the main differences between the three approaches [29] as shown in Table 7:

Table 7. Three main versions of Grounded Theory (adapted from [29])

	Classic GT	Straussian GT	Constructivist GT
Research question	Researcher should start with a topic of interest, and not define research question in advance – this would "force" the research. Such approach should make the research more relevant.	Could be defined in advance, emerge from literature, or suggested by someone. Research question is often open-ended and broad.	Start with initial research question, and specific research question will emerge during study.
Role of literature	A literature review should not be conducted until after the theory is already developing, in order to avoid influence of existing theories on the one being worked on. Considers that before RQ definition it is not clear what literature is to be reviewed.	Literature may be reviewed all through process, as concepts from literature may be used if applicable; to enhance theoretical sensitivity, as a secondary data source; to formulate questions for data collection or stimulate questions during analysis; to suggest areas for theoretical sampling.	Supports delayed literature review, highlights the need to tailor literature review to fit the purpose of the GT study.
Questions asked during analysis	- what is this data the study of?	Asking questions about whom, when, where, how, with what	- what is this data a study of?

	- what category or what property of what category does this incident indicate? - what is actually happening in the data?	consequences, and under what conditions phenomena occur, helps to discover important ideas for theory. "Free-wheeling flights of imagination".	- what do the data suggest? Pronounce? Leave unsaid? - from whose point of view? - what theoretical category does this specific datum indicate?
Philosophical influences	**Objectivism**: there exists a single, correct description of reality; the researcher therefore *discovers* grounded theory from data.	**Pragmatism** and **symbolic interactionism**: actors engage in a world that requires reflexive interaction; reality is *constructed* through interaction and relies on language and communication.	**Social constructionism**: social reality is *constructed* by our individual and collective action. GT emerges from "shared experiences and relationships with participants"; observers are not neutral.

3.2 Use of Grounded Theory in the current thesis

In their original work "The discovery of Grounded Theory" Glaser and Strauss emphasise the need to use Grounded Theory (GT) flexibly [28]. Although this thesis has adopted Straussian GT, following the techniques and procedures set up in the 4th edition of Corbin and Strauss [15], it incorporates elements from both classic and constructivist GTs.

The research started in 2015 within the framework of EU FP-7 E-CRIME project [67], and was taken further between 2016 and 2020 during the course of PhD studies. The E-CRIME project proposed cyber criminal "journey maps", depicting the workings of cyber crimes. Since the topic of journey mapping drew substantial interest from law enforcement and academia, the author decided to take this research further. The initial research question for PhD work was "Methodology for using journey mapping to support cyber crime forensic investigation and countermeasure development". Following the principles of constructivist GT a more specific research question emerged during the course of research. The original topic was too wide in including forensic investigation and countermeasure development. Data collection, interviews and literature review pointed to a need to focus on the modelling of financially motivated cyber crime as a process, before proceeding to applying it to investigation and countermeasure development.

In GT, the "analysis begins as soon as first bits of data are collected" – this is necessary because the initial analysis is used to direct the next steps in data collection and interviews [65] and theory will be actively obtained from data [15]. The data used in this thesis has been collected selectively to develop a JMAP model of financially motivated cyber crime as a process, that would be relevant and practical to law enforcement, but also to those developing policy guidelines or fighting against financially motivated cyber crime.

The analysis of initial data collection was discussed in **Publication I**. Data collection was conducted by means of a literature review of published approaches to cyber crime and modelling of cyber crime, as well as conducting expert interviews with cyber security experts and LEA representatives, and analysing publicly available data on cyber crime. Sources of information included journals and conference proceedings in the fields of law, cyber security, criminology, and information security, reports published by think-tanks and law enforcement agencies, scholarly textbooks and various internet sources.

Grounded Theory research focuses on unstructured texts – interview transcripts, documents and field notes, but may also include structured data [29]. This thesis relies on qualitative data sources – interviews, observations and documents. Data sources used included open source information about cyber crimes (both specific accounts and general information), academic literature, news media, cyber security related blogs, public documents, legislation, analysis by international organisations, and non-fiction books.

Semi-structured interviews were used as the means of data collection due to one main consideration. The semi-structured interview method follows a framework but is open, allowing new ideas to be brought up during the interview as a result of how the interviewee has responded [68]. An interview guide was prepared, which provided an informal grouping of topics to be covered during the interview. This interview method allowed for the tailoring of questions to each specific interview situation and to each person individually, according to their expertise. This was mainly due to the fact that so little is known about the process of cyber crime, or how a crime takes place from its initial preparatory stages through to exiting the crime cycle, and people with different background or area of expertise have different focus on any one part of the crime. The interviews included questions on the expertise of the interviewees and on current best practices used investigating and understanding cyber crime. Based on the expertise of interviewees, the questions also included the modus operandi of cyber criminals, analysis or overview of cyber crime cases, information obtained from convicted criminals, the cyber crime ecosystem and cyber criminal business models. The interviews resulted in more thorough data collection and the identification of interesting nuances.

Following the principles of GT research, a research journal was kept, including all secondary public sources consulted, and interview notes. After data collection, a Criminal JMAP model for financially motivated cyber crime was developed, and this model was validated after each stage. The process of data collection, updating the model and validating the model was reiterated after each validation event.

The work on this thesis and on modelling financially motivated cyber crime as a process can be divided into two distinct stages:

I. Initial work during the EU FP-7 E-CRIME project, 2015 [67], Figure 3:
   a. Collect data on cyber crime (2015),
   b. Generalise to 8 types (categories) of cyber crimes (2015),
   c. Generate preliminary model (2015-2016),
   d. Validate model on cyber range (UK, 2016).

II. Further development during PhD research (2015-2020):
   a. Collect additional data on cyber crime,
   b. Update model,
   c. Feedback on updated model during validation events and interviews,
   d. Update model based on feedback from validation.

The development of Criminal JMAP model of financially motivated cyber crime followed logically from the results of the E-CRIME project [67]. At the start of the PhD programme of study, the preliminary model was investigated, and further data on cyber crimes and crime analysis was collected. The model was initially validated at a European LEA Workshop in 2017, then updated based on the feedback received at the validation workshop. Building on these results during the following four years of research, the model was further amended and validated in Estonia, the UK and Germany. These three countries were chosen due to both their similarities (high use of digital services) and differences (different in size, administrative systems and law enforcement systems).

After each iteration and update to the model, it was validated, with comments and feedback received from the validation events included. After each validation workshop, a survey was submitted to participants. In total, six validation events were conducted with LEA representatives and academics. Additionally, two focus group discussions with European LEA representatives were held. The PhD research took place according to Grounded Theory principles in a continuous cycle over five years, as depicted in Figure 2.

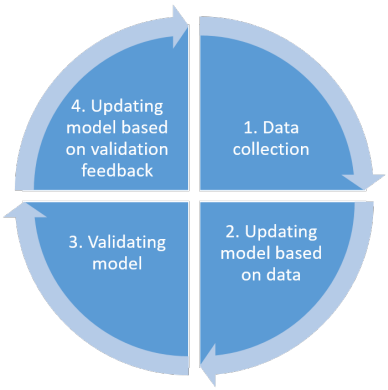

Figure 2. Use of GT as continuous cycle during research

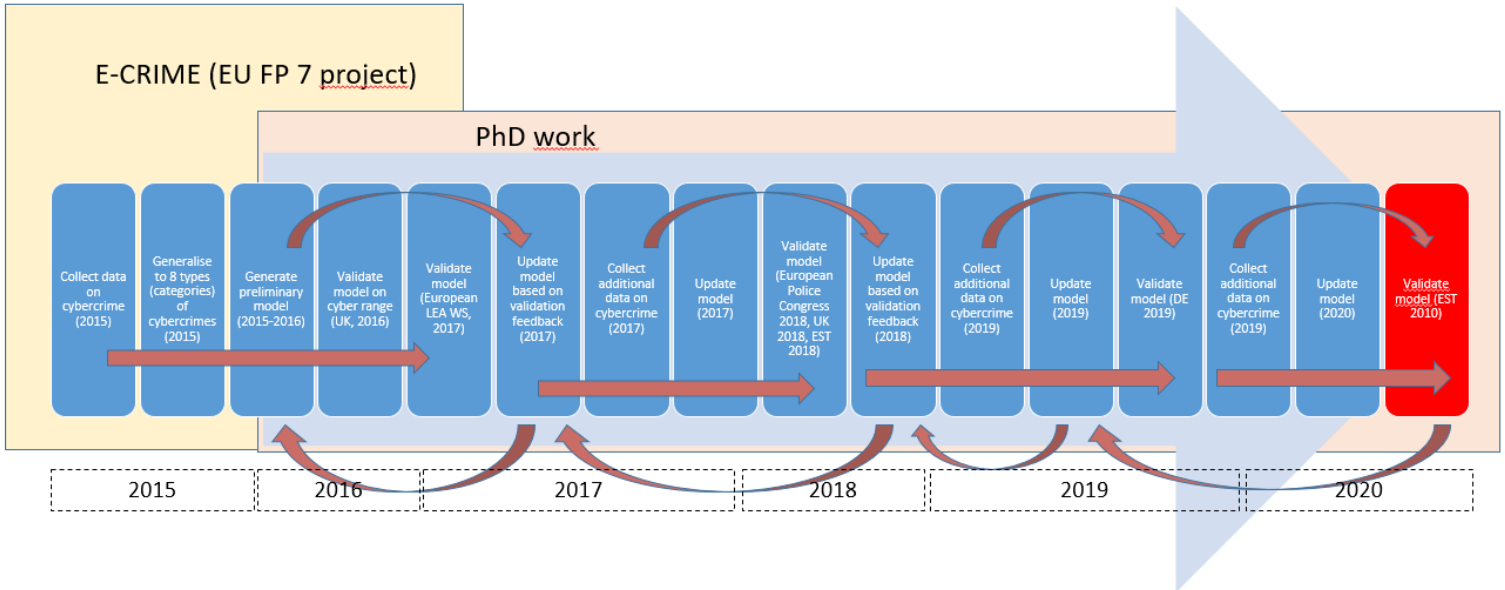

Figure 3. Overall process of work

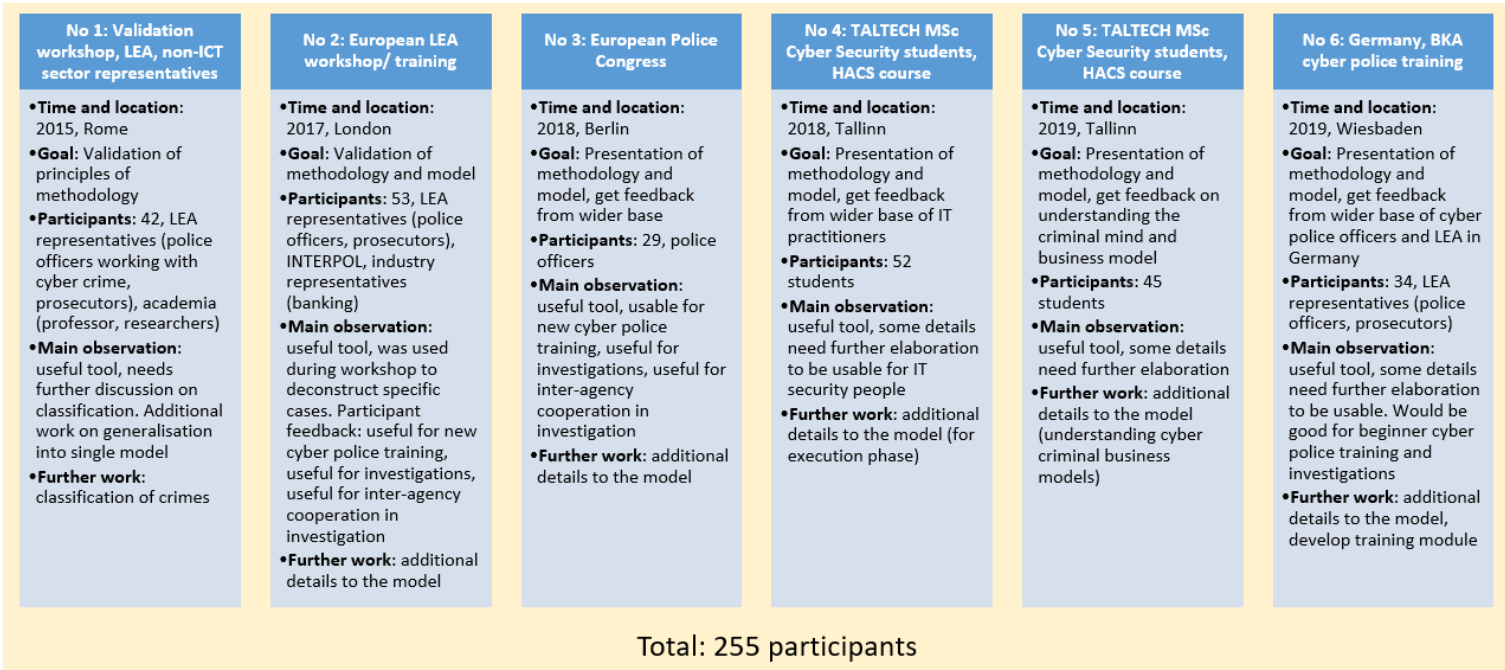

Figure 4. Validation workshops and training events

3.3 Validation

As suggested in **Publication V**, validation via expert assessment to the methodology and JMAP model was sought in two ways: focus group interviews and validation events (workshops and trainings). Eligibility criteria required that individuals work in law enforcement or academia and be knowledgeable about cyber crime. Validation of the methodology and expert feedback was sought during several training events and focus groups – national and international – in Estonia, Germany and the UK. These three countries were chosen due to both their similarities and differences. The three countries are different in size, administrative systems and law enforcement systems, yet similar in their adoption of the use of ICT. An additional step in validation was undertaken with Cyber Security MSc level students at TALTECH during the Human Aspects in Cyber Security course. The aim of conducting this additional step was to gain understanding whether the developed model could be used in training for persons unfamiliar with investigating cyber crimes. To increase the reliability of the methodology and JMAP model according to principles of Grounded Theory Methodology, the following steps were undertaken:

1) Validation workshops/ pilot group trainings to confirm the developed JMAP model was applicable for its stated purposes. The process was repeated between 2015-2020. Pilot group trainings offered an opportunity to make useful observations, which were followed by Focus Group interviews with a select number of participants in the training;
2) A post event survey after each training event was conducted to determine the practical usability of the methodology and model for LEA activities. The survey used is attached in Annex 1.
3) Focus group discussions and interviews with academics and practitioners on the usability and applicability of the methodology and model. An interview guide (attached in Annex 2) was prepared, which provided an informal grouping of topics to be covered during the interview. The interview guide was used for both Focus Group discussions and separate interviews. Once completed, the results provided additional data and some interesting nuances.
4) Analysis of validation feedback, in order to determine the usability of the proposed methodology and JMAP model. The aim of the validation was to reach a common conclusion, and not to research single activities at micro levels. Different organisations and individuals each had specific expertise and points of view on the topic, and provided valuable insight in terms of validating the methodology and model of financially motivated cyber crime.

The main challenge in validation was to get feedback from a wide range of people, in terms of their background, expertise and country of origin. The aim was that validation should, if possible, be conducted in all three participating countries and at an international scale to make sure that the language used would be understood in the same way, as the way people think is affected by their native language [27]. Therefore, in designing survey and interview, opinions on understanding the questions was sought from representatives of Estonian, UK and German LEA, as well as academics from UK and Estonia. The validity and reliability of the data was supported by overall coherence of the answers. The results were compiled into a database and analysed using Microsoft Business Intelligence (BI) data analytics software. The process of data analysis is further explained in 3.3.1, 3.3.2, and 3.3.3.

3.3.1 Pilot group training

The pilot group training was based on the journey mapping methodology and JMAP model as developed in earlier stages of research. The main principles used in the training program was used for all pilot groups although differed somewhat in their details. Following the principles of Grounded Theory Methodology, the differences in every subsequent training event were mostly due to:

- Specific focus group's background and expertise,
- Feedback from previous rounds of workshops and training, which were included in the updated model.

The main goal of the training was to confirm that that the developed JMAP model is applicable to the stated purposes, is usable for practitioners and corresponds with real life requirements. The LEA and police oriented events looked in more detail at the potential use of the tool for investigating cyber crimes, as well as the potential to use the model for developing prevention and countermeasures. In addition, the model was used in teaching TALTECH MSc students (Human Aspects of Cyber Security course). The student focus group aimed to identify if those not familiar with cyber crime could benefit from using the model, with the aim to develop training programmes to explain cyber criminal processes. An overview of the training events and main feedback is presented in Figure 4.

All training events were followed by a post-event survey, presented in the following Section (Section 3.3.2).

3.3.2 Post event survey

The pilot group training and validation workshops, as explained in Section 5.3.1 were followed by post-event survey (quantitative methods), presented in Annex 1. 255 people participated in training and 231 survey responses were received. The main goal was to get objective and quantifiable confirmation that the developed JMAP model was applicable for its intended purposes. The survey was taken at the end of classroom training within a limited timeframe. Therefore it was designed not be too extensive, with the aim that it should not take more than 10 minutes to complete. The survey consisted of multiple-choice questions in the beginning and open-ended questions in the end. The survey started with an oral introduction, stating that the survey will be anonymous and the results from survey will only be used in further development of the cyber criminal JMAP model.

In designing the survey, the main challenge was to ensure that answers would be precise and relevant [27]. According to the literature [69] [27] [70], it was also important not to ask leading questions, not to use a negative form, be mindful of the order of questions and be careful in the use of language. In order to mitigate these risks, a number of persons from the three countries (UK, Germany, Estonia) were asked to assess the survey, to make sure they understood the questions and the purpose they were designed for.

The survey results were analysed using Microsoft Excel software. Quantitative data from the survey was coded and analysed using Microsoft Excel Countif formulas. Qualitative data was analysed using a thematic approach suggested by Braun and Clark [71], followed by analysis using coding. In the thematic analysis the following steps were used: generating codes, generating themes, reviewing and refining. The qualitative answers were translated into overarching themes for two questions: missing points (gaps) in the model, and proposals for improvement of the model (Table 8). The aim of creating such overarching themes was to keep the results within a framework and not broaden the focus of the study into a wide array of directions. In order to improve the

overall results of validation, the survey feedback was used to guide focus group discussions and interviews to gain a deeper understanding and opinion of those participating in the latter.

Table 8: Themes used in thematic analysis of survey results

Question	Theme
Other uses for the model	Forensics Standard procedures Common understanding between stakeholders Awareness building Public policy Cooperation Prosecution Countermeasures Legal
Missing points in model	Decision points of criminals Engagement of LEA with developing the model Include motivation aspect Social engineering Forensics
Proposals for improvement	Develop investigation checklist Creation of online platform Intelligence and information sharing Forensics Engagement of LEA with developing the model Add decision points of criminals Use data analytics Add social engineering

In the survey, the respondents were asked to indicate the usefulness of the JMAP model for their work; make suggestions for important aspects missing in the model; make proposals for improvement and provide other comments. 168 respondents found the JMAP model to be useful in their work, 35 stated it would not be useful for their work and 28 were not sure about this (Figure 5). Further analysis of those who didn't find it useful for their work or were unsure about this, revealed that they either did not work daily in this field (37) or had general concerns about using such modelling in practical work (11). Although not specifically asked, a few respondents commented on their concern of using modelling in practical work: "crimes might be tried to fit to model or vice versa", or "what happens if the model changes and crimes don't, or if crimes change and the model doesn't". Still, the people who didn't find the model to be useful for their own work, found that the model could be used for training purposes.

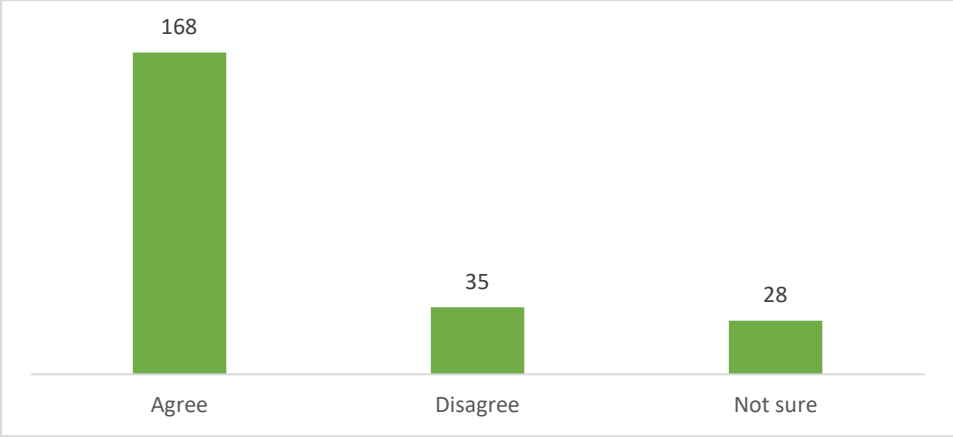

Figure 5: Post-event survey: Do you think this kind of modelling will be useful for your work?

In the follow-on question, the respondents were asked in which areas the model could be useful: training, investigation, prevention, or anything else (Figure 6). Using the JMAP model for training purposes was deemed useful by a biggest number of respondents, 213 persons. Using the model for investigation was considered useful by 110 respondents, and for prevention efforts by 76 respondents. 42 respondents answered “other areas”, and specified. The answers of “other” uses were analysed using coding and thematic analysis (as shown in Table 8). Most frequent proposals included the use of model for forensics, for developing standard procedures or for bettering common understanding in the cyber crime investigation processes. The more surprising proposals for additional uses of the model were using it for improving public policies in the fight against cyber crime, better cooperation among those fighting cyber crime, and using model in prosecution. One respondent commented, that a “common understanding would make it easier to create joint investigation teams”, both nationally and internationally. Better international cooperation in investigations was also mentioned as one potential future use of the model.

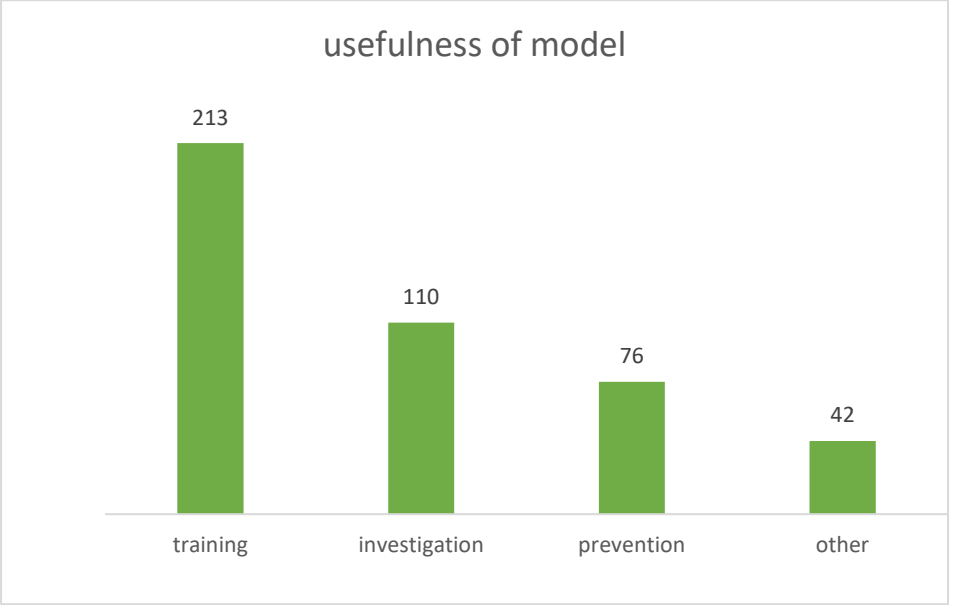

Figure 6: Post-event survey: in which areas could the model be useful?

In response to the question, if there were gaps (any important points missing) from the JMAP model, most proposals related to including criminal decision points in the model, and including LEA in developing the model (Figure 7). All answers were analysed using a thematic analysis (as shown in Table 8). The first of those comments – to include criminal decision points – was taken on board and included in final version of the model. Inclusion of LEA with the aim of provision of data about concrete cases of cyber crimes was not entirely possible due to sensitivity and classification issues. However, the focus group discussions and interviews provided additional information on cyber crimes that have taken place. Such information was anonymised and generalised into the model as elements of the different phases of a crime, as presented in Figure 25, Figure 27, and Figure 29. An overview of answers related to gaps in the model is presented in Figure 7.

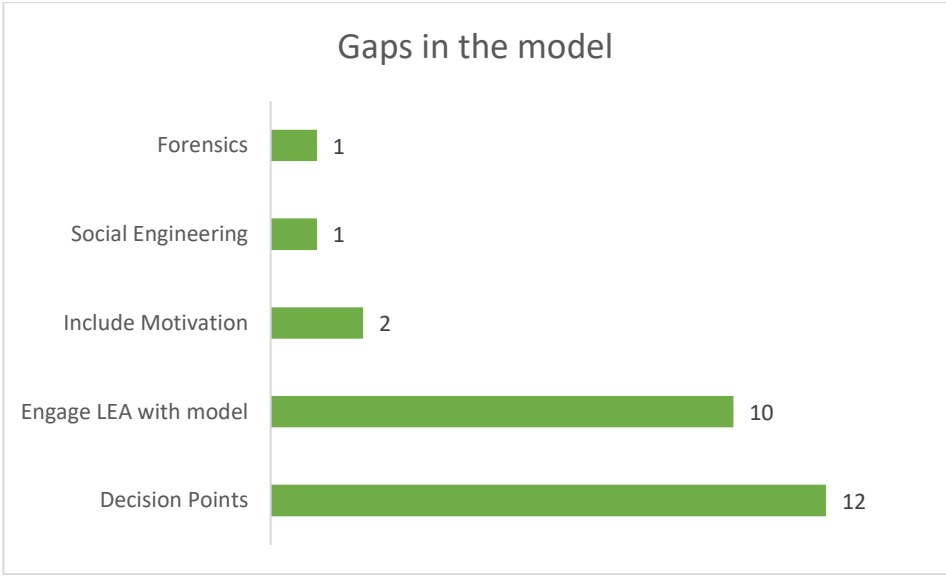

Figure 7: Post-event survey: gaps in the model

A number of proposals was also made for improving the JMAP model, all of which were analysed using a thematic analysis (as shown in Table 8) and results are presented on Figure 8. Two interesting suggestions made by biggest number of those who answered this question was a proposal to create an online platform to exchange analyses of crimes, and development of an investigation checklist, according to the JMAP model. Further interviews revealed that the model could be used for data exchange without breaking regulations covering sensitivity of information, at least at a national level. The rationale behind these proposals was that it would assist both national and international investigations involving various parties, in order to find tendencies or trends and improving prevention possibilities. For example, there were comments such as: "develop checklist for investigation based on model"; "create online platform to exchange information amongst all cybercrime police"; "establishing a closed user group in internal networks"; "online quick cooperation in Europe". For intelligence and information sharing it appeared there are many issues around exchange of sensitive or classified data and information, both nationally and internationally, and many respondents thought that the model "can be used for sharing sensitive info, both national and international".

Some respondents emphasised the need to develop a better understanding of the preparation stage of the crimes, as most of the time investigators currently focus on the execution stage. One respondent posed a question "Can additional aspects be included in the model: legislative aspects, data analytics, etc.?"; another respondent asked whether and "how specific technical or non-technical aspects can be included in the model?"; yet another stated that in using model for training "emphasize the importance of gaining information for the initial preparation step. The normal starting point for law enforcement is somewhere in the post-execution phase". There was also one proposal to include other (alternative) data sources (e.g. social media) and a few which were about using big data and data analytics in line with the model, in order to analyse trends with cyber crime. One respondent commented, that while flexibility of the model is very useful, there might be cases when it would be counterproductive. A few responses were

about explaining cyber crime to those not knowledgeable about it ("model can be used to explain cyber crime to politicians", "could be useful to train prosecutors to develop better understanding of cyber crime whole process"). Interestingly, no comments were made with relation to the exit and monetization phase. This is probably due to the fact that it generally falls under the financial crimes category and is treated separately from cyber crime investigations.

To conclude, the surveys indicated that the model can be useful for LEA. Many proposals and concerns with the model centred around practical uses, which is a clear indication that LEA representatives who used the model in trainings found that there might be usable application of the model in areas specified.

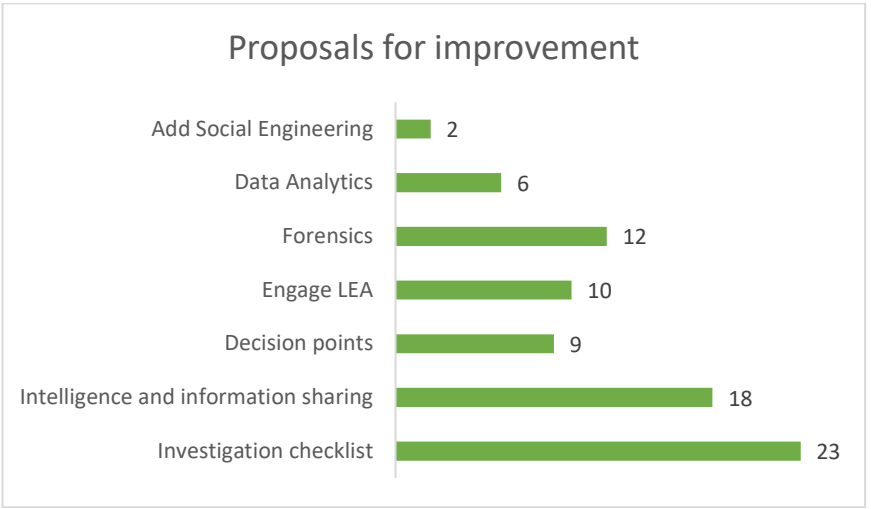

Figure 8: Post-event survey: proposals for improving the model

Some participants expressed concerns regarding the JMAP model. These comments were centred on the sensitivity issues in investigating cyber crime. Even though respondents felt it useful to exchange data between all stakeholders in the cyber crime investigation process (nationally and internationally), there was a concern about exchanging sensitive or classified data and information. For example, there were comments such as "how to share sensitive information based on the model", "how to identify, at which points and on what details should intelligence be shared?", "European information exchange will be problematic". Another interesting concern expressed was related to the JMAP model itself: what happens if the model changes, or the crimes change and model doesn't ("there might be a problem of fitting crimes to the model when not appropriate", "what happens if the model changes? Problem: applying quick updates to the models to cover new situations"). This concern was addressed in later work, by making the model more generic, and providing options to go into more detail when analysing specific crimes.

3.3.3 Interviews and Focus Group discussions

The qualitative aspects of the JMAP model were assessed by conducting focus group discussions and interviews in the three countries and different organisation types: LEA, investigators, prosecutors and academics. Semi-structured interviews were chosen as the method of choice because these allowed for establishing the main goals of the interview

and fix core questions, but still gave freedom to ask additional follow-up questions [27]. In the case of structured interviews the wording and order of questions was exactly the same for each respondent so that any differences in answers were due to differences among respondents rather than in the questions asked. In contrast, the semi-structured interview method followed a framework but was open, allowing new ideas to be raised during the interview as a result of how the interviewee has responded [68]. An interview guide was prepared (Annex 2) that provided an informal grouping of topics to be covered during the interview. The semi-structured interview method allowed for the tailoring of questions to each specific interview situation and to each person individually.

Throughout this research work, 134 persons participated in focus group discussions, and 21 separate interviews were conducted. Only notes were taken during both the semi-structured interviews and focus group discussions. Notes were inserted into a table, coded, and the results analysed using a thematic approach suggested by [71]. The qualitative answers were coded and translated into overarching themes (as shown in Table 8) and subsequently analysed. The aim of creating such overarching themes was to keep the results within a framework and not broaden the focus of the study into a wide array of directions. In order to improve the overall results of validation, the survey feedback was used to guide focus group discussions and interviews to gain a deeper understanding and opinion of those participating in the latter.

The focus group discussions and interviews lasted for about an hour each. The questions formulated followed the same logic as the one used for survey, in order to later analyse the answers along the same principles. The focus was on law enforcement operating at regional and national levels, industry based cyber security experts as well as experts from academia (Figure 9).

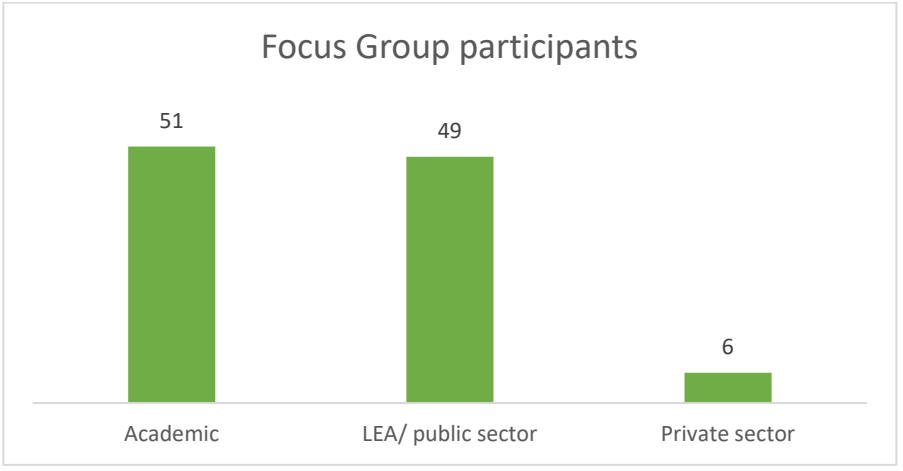

Figure 9: Focus Group and interview participants

The interview results were anonymised foremost for ethical reasons, in order not to reveal the identity of those working in cyber crime. Researchers and journalists writing about cyber crime have been threatened by cyber criminals, and in some cases cyber criminals have used psychological or even physical violence against police officers or journalists investigating cyber crimes [19]. The focus of these interviews was on the requirements and needs of both individuals and organizations, concentrating on the

experiences of interviewees. The interviews were concluded by discussing the potential application of the developed model.

The interviews resulted in a more thorough data collection and the identification of interesting nuances. Academics, law enforcement and cyber security specialists all had their unique views on real cyber crimes and/ or incidents, which provided useful input into the design of the model. The resulting analysis is provided below in Table 9. In addition to the interviews below, academics working on cyber security in TALTECH (Estonia) and Warwick University (UK) were consulted throughout the five years of research.

Table 9. Semi-structured Interview results

Method	Target group	Timeline	Main findings
Semi-structured interview	Cyber security professionals and academics (11 participants)	September-December 2015	Information on specific aspects of attacks, reconnaissance on victims, technical details on conduct of attacks
Semi-structured interviews	Academics and practitioners at ECCWS 2016 (20 participants)	July 2016	Round-table discussion on modelling cyber crimes as part of ECCWS 2016 conference. Information on specific aspects of initial stages of the crime, and execution of the crime
Focus Group	Focus Group discussion at LEA workshop, based on their knowledge of LEA actions in investigating cyber crime (9 participants)	March 2017	Group and individual interviews with prosecutors, police officers and academia on the overall process of crime. Each participant provided important input from their professional background into consideration of building the model (practical, legal, investigation, prosecution).
Semi-structured interview	Interviews with Estonian LEA (3 participants)	May 2017	Useful input in terms of using model to explain cyber crime to leadership and policy levels, as well as international cooperation in investigation.
Semi-structured interview	Academics and practitioners at ICCWS 2018 (19 participants)	February 2018	Useful input in using model for modelling cyber attacks other than crime (trolling, warfare, etc.)
Semi-structured interview	Interviews in UK with academia and LEA (police officers) (8 participants)	July 2018	Useful input to the potential applicability beyond what was foreseen (i.e. awareness-building, policy options, countermeasures in addition to training). Potential use of model in investigation, national and international cooperation as well as training.
Semi-structured interview	Interviews with a select number of participants at European Police Congress (5 participants)	February 2018	Useful input to validity, additional input to exit and monetization phases of crime. Additional contacts with researchers to research monetization aspects. Useful input in developing training module.

Semi-structured interview	Academics and practitioners at ICCWS 2019 (15 participants)	February 2019	Useful input in workings and threat of cyber crime in a non-transatlantic region (i.e. Africa), additional information on preparation phases of cyber crime. Potential use of model to training discussed, input received.
Semi-structured interview	Academics and practitioners at ECCWS 2019 (11 participants)	July 2019	Useful input to various taxonomies and general understanding of cyber crime processes.
Focus Group	Focus Group discussion with German LEA representatives attending BKA cyber police training (34 participants)	October 2019	Useful input on potential for practical use of model in police work. Potential for investigation, checklists, trainings were proposed.

3.3.4 Data analysis

In order to determine the usability of the JMAP model at both individual and organization levels, feedback and data from 3.3.1, 3.3.2, and 3.3.3 were analysed according to the principles of GT methodology. This stage also drew conclusions on the entire validation process and outcomes.

The inputs and feedback as explained in sections 3.3.1, 3.3.2, and 3.3.3 were all included in the model of financially motivated cyber crime as foreseen in the Grounded Theory Methodology. Although extensive research has been carried out on various components of cyber crime, most notably technical aspects, there have been very few studies on the mechanisms of cyber crime. One of the advantages of using GT methodology is that work can start even with incomplete data: for this dissertation work started with collecting inputs from cyber security professionals, LEA representatives and academia. There are certain problems with the use of these focus groups, as all of them have a subjective outside view on cyber crime. However, secondary data sources were also relied upon as cyber criminals are not willing to reveal their modus operandi and business models. It is clear that people with different background or area of expertise have a specific focus on a part of crime, which made the integrated approach relevant to all stakeholders, as post-event surveys showed. The integrated approach and resultant inclusion in the JMAP model resulted in more thorough data collection and the identification of interesting nuances. In addition to the research and investigation of data on cyber crimes, interviews were held with researchers and former LEA officers who have been active in studying the mechanics of cyber crime. Validation of the JMAP model was conducted after several rounds of data collection and feedback inclusion, resulting in a generic model for financially motivated cyber crime. Since cyber criminals are innovative and agile, changing their modus operandi very quickly, such exercise should be re-taken on a regular basis to ensure the model remains relevant and updated. Further data collection is required to determine exactly how changes in cyber security environment affect not only tactics, techniques and procedures of cyber criminals, but also their business models.

3.4 Use of journey mapping for training

The result of this thesis – a criminal JMAP model developed to model financially motivated cyber crimes has been applied to several training events over the past five years. For the purposes of training, a "Training Manual" has also been prepared and used in conducting such training events. The JMAP model was used at training events for LEA representatives; and also for MSc Cyber Security students at TALTECH for the Human Aspects in Cyber Security course in 2018, 2019, 2020 and 2021 to improve the understanding of cyber crime among students not familiar with the subject. Drawing on the feedback from training events, the JMAP model can be successfully used for training both new and experienced LEA officers, but also for improving cooperation in investigation among different law enforcement agencies both nationally and internationally.

4 Defining financially motivated cyber crime and choosing taxonomy

Maintaining an awareness of cyber crime as a big and growing problem worldwide is a significant issue as cybercriminal revenues are increasing constantly [30] [72] [39] [10]. Nobody disputes the need to protect cyberspace from criminal activities, yet our understanding of cyber crime, its consequences (social, organisational, economic) and the range of best methods to address its spread and manage its impact is still limited.

The literature and study of cyber crime is vast, but thus far there is no universally accepted definition [30]. Definitions mostly depend on the purpose of using the term [72]. There is also no consensus on classification, economic implications, security standards and solutions.

Section 4.1 below will answer research question 1.2. "How do our understanding shape or affect the way financially motivated cyber crime is being analysed and approached" and will propose a definition to be used in this thesis. Section 4.2 below will answer research question 2.2. "How appropriate are existing taxonomies for classifying financially motivated cyber crime?" and will provide a taxonomy to model financially motivated cyber crime.

Crimes are a legal construct, and they exist when they are identified as such in legislation [34]. The legislation that defines crimes is national. At the same time, cyber crime is an international phenomenon, making its study all the more complex. Academic literature, as well as public and private bodies, have studied the subject from legal, technical, psychological, and criminological aspects This chapter is based on **Publication IV** and proposes both a definition and taxonomy to use in understanding the processes and modelling of financially motivated cyber crime.

4.1 Proposed definition

In majority of current approaches, cyber crime is referred to as "pure" or "cyber-dependent" crimes, i.e. such crimes, that would not happen without the use of ICTs [34] [39] [54] [59] [61] [36] [37] [38] [35]. The aim of mapping cyber criminal processes is to understand how a crime takes place from the criminal's point of view. Important players/actors and aspects in this process are the criminal, their motivations, the victim, impacts on victims, attack vectors and methods, criminal gain, and exit from crime. Schematically this can be represented as provided on Figure 10.

Figure 10. Actors and aspects in a cyber criminal cycle/ journey

Deriving an overarching definition for cyber crime is not easy. As stated in Sections 2.1, 2.2 and above in this chapter, there are a number of different perspectives, that should be considered in proposing such a definition. Any definition which attempts to be all-encompassing would be either too limited or too complex to be helpful. However, for the purposes of mapping financially motivated cyber criminal processes, **Publication IV** and this thesis have offered such a definition. The aim is that this should be applicable and embody a multitude of concepts for those crimes that would not happen without the use of ICTs. A usable overarching definition for the purposes of modelling financially-motivated cyber crime is needed that would be both general and flexible.

A new definition is therefore proposed, drawing on the literature review conducted in Section 2.1. This definition does not differentiate criminals, motivations, victims, purposes, tools or attack vectors. It does not make distinction as to the difficulties of drawing a line between cyber crimes and other crimes and takes into account the continuum of cyber crime. The closest definition for current purposes can be found in [73]: proposing that cyber crime is "Crime committed over the internet". The definition proposed in this dissertation follows from [73] and is explanatory, flexible, should be durable over time and usable in any legal framework:

> "Financially motivated cyber crime is an activity that involves the use of information technology for criminal purposes at any stage of the process, with the aim of generating monetary profit for the criminal".

It is acknowledged that the proposed definition may be too broad and too overarching. For the benefit of doubt, any follow-on work on modelling specific cyber crime instances should provide their own definition, depending on which aspect of cyber crime is being dealt with.

4.2 Proposed taxonomy for mapping cyber criminal journeys

Different methods exist for developing a taxonomy. As presented in [33], "most approaches vary in terms of formality, rigour and evaluation". Building a taxonomy can use inductive or deductive approach, which is usually dependent on the academic discipline it is used in. Social sciences mostly use an inductive or conceptual approach (typology), biological science uses deductive or empirical approach (taxonomy) [33].

The main difficulty in creating a taxonomy of cyber crime is the definition of crime. Offences are crimes when they are identified as such in legislation, which is done in specific national contexts. Cyber crime is an international phenomenon, and this makes its study even more difficult and creates additional problems of terminology and taxonomy. For this reason, the author uses definition as proposed in Section 4.1 and published in **Publication IV**.

A robust taxonomy is an essential starting point [63]. The need for a taxonomy to respond to cyber crime is a practical measure as without an understanding of cyber crime, any meaningful investigative or responsive measures cannot be developed [63]. Any taxonomy created for the purposes of understanding cyber crime cannot be a static, complete, or very specific document. This is due to the connected digital world that we live in, the ever-evolving nature of cyber crime and cyber criminal ecosystem, as well as the varied legal frameworks.

The principal objective in conducting modelling of financially motivated cyber crime, or cyber crime in general, is to understand how a cyber crime takes place. Therefore **Publication IV** proposed an appropriately generic taxonomy that can be further sub-divided as the processes, actors, tactics, techniques and systems change. After researching various crime types, the cyber criminal ecosystem, victimology and cyber criminal business models, a four-dimensional taxonomy of cyber crime is proposed:

- Perpetrator, including their motivation and aim, business models, ecosystem and preparation to conduct the crime and enablers of crime;
- Attack vector, including enabling capabilities to conduct the crime;
- Victim, including the impact of crime on victim;
- Exit, including monetization of crime.

The basis for the proposed taxonomy is the underlying crime participant actors and factors, as depicted on Figure 11. This classification covers all aspects within a cyber crime process. In case one actor or factor is missing, the crime cannot, in principle, take place. This will be useful in the fight against cyber crime, in providing an overview of crime actors and factors. In a general sense, it will provide opportunities for major facilitating aspects of where to concentrate awareness campaigns, countermeasure development or investigative actions.

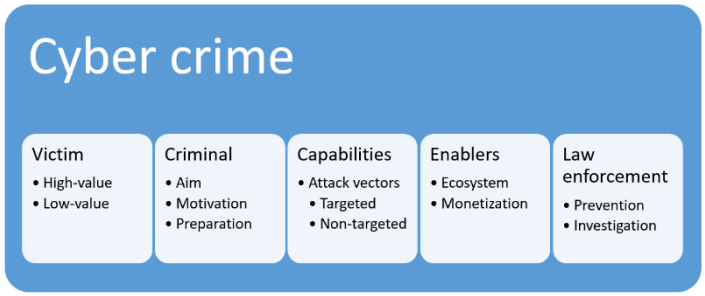

Figure 11: Cyber crime participant factors

The above classification covers all aspects in a crime and for the purposes of modelling a cyber criminal journey can be further developed and presented as depicted in Figure 12 and explained below. Discussion on this classification is also presented in **Publication I** (with a focus on cyber crime) and **Publication II** (explaining the classification of **Publication I** in more detail, and adding aspects of cyber warfare to the equation). **Publication IV** has taken this classification further and proposed a four-dimensional taxonomy as presented in Figure 12.

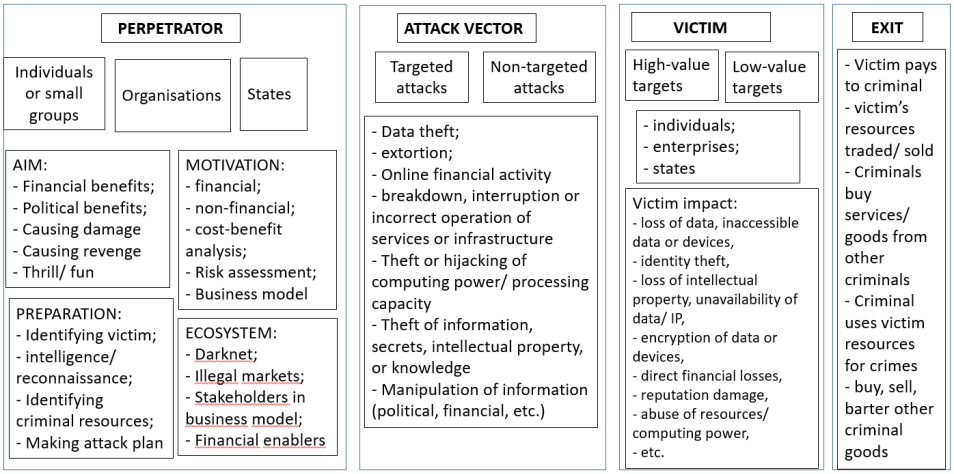

*Figure 12. Four-dimensional taxonomy proposed for cyber criminal journey mapping, as presented in **Publication IV**.*

Based on the proposed classification and taxonomy above in Figure 11 and Figure 12, a general overview of financially motivated cyber crime can be presented. In the case of financially motivated cyber crime, we can remove motivation from the equation, as motivation is singular: financial gain. This dissertation will not delve into discussions of criminal intent and motivation. However, several authors have proposed that the underlying processes of conducting cyber crimes or warfare, regardless of intent, is similar (e.g. [62], [74]). The perpetrators or criminals will conduct actions in preparation of committing a crime and certain enablers play an important part during preparation. The attack vectors will be developed (or outsourced/ bought) according to the needs of specific attacks and criminals need to take certain actions to execute the crime. In this stage, a number of enablers play an important role, and a major enabler is the victim –

either from their social or technical aspects. Without victims there would be no crime to commit and no financial gain to be achieved. From the criminals' point of view, victims should take (or neglect to take) certain actions, and a number of steps can be taken to assure targets will be attacked successfully. The criminals may conduct either targeted or non-targeted attacks, which will influence their choice of capabilities, including attack vectors. The process ends with an exit phase, where the actual financial gain is achieved. The whole process feeds into financial gain for the criminal, and he must take some actions to ensure that. It must be said that the whole cyber crime process is not simple and linear; rather there is a feedback loop during the whole event. The criminal may find a new opportunity or impediment along the way and revert to previous phases, or move on to another crime within the same overall process, if the opportunity presents itself. Figure 12 presents a depiction of financially motivated cyber crime taxonomy as used in this research and the following sections provide an overview of each dimension of the taxonomy.

It is acknowledged that states, in addition to criminals and criminal organisations, could also use cyber crime methods (or outsource/ finance such crimes) for financial gain, or for political (or any other) purposes. For example, **Publication III** analysed the application of the proposed methodology to the phenomenon of state-sponsored trolling, and such exercise could be undertaken for any other criminal state-sponsored act. Such acts require special attention as these would target very high-value victims. They would tend to be conducted with high levels of expertise and have guaranteed (state-sponsored) use of adequate resources. State-sponsored attacks in general tend to be very specifically targeted and tailored, and even in case such attacks would be financially motivated, they fall out of scope of the current dissertation. Adapted four-dimensional taxonomy is presented in Figure 13, based on the following constraints:

- the "perpetrator" has been narrowed to include individuals and (criminal) organisations only, leaving out states;
- The "aim" and "motivation" has been narrowed to include financial gains only.

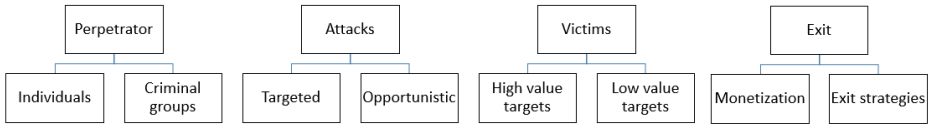

*Figure 13. Adapted four-dimensional taxonomy for modelling financially motivated cyber crime (adapted from **Publication IV**).*

4.2.1 Perpetrator

For the purposes of modelling financially motivated cyber crime, it will not be useful to classify perpetrators into a number of different categories (hackers, script kiddies, insiders, coders, black hat hackers, etc.) [44] [45] [50] [52] [53] as provided in the review of existing taxonomies presented in Section 2.2. For the purposes of modelling, we are not focused on the type of criminal, rather the interest lies in the organisation of the criminal(s): is it a lone offender, or an organised group. Furthermore, as stated in [74] [34] and [26], and since this dissertation does not discuss the motivation (intent) for conducting crimes and focusses on financially motivated cyber crime – the modus operandi for any cyber crime is similar, regardless of the end-motivation.

It has been noted, that cyber crime has changed from being a low volume crime performed by individuals to being high volume crime, which is highly organised and industry-like [72]. Published evidence on cyber crime is based on a small number of case studies or interviews, and mostly focus on the methods of the crime [59]. As stated in **Publication I**, research from fifteen or more years ago suggested that the cyber criminal world was not highly organised. However research published within the last few years suggests otherwise, with more than 80% of cyber crimes being organised activities [72] [75]. It has been suggested that whereas in mid-2000s almost 80% of cyber criminals were individuals and 20% were organised groups, 10 years later, in 2015 the situation was reversed with only 20% of cyber crime being committed by individuals and about 80% by organised groups [76]. The UN cyber crime study [72] states that cyber crime often requires a "high degree of organisation to implement and this may benefit small criminal groups, loose ad hoc networks, or organised crime on a larger scale" with the typology of cyber criminal groups reflecting that of organised crime. It also notes that many acts of cyber crime require high levels of organisation and considers it likely that conventional organised crime groups are also active in cyber crime [72]. Even though experts tend to agree that the role of individuals operating as cyber criminals is diminishing and cyber crime has become organised, not much is known about these organised groups [75]. McGuire [77] has suggested a typology (presented in Figure 14) of organised cyber crime proposing three main types of groups divided into two sub-groups. Type 1, operating mostly online, divided into swarms and hubs. Type 2, which combine online and offline crimes, divided into clustered or extended hybrids and Type 3, operating mostly offline, but using information technology to help in their offline activities. This dissertation uses the adapted typology suggested by McGuire [77] and not differentiating between offline and online activities, but on the organisation of activities.

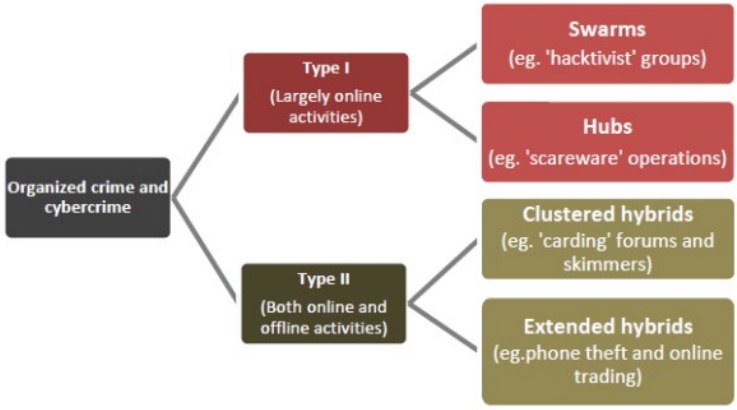

Figure 14: Structures of organised crime groups (as cited in [72])

Considering the increase of the criminal platform economy [14], using as-a-service models and do-it-yourself-kits anyone with some computer literacy can potentially become a cyber criminal. The internet and information technology provide new possibilities for short-term criminal groups convened for one crime at a time, which are different from traditionally very hierarchical organised crime organisations [72]. Bearing

all of the above in mind and drawing on McGuire typology [77], this dissertation divides financially-motivated cyber criminals into two broad categories: individuals and criminal groups, further divided as depicted on Figure 15.

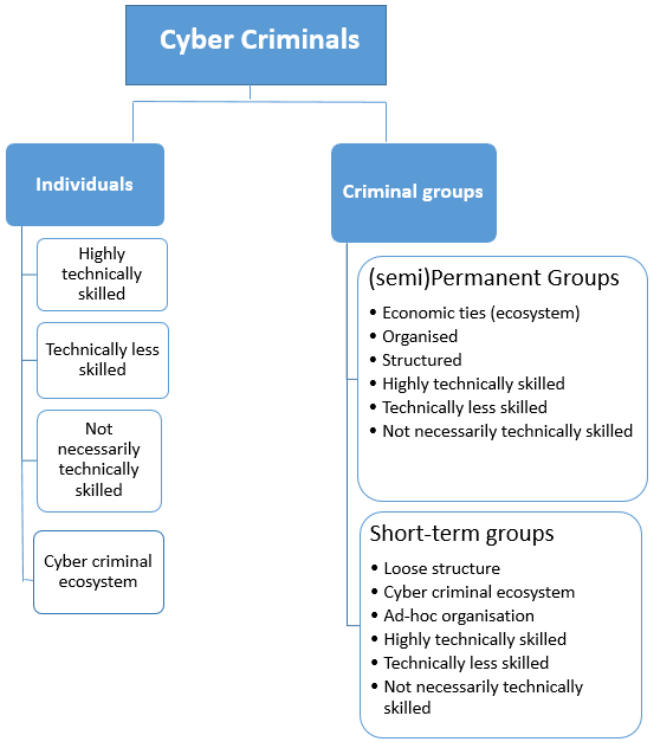

Figure 15. Two categories of financially-motivated cyber criminals

4.2.2 Victim

As suggested in **Publication I**, people, organisations and enterprises usually fall victim to cyber crime through either their actions or non-actions. One can potentially become a victim through simply using information technology (e.g. using e-mail, browsing the web, using removable media), or by not taking appropriate action to keep systems secure (e.g. not updating or poor management of systems, software or hardware; or poor password management). Having fallen victim, they will face damages, the impacts of which can be:

- personal non-financial harm (e.g. psychological harm, reputation damage, loss of data, hijacked accounts, abuse of resources, abuse of computing power);
- harm potentially resulting in direct financial consequences (e.g. loss of data, hijacked accounts, loss of intellectual property, unavailability of data/ IP, inaccessible data or devices, encryption of data or devices, identity theft); or
- direct financial losses.

The typical attacker's modus operandi is gaining or blocking access to a victim's device or its functionality [78]. A victim can be affected by targeted or opportunistic attacks, utilising a number of potential attack vectors: spam, phishing, DDoS, defaced website, malware, removable media, direct entry to system, zero-day vulnerabilities, etc.

For the purposes of the current thesis, victims have been distributed to two broad categories:

- High-value targets specifically selected for their personal or business significance. The criminals may want to attack a specific company or person, or to gain access to the data of a specific individual;
- Low value targets where criminals cast a "wide net" of attack vectors (spam, malware, etc.) hoping that some recipients will "take the bait" and this will provide them with sufficient financial benefits. The criminals may want to exploit victims that share a common characteristic (language, age, occupation, etc.).

Adopted from Ghernaouti [62], victims, both high- and low value targets, of financially motivated cyber crime, can broadly be classified into two general categories (Figure 16):

1) individuals (identity crimes, privacy related offences, direct financial crimes, extortion, etc.);
2) enterprises (theft of data or intellectual property, theft of services and resources, counterfeiting, economic espionage, etc.).

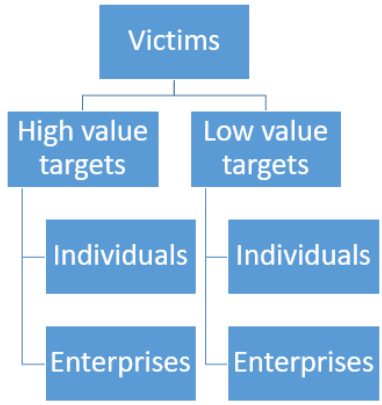

Figure 16. Victims of cyber crime

4.2.3 Categorisation of attacks

Publication I and **Publication II** show that the typical attacker modus operandi is gaining or blocking access to a victim's data, device, or functionality [78]. **Publication I** puts the emphasis on crime and looks deeper into the victim aspect, while **Publication II** adds aspects of politically motivated attacks, i.e. cyber warfare. The overview of current taxonomies and approaches to cyber crime presented earlier in Section 2.2 show two approaches in presenting attacks: 1) concrete technical means of conducting attacks (viruses, worms, trojans, denial of service, network attacks, user compromise, etc.) [46] [47] [48] [44]; 2) general attack methods (unauthorised access, malicious codes, interruptions of services, theft or misuse of data/ devices) [44] [46] [47]. In Section 4.2.2 victims were divided into two distinct groups: high value targets and low value targets. In the case of financially motivated cyber crimes and categorisation of attacks, the criminal has two approaches:

1) targeted, or victim-oriented attacks, where the victim is identified first and then means of attack (method) chosen; and
2) opportunistic (non-targeted), or attack method oriented attacks, where the criminal wants to use a specific method of attack, and the identity of victim is not important.

As the modus operandi will largely be the same in both cases (with differences in preparation for the crime), the attack dimension in the taxonomy should be based on the type of crime, which can be further sub-divided into attack means and enablers (such as malware, botnets, ransomware, etc.). The types of crime for current modelling purposes proposed are presented on Figure 17 and are the following:

- Data theft
- Extortion
- Online financial activity
- Breakdown, interruption or incorrect operation of services or infrastructures
- Theft or hijacking of computing power/ processing capacity
- Theft of information, secrets, intellectual property, or knowledge
- Manipulation of information (political, financial, etc.)

It must be noted, however, that the attack categorisation in Figure 17 is not a static division, limited to the list provided, rather this should provide flexibility for any new type of cyber crime emerging.

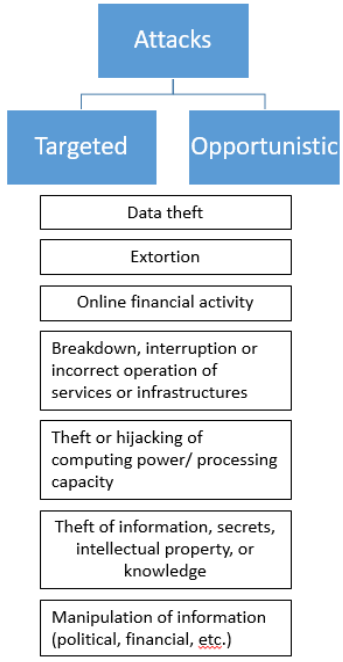

Figure 17. Attacks taxonomy, adapted from ***Publication IV***

4.2.4 Exit strategies

An exit strategy is choosing "the option that will maximise the value" and "be the most favourable from financial and personal satisfaction point of view" [79] to finalise any activity. It can be considered as a contingency plan, and there are usually two options for exit: generating gain or taking loss. Exit strategies are used in business or military campaigns and are usually planned for both positive and negative cases. In the case of cyber crime, exit can happen either at the beginning or at the end of a crime process. Early exit would be e.g. in preparation or execution stage, where criminals decide against committing a crime for any reason (e.g. after risk assessment or reconnaissance). Successful exit in cyber crime happens at the end of crime process, where gain has been already generated. In general, the gain from cyber crime can be divided into two: financial gain or non-financial gain. In other words, exiting the financially motivated cyber crime cycle means leaving the crime situation either before the crime has taken place or after the chosen objectives are achieved in generating financial gain and hiding evidence of the crime. In the case of financially motivated cyber crime, monetization is a distinct and very prominent part of exit phase and dictates the overall crime process.

A financially-motivated criminal must decide who and what to attack, attack successfully and then monetize the success. In general, there are five options to generate revenue:

1) Victim pays the criminal directly (e.g. in cases of extortion, where the victim pays to have their data decrypted after successful ransomware attack);
2) Victim's resources are turned to tangible assets where the victim's resources will be sold and traded. These resources can include credit card or banking information, personal information, loyalty points or gaming money;
3) Criminal pays for (criminal) goods and/or services to another criminal. These include outsourcing the crime or buying the means to attack from another criminal in real currency, cryptocurrency, re-sellable money equivalents, or goods and services;
4) Criminal gets access to victim resources and uses these for other (criminal) actions such as the use of victim assets in botnet operations or selling victim computing power for the purposes of e.g. illegal cryptocurrency mining;
5) Buying, selling or bartering other (legal or illegal) goods and services at dark markets (operations within the cyber criminal ecosystem, supporting further cyber- or traditional criminal activities).

It can be argued that any use of illegally obtained money or assets resulting in these funds becoming available in the legal economic ecosystem is considered money laundering. For the purposes of this dissertation, two distinct options are considered in discussing monetization of revenues from cyber crime: laundering money, and other forms of disposing of revenues [14].

Disposing of revenues here means direct use of proceeds received by the criminal, i.e. purchasing any assets, either in cryptocurrency or any other form. According to research, cyber criminals use their revenues for covering immediate needs (paying bills, buying food, etc.), buying property or vehicles, investing in financial assets or investing in anything else that holds value (e.g. art) [14].

Laundering money has been a challenge for criminal organisations since they have existed, and cyber criminals are no exception. They use the "tried and tested" means of

laundering money: utilising money mules as actors, or laundering money through legitimate businesses or financial institutions [14]. In addition, the criminals have also come up with new solutions enabled by the digital economy, such as cyber laundering, using online payment systems (e.g. PayPal.), using cryptocurrency and related platforms, or using money equivalents (gaming money, loyalty points, etc.).

In terms of cyber crime, an exit strategy (Figure 18) will be when the criminal decides to leave the crime scene, either after having completed the crime and generated revenue, for the (immediate) risk of getting caught by law enforcement authorities, for the risks or costs overweighing the benefits, or for simply not being able to make enough profit. The exit strategy also means hiding their tracks and analysing law enforcement agencies' abilities to infiltrate crime rings or their capabilities of investigating crimes.

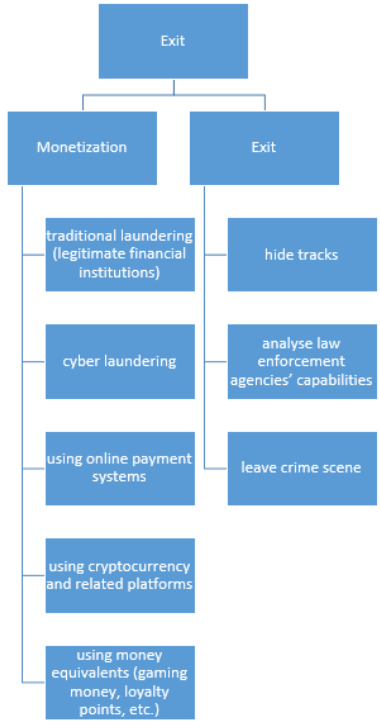

Figure 18. Exit phase of a financially motivated cyber crime

4.2.5 Interim Conclusions

Cyber crime is widely acknowledged as a vast and growing problem. Even so, understanding cyber crime as a complete system or process is not studied in detail, and to a large extent this is influenced by the lack of an appropriate taxonomy. Any taxonomy used in mapping cyber criminal journeys should be appropriately generic and based on stakeholders and actions interacting within a cyber crime cycle.

The basis for the proposed taxonomy in Figure 19 is the underlying crime process, i.e. starting with the criminal(s) identifying the victim(s) (high-value or low-value targets), choosing appropriate attack vector(s) (targeted or opportunistic), executing the crime, to finally generating revenues and turning these into tangible assets.

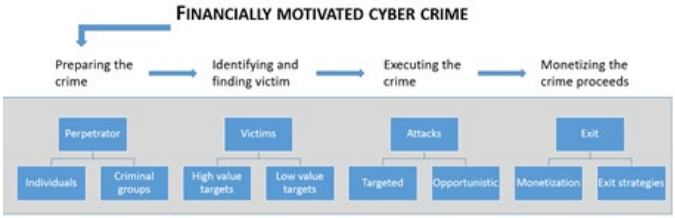

*Figure 19. Generic taxonomy of financially motivated cyber crime (Adapted from **Publication IV**)*

The validation process (explained in Section 3.3) included workshops, interviews with LEA representatives and focus groups discussions. This validation showed that the generic taxonomy proposed would allow the analysis and development of a better understanding of cyber crime as a process, as depicted in Figure 19. This illustrates how criminals and victims interconnect with each other and where attack vectors, enablers and exit strategies are analysed in a systematic context. This is significant because it would help develop an understanding of how cyber crime business processes work, but also how the tactics, techniques and procedures utilised by criminals function. In order to fight against cyber crime and understand the opponent, modelling can reflect their activities and decision processes within the crime cycle. It is especially significant in understanding organized crime, which relies heavily on processes. This could potentially lead to identifying pinch points in the cyber crime processes, find better countermeasures, and develop novel policy, awareness-building, investigative, or technical approaches in the fight against cyber crime.

4.3 How cyber crime works

In a book on Information Age, the sociologist Manuel Castells stated: "Technology is society, and society cannot be understood or represented without its technological tools" [80]. Development of technologies have brought about what Castells calls the "network society" [80] – most organisations, functions, and processes we use today are networked. While Information Age and networks provide many benefits to governments, enterprises or individuals, they also have a profound impact and are major enablers for cyber crime. Cyber crime is global, organised, innovation- and technology-driven and has developed its own economy, mirroring our contemporary legitimate economy [14].

4.3.1 Economic perspective and cyber criminal economy

Adam Smith wrote a classic book "An Inquiry into the Nature and Causes of the Wealth of Nations" in 1776 [81], stating that economies evolve from pre-historic bartering to money-driven economies, and introduced ideas such as free trade, laissez-faire economic policy and the division of labour. In [81] he also proposed the "invisible hand" approach, where free market produces widespread benefits to all, and markets will find their equilibrium without any outside interventions. Analysis on developments of cyber crime show that it has progressively moved towards such an "invisible hand" economic system with no higher intervention and a free and self-regulating market, and division of labour.

Earlier works on the cyber criminal economy referred to cyber crime industry [30]. The notion of the cyber criminal economy was suggested by [14] that the cyber criminal economy is a "connected range of economic agents, economic relationships and other factors generating, supporting and maintaining criminal revenues at unprecedented

scale" [14]. Developments in technology have not only created stronger relationships among nations or people, but also among criminals and research has shown a renewed globalisation of crime [82]. Just as Information Age has brought benefits to societies at large, it has enabled enormous growth of cyber crime. The cyber crime economy has also begun to mirror our legitimate economies, and is often out-innovating both the business models and revenue generation of legal economies [14].

The production and consumption of goods and services are used to fulfil the needs of those within economy, which is also referred to as an economic system. Economics studies how an economy functions, how goods and services are produced, distributed and consumed. Macroeconomics studies how the entire economy and market systems function, and what are the financial and economic conditions that impact the economy as a whole. Microeconomics is generally used to study the economic activities of individuals and enterprises to understand why they make certain decisions and how these decisions affect the larger economy. The aim of current chapter is not to analyse cyber crime from an economic perspective in depth, but to give an understanding of how a cyber criminal economy functions. The cyber crime economy has "become a mirror image of contemporary capitalism" [14], which has grown and scaled similar to legitimate economies. It is huge, yet there is not much known about its structure or outreach.

As suggested in [19], cyber criminals in their economic activities depend on macro, meso and micro conditions. Corbin and Strauss introduced a conditional and consequential matrix for analysing macro and micro relationships of situations. Drawing from economics and the work of [19], the matrix in Table 10 analyses macro, meso and micro conditions in the case of financially motivated cyber crime. In this analysis:

- micro refers to factors over which individual criminal or criminal organisation has control;
- meso refers to factors which an individual criminal or criminal organisation can influence;
- macro refers to factors the criminal has no (or limited) control over.

Table 10. Conditional and consequential matrix of macro, meso and micro levels of relationships in financially motivated cyber crime (based on and adapted from [19])

Macro	Meso	Micro
Legislation (national and international)	Regional and global	Individual
Law enforcement	Language and culture	Capabilities and knowledge
Technology developments	Organisations	Risk assessment
Political, societal conditions	Ecosystem (as-a-service, bartering, outsourcing)	(Business) decisions
	Marketplaces (supply and demand)	
	Networks, forums, websites, stores	
	Money mules, laundering system	
	Safe havens	
	Corruption	

Financially motivated cyber crime is not a stand-alone enterprise, but is influenced by factors both within and outside the cyber criminal economy, which can be analysed by both macroeconomics and microeconomics. Cyber crime is not driven solely by technology, but also by political, legal, cultural and economical factors at different levels. The brief analysis conducted for this dissertation provides an overview of macro, meso and micro factors influencing financially motivated cyber crime. The analysis was conducted from information provided in interviews with experts from academia and LEA. The interviewees were asked about their assessment of factors which influence cyber crime from two aspects: factors the criminals can influence or control, and those they cannot. During the course of the interviews three categories emerged: factors the criminal can control (micro), those they can influence (meso), and those they cannot control (macro). Combining the adaptation of [19] and interviews, the resultant visual representation is depicted in Figure 20.

At the centre of the criminal economy is the micro level, or the criminal themselves. The micro level refers to factors over which the criminal has full control: the individual himself, their knowledge and capabilities, risk appetite and (business) decisions. The macro level represents factors over which the criminal has very limited or no control: legislation, LEA activities and capabilities, technology developments, changes in political or societal conditions. In between the factors that can or can not be controlled by the criminal are the factors, which the criminal can influence, the meso level, the enabling factors of cyber crime. On one hand are the factors outside of the criminal ecosystem that the criminals may be able to control, such as corruption and safe havens. On the other hand these are the factors within the criminal ecosystem: marketplaces, networks, fora, websites, stores, but also money laundering capabilities (including money mules). Meso level also refers to the organisational aspects of criminal organisations: regional or global, centred around one specific nationality, (sub)culture, or language.

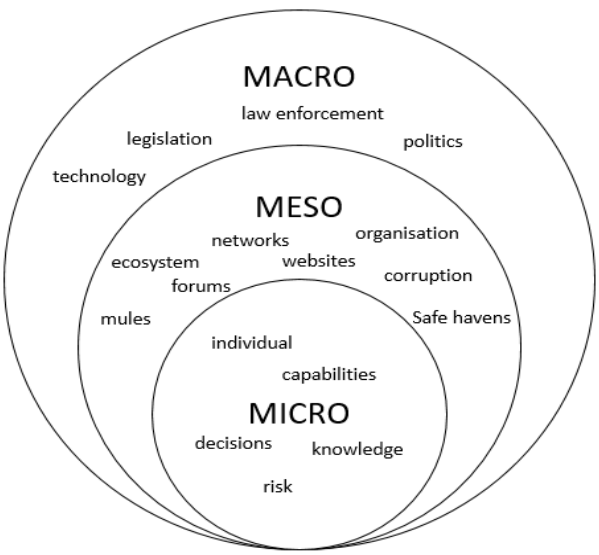

Figure 20. Factors influencing cyber criminal economy (adapted from [19] and interviews).

4.3.2 Cyber criminal ecosystem

Section 4.3.1 suggested that we are witnessing the surge of cyber criminal economy, which is mirroring the legitimate economy. Business ecosystem "is a network of organisations that drive and create/deliver services or products", and performance of one enterprise or product depends on the performance of other enterprises and products within this ecosystem [83]. Business ecosystems are dynamic and constantly evolving [84], where companies see their "ecosystems as helping them become more resilient to market changes (*in order*) to achieve market success and sustain performance" [32]. In much the same way, success of cyber criminals is dependent on innovations of other cyber criminals.

A cyber criminal ecosystem is a "dark network" [85]. It is challenging to describe the entire ecosystem of cyber crime, as it is very big, there are many players, it is disjointed and constantly changing [76]. Cyber criminal ecosystem "enables, funds, and supports criminal activity on a global scale" [14]. Based on research, four main players were identified as parts of ecosystem (see Figure 21): leader (individual or organisation), developer/ programmer, service provider, and black market. It can be said that the victim is the fifth – very important – player in this ecosystem. However, contrary to other players, victims are not part of this ecosystem from their own will [67]. The map on Figure 21 is a generalisation and simplification, as it is beyond the scope of this dissertation to provide detailed research on cyber criminal ecosystem. In actual fact, the cyber criminal ecosystem is far more complex.

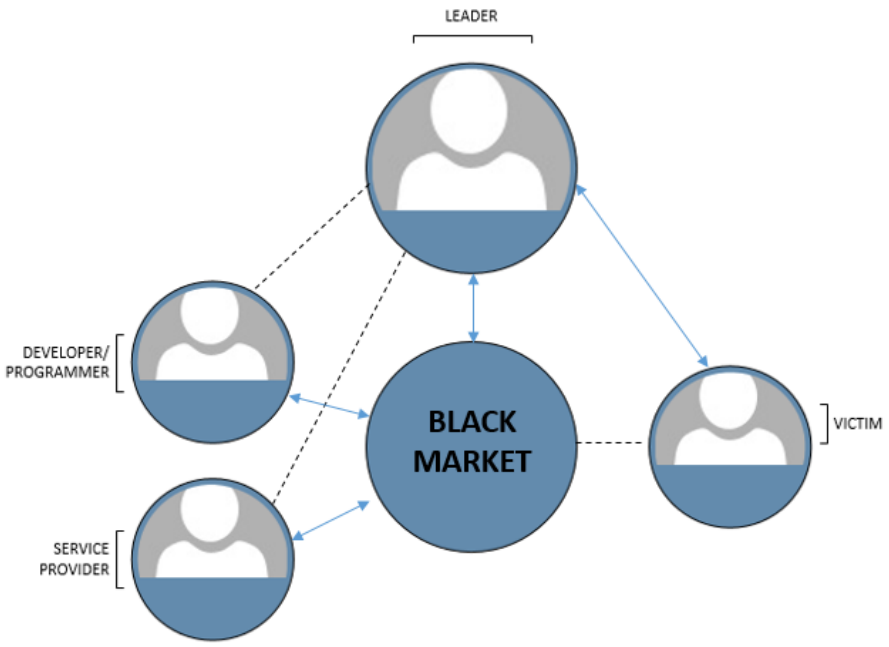

Figure 21. Main players in a cyber criminal ecosystem

The leader is the individual or group who is the organiser and primary beneficiary of the crime. This is the instance that makes all major decisions within a crime cycle and interacts with other players through the black market.

The black market is a general name, which for the purposes of this dissertation includes marketplaces, networks, forums, websites and stores where cyber criminal goods and services can be bought, sold, bartered or traded. Examples of such markets include the Silk Road, Blackhole Exploit Kit, Carder.su, etc. [76]. These marketplaces seem to disappear, re-appear, or re-organise following LEA actions or internal problems within a criminal ecosystem, such as trust which is a major element in these ecosystems [6]. There are also dedicated forums where most transactions take place. The forums display advertisements, but the actual transactions mostly seem to take place by means of encrypted and private messaging, shared e-mail, or specific locked-down social media accounts – all evolving with available technology [76]. It is estimated that more than 50% of cyber crime revenues are generated through black markets [14]. The markets and forums are a key element in (organised) cyber crime, both in terms of an initial enabler (providing the tools and services) and as a monetisation option (money laundering or bartering for other goods and services) after the crime. It must also be noted, that as stated above, such markets and forums disappear and re-appear following various disruptive activities, therefore the examples above are just historical examples and might not depict the current reality at time of publication of the current dissertation.

Skilled professionals can be recruited as developers and programmers for programming and virus writing, web designing for phishing pages, and testing [22]. A more specific skillset required are cryptographers, who are hired to evade e.g. malware detection. Kaspersky Lab noted that in general there are two kinds of programmers and developers: those who know they are working for illegal purposes and those who (initially at least) do not [22]. In other words, professionals working within the legitimate economy can be recruited by cyber criminals, either knowingly or unknowingly. This category also includes web designers, testers, and system administrators.

Just as in the legitimate economy, cyber crime has changed to become service-oriented, where some criminals develop malware, others sell access to infected devices, yet others provide money laundering services [86]. There are several kinds of service providers involved in a cyber criminal ecosystem: cyber crime-as-a-service providers, infrastructure service providers and monetization service providers. The cyber crime market is segmented and one does not need to have programming skills to conduct a crime – anything can be bought on the market [86]. The lead criminal may outsource (some aspect of) the crime, if this is more cost efficient or if they do not have the necessary skills, tools, or time. Some crimes are more effective if they can rely on criminal infrastructure providers. For example, bulletproof hosting is a concept that is very useful to cyber criminals, since such service providers will not typically cooperate with LEA. While their actions may not be illegal (depending on the jurisdiction and the case at hand) they are major enablers for cyber crime. Monetization service providers take care of monetizing the crime, either through the whole process from withdrawing the money from compromised accounts, or simply organising and utilising money mules or transferring the proceeds.

5 Modelling financially motivated cyber crime

Central to the work of this thesis is the construction of a model, a cyber criminal JMAP, for a generic financially motivated cyber criminal process. Chapter 5 will answer research question 3: "Which model can be adapted for modelling financially motivated cyber crime?". British statistician George E. P. Box has been attributed as saying "Essentially all models are wrong, but some are useful" [87]. Box meant that no model can represent the exact real behaviour, but it could be very helpful if it is close enough. Models are an abstraction or simplification of reality, leaving out irrelevant details. Models bring out those aspects of reality that we are interested in and their interconnections (elements, events, connections and relationships), and can be presented either schematically or symbolically [27]. The model developed within this dissertation is a practical mechanism, which can be used by various stakeholders in the cyber crime investigation and prevention process.

The financially motivated cyber crime process model (Criminal JMAP) is presented schematically, and highlights major stepping stones or pinch points within a cyber crime process, showing connections between important elements, enablers and events within this cycle. Rather than focusing on the solely technical elements of cyber crime, the JMAP model will show other aspects of the attack related to an attacker's intent, resources, interactions between all players in an attack process, preparation for and execution of an attack, desired end state and exit/ monetization strategy. This is significant because understanding the whole sequence of events in a crime can help identify pinch points in the criminals' activities and business models (**Publication I**), especially in the context of organised crimes that rely heavily on processes. As suggested in **Publication I**, the aim is to allow those investigating cyber crimes or developing countermeasures to quickly apply new crimes to the model and focus on the specific known (or unknown) pinch points in order to conduct their work more effectively.

As a result, the JMAP model can give a better oversight on where to best focus Law Enforcement Agencies' activities in investigating cyber crime. It can also provide insight into which actions can be taken in the fight against cyber crime: policy initiatives, awareness campaigns, legislative/regulatory changes, development of new technological applications, behaviour modification of potential victims, and/or increased monitoring by LEAs in order to prevent cyber crime.

Cyber criminals are always ahead of investigators [14]. The scope and scale of cyber crime is acknowledged, but most research until now has focussed on modelling how cyber crime is conducted, i.e. technical factors (see e.g. [21] [20] [88]). Recently, the importance of the weakest link, the human factor, has also been researched. What has not been researched to a significant extent, is an understanding of cyber crime as a system [14] [10], which is dynamic and constantly changing. As expressed in **Publication I**, understanding cyber crime as a process provides a different view on how cyber crime happens, thereby providing better options to investigate such crimes, find or develop new countermeasures or develop awareness building measures.

Section 4.2 proposed a new taxonomy to depict cyber crime with the purpose of modelling it as a process in a more useful way. Considering the proposed taxonomy of Section 4.2 in general and discussions in Sections 4.2.1, 4.2.2, 4.2.3, and 4.2.4 in particular, Figure 22 below presents the cyber crime process.

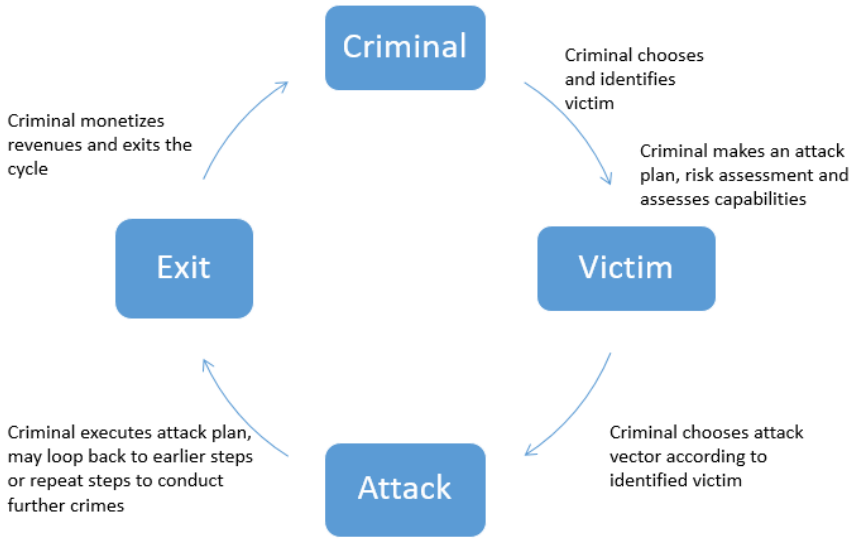

Figure 22. Cyber criminal cycle, following proposed taxonomy (adapted from REF Pub 4)

5.1 Related work

Section 5.1 will answer research question 3.2 "Which existing models are available or can be adapted to model the process of financially motivated cyber crime?", by looking at three related concepts: journey mapping, phase-based approach and crime scripting.

5.1.1 Journey mapping

Journey mapping is a methodological tool that has been traditionally used in mapping customer experience [89] and public service transformation [90] (e.g. visiting a doctor, improving emergency services' response activities, improving traffic behaviour of drivers [89]). Journey maps focus on human experiences [90]. Most commonly, the structure of a journey map consists of phases and steps which define the visualized experience [90]. The scale of a journey map can range from a high-level map (depicting the entire end-to-end experience) to a very detailed journey map (showing only a few instances in great detail). Journey mapping always represents a single experience without mapping the decisions, or decision trees [90]. Journey maps are typically meant to be a catalyst, not a conclusion, and help to identify the opportunities, pain points, and calls to action.

A journey describes all events and experiences that specific individuals or organisations go through to reach a goal or fulfil a need. A journey consists of events that describe what has happened and experiences that describe how the person or organisation involved felt during these events. Events and experiences are then translated into a visualisation map to show the full event process, key steps as well as positive and negative events. This tool is often used by strategy consultancies and public organisations to shape customer strategies and public service transformational programmes.

5.1.2 Phase-based models

Phase-based approach has been used in the armed forces [91] [92] to find capability shortfalls and make decisions on the development of new capabilities [93]. It has also been used to model Improvised Explosive Device (IED) attacks to model entire process from adversary funding to attack execution. In addition, phase-based models have been used for anti-terrorism planning, with the U.S. Army describing terrorist planning cycle as a multi-stage process that provides a baseline to assess intent and capability of terrorists [94] [92] [93].

In addition to military, phase-based approach has been used in information security field. Sakuraba et al [95] provide a framework for Attack-Based Sequential Analysis of Countermeasures providing opportunity to map countermeasures along the time phase in an attack. Willison and Siponen [95] use Situational Crime Prevention model, modelling crime from the attackers perspective during phases of crime. Hutchins et al [20] developed a Cyber Kill Chain, providing a cyber intrusion kill chain model with seven phases, from reconnaissance to actions on target.

5.1.3 Crime scripting

The early theoretic script approach is illustrated by what is commonly known as a Restaurant script [96], describing a customer perspective of eating in a restaurant. This is comprised of four phases: entering the restaurant, ordering a meal, eating the meal and leaving the restaurant, each phase consisting of explicit steps [97]. Scripts have become to be used in many disciplines and they are a depiction of sequence of activities constituting one single event [97], or more specifically "[a] script is simply a sequence of actions which make up an event" [98]. The past decade has shown a growing interest in crime scripting [99] [100], notably on modelling "crime commission processes" in cases of both physical and cyber crime [101]. Crime scripts have become "an increasingly popular method for understanding crime by turning a crime from a static event into a process, whereby every phase of the crime is scripted" [10]. The requirement to better understand the "where-when-how" of crimes has been identified in many disciplines, among these cyber security [101]. In crime scripting, "a script is considered a predetermined, stereotyped sequence of actions that define a well-known situation in a particular context" [97]. Crime scripts are schematic representations explaining "how knowledge is organised about how to understand and enact behavioural processes" [97], or how we believe a sequence of events will occur [102]. As scripts alone could not explain how an event happens, they were described in a broader framework to include goals and plans; based on the idea that goals are achieved by planning a sequence of events [96]. It has been argued that crime scripts are effective in helping to understand criminals' behaviour and routines during the crime process [10].

One of the first to introduce crime scripts, Cornish indicated that crime is an event containing a number of steps from start to finish, and proposed a modelling approach to depict criminals' decisions during the crime event [103]. Cornish also introduced crime scripts to criminology, proposing to turn a crime from single event to a process [103]. Consequently, the concept of crime scripting can make it easier to understand the process of committing a crime [99]. A decade later, it was proposed that crime scripting is an important means to understand complex crimes [104]. Scripts can be useful in many crimes, but are considered specifically useful in new and complex crimes [98], their usefulness being in allowing us to identify the decision points (pinch points) in criminal operations [105]. Levi has suggested that crime scripts can provide an innovative way to gather more insight of "complex forms of crime in a review of organized crime-reduction

strategies" [104]. Crime scripts highlight the procedural nature of crime [97] and should be able to reveal an overall picture of the sequence of actions a criminal undertakes before, during, and after a crime has occurred. Crime scripting classically involves breaking down the actions of the criminal into four main stages – preparation, pre-activity, activity, and post activity, with each stage concentrating on the main elements of a crime (who, what, when, where, why, and how). Classically, the most important information gathered is how the criminal conducts the crime and what decisions they make along the way. Although there are numerous papers about crime scripts in criminology, there are almost none about utilising crime scripting for cyber crimes [10].

As there are no universally accepted rules or specific software for creating crime scripts [98] [97], they vary greatly in form, detail, and content. A literature research indicates that there are many articles about crime scripts in general, but almost none on scripting the crime process comprehensively, which is why crimes have predominantly been modelled not following structured methods, but intuitively [24]. Some crime scripts simply list a sequence of actions, others provide a graphical picture showing this sequence of actions and decision-points [98]. Crime scripting allows crimes to be logically deconstructed to their component parts, even from a small and incomplete dataset [98]. Borrion et al conducted an exploratory study of video-based crime scripting showing that "different individuals produce scripts of varying quality" [101]. Since there are no standard rules or software for either journey mapping or crime scripting, this dissertation has used its own symbols: a series of chronological boxes linked by arrows. The boxes indicate actions or decisions, and arrows indicate direction of flow. Similar logic has been followed in graphical presentation in some cases of crime scripts [98].

5.1.4 Mapping and modelling cyber criminal journeys: the JMAP model

In the cyber crime context, a combination of elements from journey mapping (as explained in 5.1.1), phase-based approach (as explained in 5.1.2) and crime scripting (as explained in 5.1.3) can be used to describe all events and experiences that cyber criminals go through to fulfil their objectives during the cyber criminal process. The JMAP model that is suggested in this dissertation has been developed based on journey mapping and crime scripting methodologies, with the aim to analyse a cyber crime process, including actions and decisions of criminals. This process is presented as a step-by-step chronological account of actions: the steps before, during and after the crime. It is important to emphasise that mapping was conducted from the criminals' point of view. Development of the JMAP model started initially by developing single event journeys, followed by generalisations to develop generic journey maps according to typologies of crimes. To assess the quality and adequacy of such journey mapping, the JMAP model was used as a catalyst for conducting semi-structured interviews and brainstorming sessions. While the model as a whole was discussed and analysed, each phase in the process model was addressed separately.

The initial input for journey mapping that forms the background of this thesis, was conducted during the E-CRIME project [67]. The E-CRIME project focused on the perpetrators and deployed crime scripting techniques to develop eight journeys, mapping the key actions of the perpetrators. The E-CRIME project developed eight cyber criminal journeys [67]:

1) Building a botnet;
2) Extortion (ransomware);
3) Espionage (APT/ APA);

4) Malware development/ zero-day exploit development;
5) Cryptocurrency mining;
6) DRM cracking;
7) VoIP attacks;
8) Click Fraud

The selection of journeys was based on commonalities between different crimes derived from literature, results of expert interviews, and validation at expert workshop. For each script, a mapping was conducted of the three principal phases of a cyber crime: preparation, execution and monetization. Since there are no standard rules or specific software for crime scripting or journey mapping [90], the project used its own symbols and drawings. These journeys were validated in the EU FP-7 E-CRIME project's validation workshop, held in Rome on January 19-20, 2015. Having scripted the eight different types of cyber crime, a general crime script, or "journey map", was developed. This work deconstructed the lifecycle of crime events and translated these into a visualisation map to show the full event process.

The current dissertation has used journey mapping, crime scripting and phase-based approach, as put forward in **Publication II**. The work deconstructed cyber crimes into four principal stages (Figure 23). While the motivation phase is important in understanding cyber criminal actions where the criminal makes a conscious decision to engage in a crime, it has been omitted in the work that follows. The current dissertation looks at financially motivated cyber crime, which already includes motivation in itself, therefor the current modelling and the JMAP model has omitted the first stage – motivation – and provides a JMAP model of three stages: preparation, execution and exit. The thesis looks at crimes from the criminal's perspective, and the process of crime includes preparation, execution and exit phases.

Figure 23. Four phases of a general cyber crime process

After initial work following Grounded Theory Methodology, the scripting was validated throughout the validation process. After each validation event, comments and feedback were considered and the JMAP model was refined, following the GTM. The validation process was explained in detail in Section 3.3.

In taking further the work completed as part of E-CRIME project [67], this thesis looked more deeply into crime scripting, journey mapping, phase-based approach and several other attempts which have attempted to model cyber attacks in general and cyber crime in particular. Most researchers have focused on modelling cyber attacks with less attention being paid to modelling cyber crime. Therefore more attention has been paid to how cyber attacks take place and are executed (malware, security holes, APT, DDoS,

ransomware, etc.), but cyber crime as a system or process has received little attention [14]. Based on previous work, and as put forward in **Publication I, II** and **III**, a JMAP model for financially motivated cyber crime was developed. **Publications I** and **II** provided an overview of principles used for modelling cyber criminal journeys. **Publication I** concentrated on cyber crime, **Publication II** widened the scope to include cyber warfare, and Publication III applied the methodology to trolling.

5.2 Cyber crime as a process: Criminal JMAP model

A successful cyber attack of any kind means the perpetrator has to take a series of consecutive steps [23]. In modelling, these steps are combined into logical groupings and further into phases, thereby creating a cyber attack process. The cyber attack processes consisting of a number of phases are referred to as cyber kill chains or cyber attack life cycles [21] [20]. They are practical representations (models), which describe cyber attacks in different intrusion stages. Section 5.2 addresses research question 3.1 "Which models have been used for modelling cyber crime?" and research question 3.3 "Can existing models be adapted for financially motivated cyber crime?", and proposed a Criminal JMAP model.

Publication V has analysed the best-known models that have gained prominence for practical use: Cyber Kill Chain, HP Attack Life Cycle, and ATT&CK Matrix by the MITRE Corporation. A summary of this work is provided in the following section.

Maimon and Loderback [23] discussed cyber enabled crimes and divided successful ones into four stages:

- initial stage, which includes initial reconnaissance of potential targets' vulnerabilities and collecting available intelligence;
- second stage, utilising the results of initial stage and gaining access to previously identified target assets;
- third stage, which includes elevating privileges and commissioning the actual crime; and
- final stage, where the criminals conceal their tracks and hide evidence [23].

Hutchins et al introduced the widely acknowledged Lockheed Martin (LM) Cyber Kill Chain concept [20], which defined any cyber intrusion as an end-to-end chain process. In their definition, any attack is made up of seven steps:

- reconnaissance,
- weaponization,
- delivery,
- exploitation,
- installation,
- command and control (C2), and
- actions on objectives.

Hewlett-Packard's Attack Life Cycle [21] includes 10 stages:

- reconnaissance,
- attack delivery,
- exploitation,
- installation,
- command and control,
- regional seizure,

- internal exploration,
- elevation of privilege,
- channel creation, and
- information theft.

HP's approach is different from LM in one aspect: the stage after the attacker has infiltrated the target system is further subdivided into three steps: internal search, elevation of privilege, and information theft, and their proposed life cycle does not include weaponization [21] [20].

The MITRE corporation has proposed the ATT&CK Matrix, which is a "knowledge base of adversary tactics and techniques based on real-world observations" [88]. In essence this is an adversary behaviour model, reflecting attack life cycle. The ATT&CK Matrix divides attacker actions to 12 steps:

- initial access,
- execution,
- persistence,
- privilege escalation,
- defence evasion,
- credential access,
- discovery,
- lateral movement,
- collection,
- command and control,
- exfiltration,
- and impact;

In their matrix, the MITRE corporation has further decomposed each step into tactics or techniques employed by adversaries [88]. There is also A PRE ATT&CK model which reflect actions before an attack itself, e.g. finding targets and taking initial steps to prepare attack commission.

As previously published in Publications I and II, the cyber criminal journey mapping and the resultant JMAP model are based on mainly three concepts: crime scripting as used in criminology, phase-based approach as used in military, and customer journey mapping as used in business and public services. Furthermore, the Cyber Kill Chain, Attack Lifecycle and the ATT&CK Matrix together with PRE ATT&CK model have also been considered when developing the JMAP model.

Much of the current literature potentially underestimates the amount of time, effort and planning that would go into achieving a profitable and sustainable cyber-crime business. Just because a piece of malware can be developed and deployed does not mean that the revenue flows immediately. In order to commission a successful cyber crime, the criminals need to have successful business models. This is a complex task comprising of investments in setting up and managing technical infrastructure, identifying targets, selecting victim base, generating profit from victims, evading detection and generating monetary gain. A certain level of mutual trust must exist among all parties (including buyers and partners) in the criminal ecosystem, which needs to be better understood. There are also some indirect costs the criminals occur during the complete process of committing a crime, e.g. developing a trust and honour system amongst criminals can be complex and costly. Finally the monetizing of profits into tangible currency or assets all

comes at a cost, i.e. when cyber criminals use external experts (money mules or money laundering options), this will have a direct impact on their proceeds.

The different elements of cyber crime have been studied separately by academics, law enforcement, or cyber security enterprises. While this allows all component elements to be studied in detail, it has only superficial effects [106], since the critical parts of ecosystem or criminal processes have not been included. This dissertation has sought to broaden the approach of studying cyber crime processes, by exploring cross-disciplinary links, thereby supporting the research and practice of more demanding procedural analysis of cyber crime.

Based on the above overview and on Publications I and II of journey mapping and crime scripting it has been concluded that it is useful to split the process of cyber crime into four phases: intent, preparation, execution, and monetisation. Even though the main steps and modus operandi of criminals may be the same (see [25] [26]), any other motivations and their impact on a cyber crime process should be discussed separately. The model proposed follows from the crime scripting approach described in Publication I of breaking the actions of criminals to four main stages – preparation and pre-activity, activity, and post activity. Publication V concluded that the stages used in crime scripting and the proposed model can be related as depicted on Table 11.

Table 11. Adapting crime scripting methodology to modelling financially motivated cyber crime

CRIME SCRIPTING	MODELLING FINANCIALLY MOTIVATED CYBER CRIME
Preparation Pre-activity	(Motivation) Preparation
Activity	Execution
Post-activity	Exit

For the purposes of this dissertation the details of intent (motivation) phase of a cyber crime have not been considered, since the work is based on the underlying restriction that the intent is financial gain. For phases of preparation, execution and monetization similar actions have been grouped under broad terms.

Figure 24 presents the main result of the current dissertation, the Criminal JMAP model for financially motivated cyber crime. The model has been developed based on journey mapping and crime scripting methodologies, utilising other existing models as explained above. The proposed framework JMAP model is explained in **Publication V** and it is a result of generalisation after analysing several cyber crime types. Although the JMAP model proposes four specific phases in a cyber crime process, the findings from analysing different crime types suggest that depending on the crime type, the emphasis on any one stage differs. For instance in people-focussed crimes (e.g. CEO fraud, ransomware attacks, payment scams, romance scams, etc.) the main emphasis may be on the preparation phase, whereas the technology-focussed cyber crimes (where cyber systems are targets) the main emphasis is on the execution phase. In developing the JMAP model, specific crimes were deconstructed to their component parts and modelled, thereafter specific models were generalised to develop a generic process model. As cyber criminals are constantly innovating, making use of new technologies and business models, it is clear that any process model developed can not be exhaustive. The aim of the current modelling approach is to present a generic high-level process

model, providing an overview of the entire end-to-end experience. This generic model does not focus on details or map the specific if-then decisions or decision trees and is not meant to be a conclusion. It is rather meant to be a catalyst and inspiration to help identify major steps, decision points and pinch points within a cyber criminal cycle. As stated above, not all steps within the three phases are necessarily present for any one crime type, and crime is not a linear process: steps in it can be omitted, steps may be added, and previous steps can be reverted back to when there is such a need, or when a course of action taken presents another criminal opportunity. The JMAP model is intended to be a guide for identifying criminal actions and decision points throughout a crime cycle.

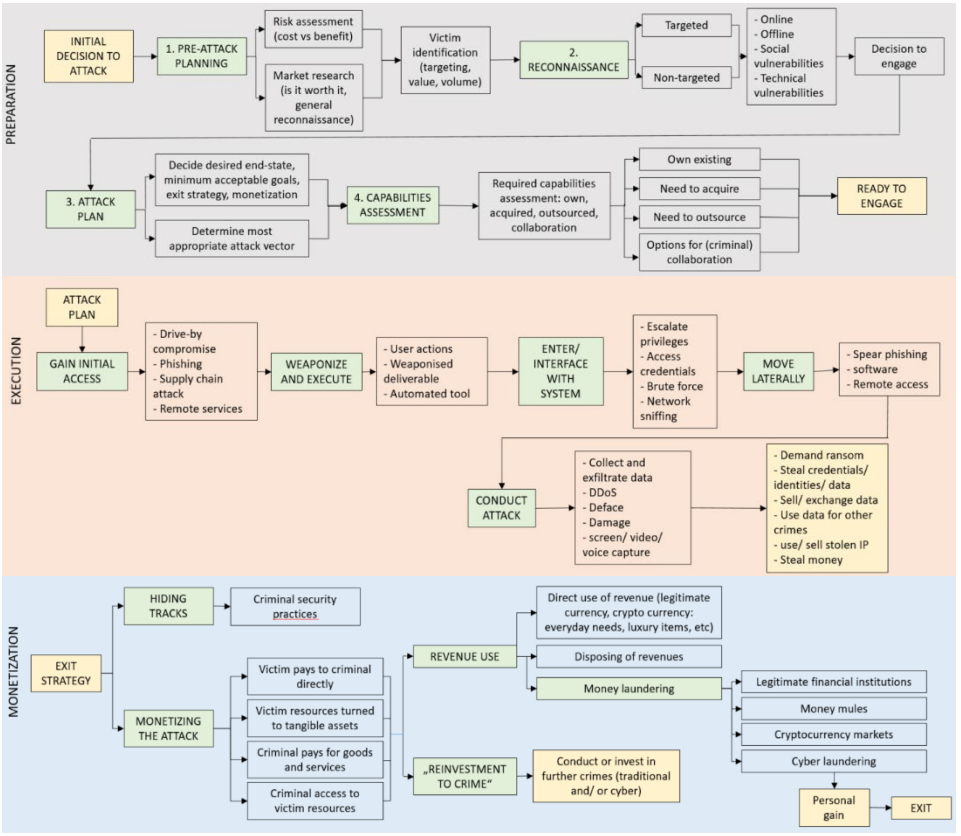

Figure 24. Cyber Criminal JMAP model

It is important to note that throughout any one criminal journey, the perpetrator can loop back to an earlier step (if a chosen attack method fails, they need to find a new one, or they may 'accidentally' find unforeseen vulnerabilities to take advantage of), or they can repeat steps, or they may just quit once they realise the efforts are not worth the results.

As opposed to offline crime, cyber crime in general and organised (cyber) crime in particular rely heavily on processes, which can be better explained by the developed JMAP model. Modelling the processes and decision-making of criminals can also help in developing an understanding of the role and practices of those interacting in a crime cycle, within the cyber criminal ecosystem. The findings in **Publication V** highlighted potential uses of the model in:

- investigating cyber crime;
- preventing cyber crime;
- identifying the pinch points within the criminal process;
- experiment the application of countermeasures in virtual environments;
- developing guidance in efforts to adapt or develop additional legal countermeasures;
- training of law enforcement authorities.

Sections 5.2.1, 5.2.2, 5.2.3 below explain each phase within a general crime cycle in more detail.

5.2.1 Preparation phase

Section 4.2.2 divided victims into two groups: high-value targets and low-value targets. Section 4.2.3 stated that the criminal has two options in conducting the crime:

- victim-oriented (targeted) approach, where the criminals choose a high-value victim on the basis of their personal, business or public importance; and
- attack method oriented (opportunistic, non-targeted) approach, where the criminals indiscriminately concentrate on using a specific attack method and target many users, services or devices (low-value targets) at the same time.

In victim-oriented approach, the criminals typically conduct targeted attacks aimed at high-value targets (i.e. specific public entity, company, person or service), in order to gain access to specific data. These are targeted attacks, with more focussed strategies, which are carefully prepared and aimed at a specific organisations or people. APT/APA attacks usually belong to this category. Targeted attacks may be more successful and are therefore more lucrative to the criminals.

In following an attack method oriented approach, the criminal wants to use a specific method of attack, and the identity of victims are not important. The attack method oriented attacks are usually mass campaigns, aiming to entrap as many people as possible. Victims are low-value targets, with criminals using attack vectors (spam, malware, etc.) for mass campaigns, hoping that some recipients will “take the bait” and this will provide them with sufficient financial benefits. Such mass campaigns usually do not provide high earnings. In such attacks, the criminals may target victims who share a common characteristic (geographic location, language, gender, age, etc.).

In terms of planning for the crime, and notwithstanding subtle differences between the two approaches, the phases and steps in the conduct of crime are the same. The difference of the two approaches is where the emphasis of effort is placed: in victim-oriented approach the role of preparation and reconnaissance plays a more significant role, whereas in the attack-method oriented approach the development of specific attack vectors and tools is more prominent.

The preparation phase includes everything concerned with planning the commission of crime. The specific steps in this phase encompass:

- identifying the victim(s),
- conducting research and reconnaissance on chosen target,
- developing an attack plan (including deciding the preferred attack vector(s)), and,
- assessing available capabilities (either own, or those that can be bought or outsourced from criminal markets and fora).

Preparation is a continuous process of getting ready to conduct the crime, with several feedback loops. The reconnaissance step may also reveal new or additional potential criminal opportunities. This means the criminals may change the focus of the crime, decide to conduct more crimes in addition to the original crime (resulting in a more complex crime), or abandon their preliminary idea altogether. The preparation phase may be conducted using either legal or illegal means: either by conducting simple internet research of social media, websites, conference proceedings, etc.; or by conducting port scans, searching for information on technical or organisational weaknesses.

As proposed in **Publication I**, the preparation phase has two main components. Firstly the major decision point is the actual conscious decision to attempt to conduct a crime. As a first step, a "market research" is undertaken in the sense of determining and weighing the risks, costs and benefits of the options available to them. The criminals may find that risks or costs outweigh potential benefits and may decide not to conduct the crime. They may also find that there are additional opportunities, which they had not considered before, stemming from their research of target(s). At the same time, it must be noted that the criminals might not consider potential outcomes systematically at all and will act opportunistically.

The second component of the preparation phase concerns the identification of the potential victims. This includes exploring their potential technical, organisational and social vulnerabilities by conducting both online and offline reconnaissance. In this step, based on previous information gathering on targets, the criminals assess the capabilities needed to conduct this particular crime. They may possess the required capabilities themselves, or they may need to find capabilities from elsewhere. In the latter case the options available include either purchasing the capabilities from another criminal, or outsourcing the conduct of the crime. The preparation phase concludes with making a final conscious decision to continue the execution of the criminal act, and deciding on the attack methods and tactics to be used.

Publication V suggested that the two components of the preparation phase can be decomposed into four major steps: pre-attack planning, reconnaissance, attack plan, and capabilities assessment with each of these further sub-divided as depicted on Figure 25. The preparation phase ends when the criminal is ready to engage in criminal activity and is able to move on to the next stage of commissioning the crime. The steps in preparation for the crime will have a different emphasis in the case of targeted or non-targeted attacks. Preparation phase, depicted in Figure 25, is to some extent always present in a crime process, and this phase is where it is usually decided how a crime will be commissioned.

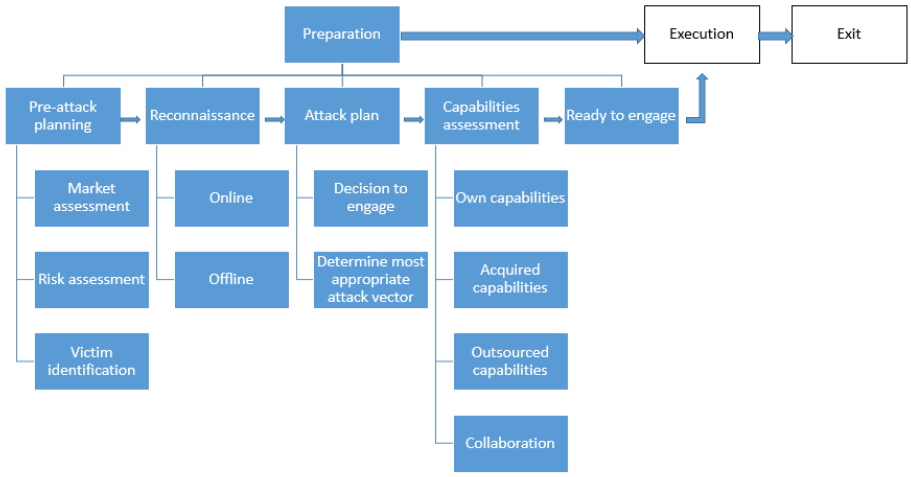

*Figure 25. Elements of preparation phase of cyber crime (adapted from **Publication V**)*

The pre-attack planning step usually involves a process of analysis around the question "Is it worth it?". The criminals conduct a market assessment to decide whether it is worth buying or outsourcing the required enabling capabilities (e.g. CaaS, Botnet development, Malware development, etc.). Further, they conduct a risk assessment in order to determine if the potential proceeds from commissioning the crime outweigh the risk from law enforcement actions (i.e. getting caught and legal actions). The risk assessment is a very important step within a crime process, and one where commission of crime may be prevented. In cases where the risks outweigh benefits, the crime might not take place. As the last pre-attack planning sub-step, they identify target victim.

In the reconnaissance step, the criminals will research their chosen target by either legal or illegal means. The aim of this step is to find any and all available weaknesses in the chosen victims: either people-related, organisation-related or technology-related. An important part in many cases of cyber crime is identification of weaknesses by the conduct of a simple social or technical information gathering. Social information gathering is conducted by simply exploring the internet: social media or traditional media, other websites, social or professional relationships, etc. In gathering information on organisational weaknesses, the criminals look into information available on the organisation's inner workings and standard procedures, in order to make use of potential weaknesses of processes. The aim of gathering technical information is to discover any critical technical elements stemming from technology, i.e. network architecture, IP address space, network services, e-mail format, and (security) procedures. In doing so, the criminals will attempt to find vulnerabilities in the victim IT systems. Researching the target (IT) systems is not relevant in some cases of more technically-focussed cyber crime, but generic research relating to the common characteristics will be important (e.g. developing malware, botnets, other relevant capabilities, or in cases of non-targeted attacks).

The next step in the process is developing an attack plan. Most criminals do not write down, or are even aware of this step, but it is a very important decision point within overall crime process. In this step, the criminals make a final decision to conduct a crime and determine the most appropriate attack vector for use.

The capabilities assessment step will be one in which the criminals identify if they have the capabilities needed for the crime themselves, or abilities to develop such capabilities, or whether there are possibilities to acquire capabilities, outsource the crime itself, or collaborate with other criminals to conduct a wider crime. Once all the steps in preparation phase are concluded, the criminal will be ready to move on to next phase within a crime process: execution.

The process model for the preparation stage of a cyber crime is depicted on *Figure 26*. It must be noted that it is not a simple and linear process, but the criminal may also move laterally within this phase. In addition, when additional opportunities are identified during any one of the steps, the criminals will repeat other preparatory steps as needed.

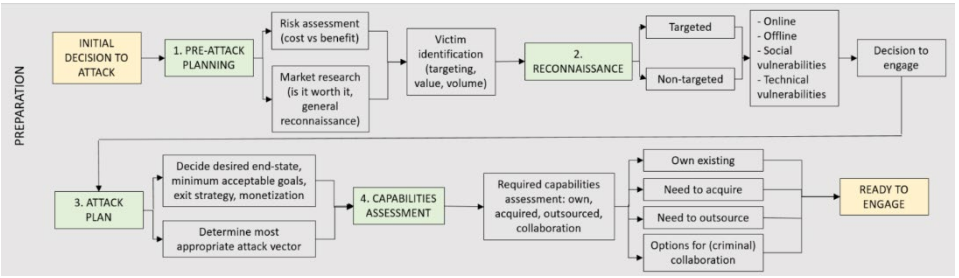

Figure 26. JMAP model: process mapping of preparation phase of a cyber crime

5.2.2 Execution phase

The execution phase starts where the preparation phase ended: the attack plan. In this plan the criminals make decisions on the desired end-state of the crime, minimum acceptable goals, as well as monetization and exit strategies. The attack can be executed in three ways: using own means and capabilities, buying these from other criminals, or outsourcing the crime.

In case where the criminal has the required means and capabilities himself, the other players within a criminal ecosystem do not play a significant role. In such case, the criminal moves on to the Execution phase and conducts the actual execution of the crime directly. In case he does not possess required capabilities, he will choose one of the other options possible. They may acquire required means and capabilities from another criminal. In this case the criminal ecosystem plays an enabling role: there are sellers/ brokers/ deal-breakers, developers, programmers, etc. Another enabling factor in this process is the specific forums, markets and online stores where such “goods” are traded. Alternatively, the criminals may outsource the whole crime, also making use of the criminal ecosystem and forums, markets and online stores. This is Crime-as-a-service model, where the criminal pays another criminal to conduct the crime.

As presented in Section 5.2.1, the attacks can be either targeted or opportunistic. The aim of conducting a cyber crime could be, among others,:

- data theft;
- extortion;
- online financial activity;
- breakdown, interruption or incorrect operation of services or infrastructure;
- theft or hijacking of computing power/ processing capacity;
- theft of information, secrets, intellectual property or knowledge;
- manipulation of information.

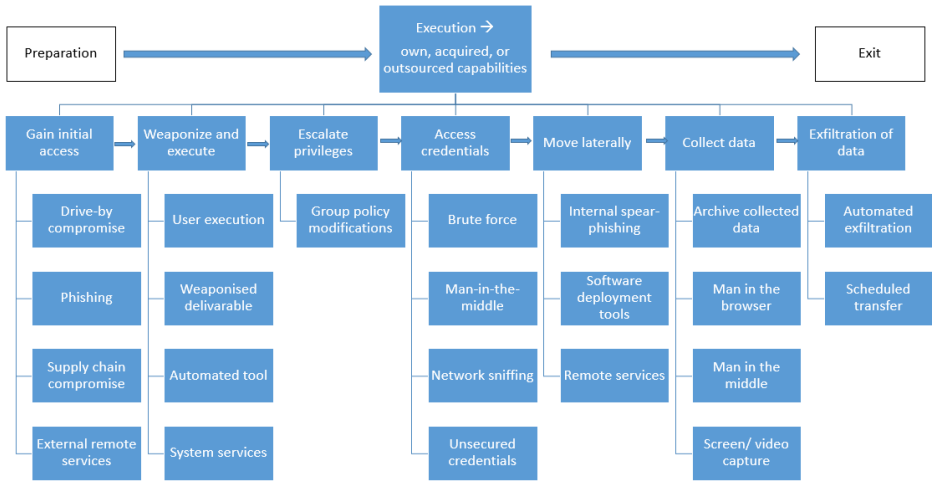

*Figure 27. Elements of execution phase of cyber crime (adapted from **Publication V**)*

As suggested in **Publication V,** there are many steps involved in the execution phase (see Figure 27).

As a first step, the criminal should gain access to the target systems. In order to accomplish this, the criminal will make use of social engineering and/ or available attack vectors (e.g. malware, drive-by downloads, user actions, etc.). The requirement for a specific attack vector will be decided during the conduit of reconnaissance and attack plan, and will depend on specific vulnerabilities related to people, organisation or technology.

Next, the criminal will enter/ interface with target system. Once access to victim systems and devices is gained, the criminal will map the network, escalate privileges, and access credentials. This will allow the criminal to enter or interface with the target system based on their desired and decided goals and end-states. Having accessed the system or device, the criminal may move laterally within the system or device, and when additional (criminal) opportunities present themselves, may change course or conduct multiple crimes. The final step of execution phase is conducting the attack/ crime, aimed at collection and exfiltration of data, DDoS, defacement, or otherwise incurring damages on the victim.

The execution phase is very complex and consists of a number of steps: gaining initial access, execution, privilege escalation, credential access, lateral movement, data collection, and exfiltration [88]. Each of these steps will have sub-steps, which might have sub-steps themselves. These technical steps and aspects of executing an attack have

been researched by both scholars and practitioners extensively (see e.g. [49] [20] [23] [44] [21] [47] [88] [104] [50] [46] [53]). Therefore, they will not be discussed in detail here. The purpose of developing a model for financially motivated cyber crime is to present a sense of processes the crime goes through, and not research each step in detail. The overall process model of the execution phase is presented in Figure 28.

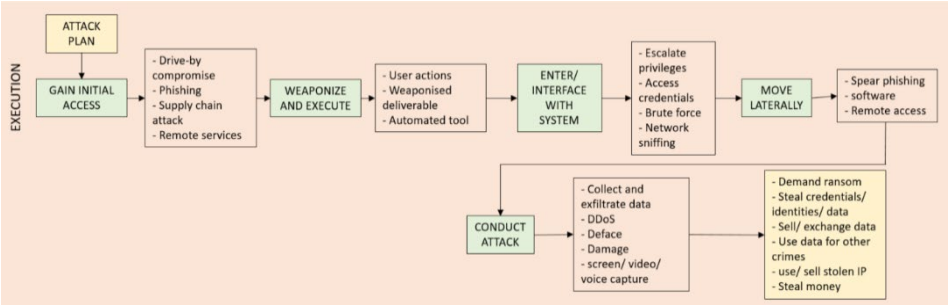

Figure 28. JMAP model: process mapping of execution phase of cyber crime

5.2.3 Exit phase

The most commonly perceived aim of all cyber crime is financial gain. Yet, our knowledge about criminal revenue generation is limited and fragmented [14]. There are many avenues for generating revenue: illicit online markets, sale of IP and trade secrets, data trading, crimeware and CaaS, malware, botnets, etc. As proposed in **Publication V,** the exit phase of a cyber crime consists of three principal steps: monetising the attacks, hiding tracks, and using revenues (Figure 29).

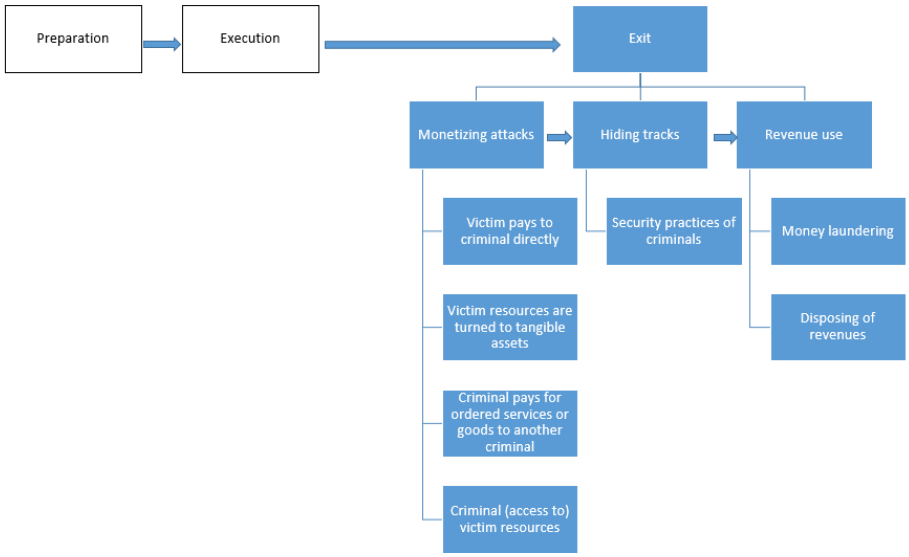

*Figure 29. Elements of exit phase of a cyber crime (adapted from **Publication V**)*

Financial gain from crimes can be generated in four principal ways. First, and most widely known is in the cases of extortion (e.g. utilising ransomware or DDoS extortion schemes), with victim paying the criminal directly. Secondly, the criminals can turn illegally obtained victim resources to tangible assets, which are subsequently traded and sold. Third, using the cyber criminal ecosystem, one criminal will pay another criminal for goods and/ or services obtained at dedicated marketplaces and forums (which could be considered as a way to circumvent the necessity of money laundering). Such payment can be conducted in hard currency, crypto currency, re-sellable money equivalents (e.g. gaming assets, loyalty points), or in goods and services (real or virtual, legal or illegal). Fourth, the criminal may sell access to victim resources to other criminals. Similar to above, this trade utilises the criminal ecosystem and marketplaces, and payments are conducted in all means available. A further option is to buy, sell or barter other – legal or illegal – goods and services in dark markets, and thereby support further cyber or traditional crime. It must be noted, however, that the above four options may not be the only ones, as criminals keep innovating and finding new ways of generating gain from cyber crime.

Having conducted a successful cyber crime, the criminals take steps to hide any tracks to evade getting caught and prosecuted by law enforcement authorities. This is achieved by using several security practices [19] focussed on (but not limited to) protection and anti-forensics.

Gaining revenue is only one aspect of generating income from cyber crime. In order to make use of this revenue, it must be converted to usable assets or currency. Finding ways to conduct money laundering has been a problem for criminals in the offline world for a long time, and finding innovative methods for this has been a challenge for as long as crime has existed [14]. Consequently, the emergence of the digital economy has also brought about new forms of money laundering (sometimes referred to as cyber-laundering) involving digital payments, cryptocurrencies, mobile payments, etc. [14]. Traditional money laundering is used by cyber criminals: e.g. legal banking system, fake businesses, investments into assets, gambling and casinos, wire transfers, money mules or cash drops [14]. Another layer on the traditional laundering is the use of crypto currency, which provides additional security for criminals

There is little empirical evidence on how cyber criminals, or indeed offline criminals, spend their revenues. Some researchers have attempted to gain an insight to this. Research conducted recently [14] analysed available data (interviews, as well as dark web and open web sources), which suggested that cyber criminals use their proceeds similar to offline criminals [14] [107]. They use their income for covering daily expenses (paying bills, buying food, etc.), but much of the income generated is also spent on hedonistic pursuits (e.g. buying drugs, luxury items, prostitution), or to gain status (e.g. buying luxury items, art, other collectibles). An additional use of criminal revenue is further reinvestments into crime, or investments to additional criminal opportunities through corruption [107]. However hedonistic their lifestyles, some criminals also consider the need to retire and therefore conduct more calculated spending, e.g. savings on bank accounts or investments in property or financial assets [107].

Turning cyber crime proceeds into real assets of value, or tangible currency, is challenging for criminals. In order to turn criminal proceeds to tangible assets, the criminals use special enablers brought about by the emergence of digital economy: cryptocurrencies and specialised web portals offering the sale of property, cars, luxury items, etc., for cryptocurrencies [14]. Criminal proceeds may be used in seemingly

legitimate ways such as investments to legitimate economies by creating enterprises or investing in existing ones, or sponsoring various events [107].

In the exit phase, the criminals hide their tracks. In order to do that, there are a number of countermeasures they employ throughout all phases of the crime process: preparation, execution, and exit. The majority of the security practices they use are of technical nature. However, there are other practices, most notably corruption, which are used to evade prosecution. By the end of the exit phase, and the overall financially motivated cyber criminal cycle, the criminals have generated financial gain of some kind, and the cyber criminal process has come to a close. However, the criminals may also reinvest their proceeds into further crime, which will be the start of another process of crime. The process of exit phase of a cyber crime is depicted below in Figure 30.

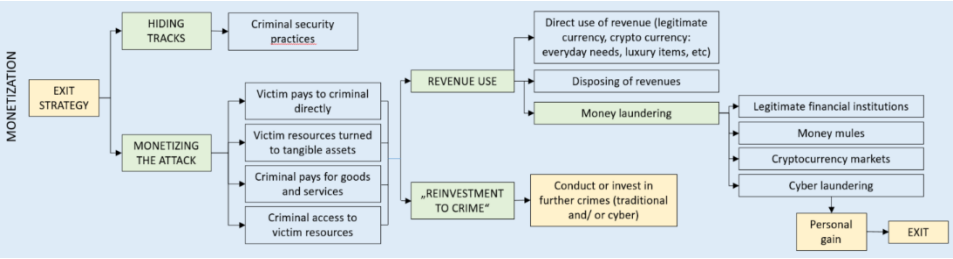

Figure 30. JMAP model: process mapping of exit phase of cyber crime

6 Conclusions and future work

6.1 Summary and conclusions

This thesis addresses financially motivated cyber crime. The main contribution of this dissertation is to present a Criminal JMAP model for financially motivated cyber crime as a process. The validation process indicates that the JMAP model developed is a practical tool, which can be used by various stakeholders in the cyber crime investigation, prevention and countermeasure development process. This work contributes to the existing knowledge of cyber crime by providing a mapping of step-by-step account of actions taken by the criminals throughout the crime. It is not intended to be a rigid or linear process but a flexible mechanism to understand the key steps within a cyber crime process, allowing the identification of pinch points the criminals pass through. An important practical implication is that the JMAP model can assist in understanding cyber crime across the various players involved in the cyber crime investigation process. This information can be used to develop targeted interventions aimed at reducing cyber crime. The aim is to allow those investigating cyber crimes or developing countermeasures to quickly apply new crimes to the model and vice versa – and focus on the specific known (or unknown) pinch points in order to conduct their work more effectively.

The main research question of this dissertation was: how to model the process of financially motivated cyber crime? This was answered by three main research questions, followed by sub-questions, which sought to address related aspects.

In the introduction an overview of the cyber crime problem was given, together with the need for modelling financially motivated cyber crime. Chapter 2 provided an overview of related work and background of cyber crime in general and financially motivated cyber crime in particular.

Chapter 2 answered research questions 1 and 2 by analysing the currently available definitions and taxonomies. In the analysis, it became apparent that there is no universally accepted definition or taxonomy for cyber crime. The two issues studied – definition and taxonomy – are interrelated. In an attempt to conceptualise the cyber criminal process, the underlying question after research was: how to provide a taxonomy, which would give better insight into and understanding of cyber criminal processes, reflecting all possible steps a criminal passes through and the decision points within that process?

Chapter 3 gave an overview of the methodology used. Grounded Theory methodology was chosen because it derives theory from data, not the other way around. It can be used with (sometimes) incomplete data, and it has been used in computer science and cyber crime research previously. The process of collecting data, generating/ updating the JMAP model, and validating the JMAP model was reiterated once every year, with each validation event providing further interesting details into the development of the model. The chapter further provided details and overview of expert assessment as used in validation.

Notwithstanding the difficulties in creating a definition and taxonomy, and building on work of previous analysis, Chapter 4 proposed a new definition of financially motivated cyber crime. It also proposed a taxonomy for use in the modelling of financially motivated cyber crime. The author acknowledges that both the proposed definition and taxonomy may be too broad and too overarching and it is suggested that any follow-on work on modelling specific cyber crime instances should provide their own definition and

taxonomy, depending on the emphasis and aspect of crime studied. Chapter 4 also provided an overview of economic perspectives and the cyber criminal ecosystem.

Chapter 5 answered research question 3 by exploring the currently available models used to describe cyber attacks or cyber crime, and looked at how these existing models can be adapted to model the process of financially motivated cyber crime. Chapter 5 discussed crime scripting, phase-based approach and journey mapping and found that these can be adapted to model the process of financially motivated cyber crime. As the main result of the current thesis, Chapter 5 presented a Criminal JMAP model for financially motivated cyber crime. The developed Criminal JMAP model looked at a crime from the criminals' perspective. This provides an insight into the specific metaphorical gates the criminals pass through within a crime process. Further principles of crime scripting were used to deconstruct a crime to small component parts to understand all phases and steps a criminal passes through during a crime. The aim of modelling was to present a general process model, which can be used to deconstruct cyber crime and improve general understanding of the modus operandi of criminals.

Most studies in the field of cyber security have focussed on technical execution, human factors, money laundering or victimisation. These studies have been conducted by either academics or practitioners, i.e. security providers or LEAs. The current dissertation has offered an interdisciplinary approach to developing a model, drawing on social sciences and criminology. Criminology itself is an interdisciplinary field of study drawing on social sciences and the research in sociology, political science, psychology, economy, and law. The investigation of definitions and taxonomies used currently showed that to date there has been little agreement on what cyber crime is: there is no universally accepted definition, ontology or taxonomy applicable to the field of cyber crime. Returning to the main research question, the current dissertation has proposed a model to map the processes of financially motivated cyber crime. The Criminal JMAP model is based on a proposed definition and taxonomy, utilising an interdisciplinary approach. Traditionally non-cyber concepts from journey mapping, phase-based approach and crime scripting were used to develop a process model for the currently predominantly technical understanding of cyber crime. The relevance of the Criminal JMAP model is clearly supported by results of the validation process. The most obvious finding to emerge from validating the JMAP model is that it is useful in the provision of training to LEA officers, but also in providing insight to (organised) cyber crime, which relies heavily on processes.

The current dissertation extends our knowledge of cyber crimes as a process. The work contributes to existing knowledge by developing a process model for financially motivated cyber crime. The current work adds to a growing body of literature on utilising crime scripting methods to analyse cyber crime. Additionally, the work has looked at cyber crime from criminals' perspective, utilising the journey mapping methodology.

Despite its exploratory nature, this dissertation offers some insight into cyber criminal processes. Although the work is based on a relatively small sample of cyber crime acts, the findings suggest there is utility in modelling the processes of cyber crime. The research has several practical implications. The Criminal JMAP model developed can be modified and further detailed for specific crimes. Such representation of a sequence of events constituting a cyber crime can provide novel insights to forensic analysts, incident response teams and law enforcement agencies. Such modelling can help to facilitate the development of prevention efforts, but also aid the identification and development of countermeasures. The approach and the Criminal JMAP model proposed

is useful to various organisations as it can aid in their decision processes and in their efforts to fight cyber crime.

Finally, although this study has successfully demonstrated that a Criminal JMAP model for financially motivated cyber crime can reflect cyber criminal processes, a number of limitations must be considered. First, the study was limited by secondary data sources on cyber crime, as the research purpose was on modelling cyber criminal processes. For this reason, secondary sources were considered sufficient and reliable. However, practitioners from LEAs were consulted throughout this research in order to mitigate this limitation, mainly by gaining insight to applicability and relevance of model at validation events. Secondly, the current study did not look in detail to cyber criminal business models. This may provide additional insight to the processes of cyber crime within a changing cyber security environment, which could provide insights for potential future research and make the model even more useful in analysing cyber crime as an economy. These limitations provide insights for potential future research and could make the model more useful in pursuit, prevention, preparation and protection.

6.2 Future work

The author acknowledges that even though this dissertation is significant in proposing a Criminal JMAP model for financially motivated cyber crime, it can and should be developed further. As the principles of Grounded Theory methodology state, the developed theory should be constantly updated and re-validated. This is especially true in a subject like cyber crime – which is a dynamic, innovating and constantly changing process. In order for the JMAP model to remain up-to-date and relevant, new developments should be validated as they become known.

Future work should also research aspects listed as limiting factors of current research. Firstly, detailed information on real cyber crimes, and not only secondary data, should be used to populate the JMAP model in order to validate its use in LEA work, or developing preventive actions and countermeasures. Second, cyber criminal business models should be researched and mapped into the JMAP model. This could provide additional information of major decision points and risk factors for conducting a crime, thereby providing insights on where to focus action in the fight against cyber crime. Thirdly, it would be important to move on from mapping criminals' actions only. Victims (including past and potential victims) and their actions should be mapped into the (Victim) JMAP model, reflecting the interaction points between victims and criminals in order to find potential novel options to deter cyber criminals. It is also suggested that future work look into the economic aspects and cyber criminal ecosystem and map these to the JMAP model. The work on mapping victim aspects has already started, and it has become obvious that such mapping, in combination with economic aspects from criminals' view, will provide further nuances on the macro and micro factors influencing cyber crime.

Future work could also use the JMAP model developed as a basis for developing training programs, as a quick introduction to this new type of crime. The author has started this work, in developing specialised training programs for law enforcement.

The Criminal JMAP model can also be used to help experiment via virtualised or desktop exercises on cyber ranges. These may focus on the application of countermeasures at various points along the cyber criminal process, with the goal of taking forward the most effective ones for application in real world scenario. In much the same way, the JMAP model can be used in developing public policy or new legislative measures in the fight against cyber crime.

List of figures

List of tables

Bibliography

[1] M. Watin-Augouard, *Le cyberespace n'a pas de frontière : sa sécurité est l'affaire de tous,* Paris, 2010.

[2] Statista, Internet usage worldwide - Statistics and Facts.

[3] R. V. Clarke, Situational crime prevention: successful case studies, R. V. Clarke, Ed., Harrow and Heston, 1997.

[4] S. Kaplan, Y. Y. Haimes and J. B. Garrick, "Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of a risk," *Risk Analysis,* vol. 21, no. 5, 2002.

[5] R. Willison, "Applying Situational Crime Prevention to the Information Systems Security Context," in *Perspectives on Identity Theft*, Criminal Justice Press/Willow Tree Press, 2008, pp. 151-167.

[6] M. Corcoran, Interviewee, *Cyber criminal ecosystems. Cyber criminal processes.* [Interview]. 06 July 2018.

[7] M. Corcoran, Interviewee, *understanding and modelling cyber crime.* [Interview]. 15 July 2018.

[8] B. Focus group discussion, Interviewee, *Mapping cyber criminal journeys.* [Interview]. October 2019.

[9] L. Focus group discussion, Interviewee, *Understanding cyber crime.* [Interview]. 18 March 2017.

[10] S. Warren, G. Oxburgh, P. Briggs and D. Wall, "How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?," in *International Conference on Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292*, 2017.

[11] T. Watson, Interviewee, *Understanding cyber crime.* [Interview]. 12 July 2018.

[12] A. U. c. c. investigator, Interviewee, *Cyber crime investigation.* [Interview]. 18 March 2017.

[13] T. H. Ilves, *Rebooting Trust? Freedom vs Security in Cyberspace,* Munich Security Conference, 2014.

[14] M. McGuire, Into the Web of Profit: Understanding the Growth of the Cybercrime Economy, Bromium, Inc, 2018.

[15] J. Corbin and A. Strauss, Basics of Qualitative Research: Techniques and Procedures for developing Grounded Theory, 4 ed., Sage, 2015.

[16] J. Engelbrecht and R. Kitt, *Complex Systems: the whole is bigger than the sum of parts,* Postimees Kirjastus, 2020.

[17] International Labour Office, Management Consulting: A Guide to the Profession, 4 ed., M. Kubr, Ed., Geneva, 2002.

[18] R. Anderson, A Guide to Building Dependable Distributed Systems, 2 ed., Wiley, 2008.

[19] E. Van de Sandt, *Deviant Security: The Technical Computer Security Practices of Cyber Criminals,* Bristol: University of Bristol, 2019.

[20] E. M. Hutchins, M. J. Cloppert and R. M. Amin, *Intelligence-Driven Computer Network Defense Informed by ANalysis of Adversary Campaigns and Intrusion Kill Chains,* Lockheed Martin Corporation, 2011.

[21] Hewlett Packard Enterprise, *HPE Attack Life Cycle Use Case Methodology. Technical White Paper,* HPE, 2016.

[22] Kaspersky Lab, "Russian financial cybercrime: how it works," 2015.

[23] D. Maimon and E. R. Louderback, "Cyber-Dependent Crimes: an Interdisciplinary Review," *Annual Review of Criminology,* pp. 191-216, 2019.

[24] H. Borrion and H. Dehghanniri, "Toward a More Structured Crime Scripting Method," in *IEEE 24th International Requirements Engineering Conference Workshops (REW)*, Beijing, 2016.

[25] E. Filiol, "Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct," in *Cyberwar and Information Warfare*, D. Ventre, Ed., Wiley, 2011.

[26] S. Ghernaouti, "Cyberpower: Crime, Conflict and Security in Cyberspace," EPFL Press, 2013.

[27] R. Raudla, *Lecture series "Research Methods in Social Sciences",* Tallinn: Tallinn University of Technology, 2019.

[28] B. G. Glaser and A. L. Strauss, The Discovery of Grounded Theory. Strategies for Qualitative Research., 2006 ed., Aldine Transsaction, 1967.

[29] K.-J. Stol, P. Ralph and B. Fitzgerald, "Grounded Theory in Software Engineering Research: A Critical Review and Guidelines," in *2016 IEEE/ACM 38th IEEE International Conference on Software Engineering*, 2016.

[30] N. Kshetri, The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives, Springer, 2010.

[31] Encycolpedia Britannica, [Online]. Available: https://www.britannica.com/topic/cybercrime. [Accessed 15 June 2018].

[32] E. Kraemer-Mbula, P. Tang and H. Rush, "The cybercrime ecosystem: Online innovation in the shadows?," *Technological Forecasting and Social Change,* vol. 80, no. 3, pp. 541-555, 2013.

[33] R. Barn and B. Barn, "An ontological representation of a taxonomy for cybercrime," in *Twenty-Fourth European Conference on Information Systems*, Istanbul, 2016.

[34] S. W. Brenner, "Is There Such a Thing as "Virtual Crime"?," *California Criminal Law Review,* vol. 4, 2001.

[35] European Commission, "Towards a general policy on the fight against cybercrime," EC, Brussels, 2007.

[36] Council of Europe, "Convention on Cybercime," 23 November 2001. [Online]. Available: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561. [Accessed 21 January 2015].

[37] United Nations, "The United Nations Manual on the Prevention and Control of Computer Related Crime," New York, 1994.

[38] INTERPOL, 2016. [Online]. Available: https://www.interpol.int/Crimes/Cybercrime. [Accessed 15 July 2016].

[39] D. Wall, Cybercrime, Cambridge: Polity Press , 2007.

[40] Bundeskriminalamt, "Internet Crime," [Online]. Available: http://www.bka.de/nn_194550/EN/SubjectsAZ/InternetCrime/internetCrime__node.html?__nnn. [Accessed 17 Nov 2015].

[41] Police and Border Guard Board, Estonia, [Online]. Available: https://cyber.politsei.ee/questions. [Accessed 15 May 2020].

[42] UK Home Office, *Cyber Crime Strategy,* 2010.

[43] C. E. Landwehr, A. R. Bull, J. P. McDermott and W. S. Choi, "A taxonomy of computer program security flaws, with examples," in *ACM Comput Surv*, 1994.

[44] J. D. Howard, "An analysis of security incidents on the internet, 1989-1995," Carnegie-Mellon University, Pittsburgh, Pennsylvania, 1997.

[45] J. D. Howard and T. A. Longstaff, "A Common Language for Computer Security Incidents," Sandia Nationa Laboratories, 1998.

[46] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Computers and Security,* vol. 24, pp. 31-43, 2005.

[47] M. Kjaerland, "A classification of computer security incidents based on reported attack data," *Journal of Investigative Psychology and Offender Profiling,* vol. 2, no. 2, pp. 105-120, 2005.

[48] C. Meyers, S. Powers and D. Faissol, "Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches," Lawrence Livermoore National Laboratory, 2009.

[49] C. B. Simmons, S. G. Shiva, H. Bedi and D. Dasgupta, "AVOIDIT: a cyber attack taxonomy," in *9th Annual Symposium of Information Assurance (Asia '14)*, Albany, New York, 2014.

[50] M. Rogers, *A new hacker taxonomy,* University of Manitoba, 1999.

[51] M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors," *Computers and Security,* vol. 25, pp. 522-538, 2006.

[52] M. Rogers, *A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study,* University of Manitoba, 2001.

[53] M. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," *Digital Investigation,* vol. 3, no. 2, pp. 97-102, 2006.

[54] A. Alkaabi, G. Mohay, A. Mccullagh and N. Chantler, "Dealing with the problem of cybercrime," in *2nd International ICST Conference on Digital Forensics & Cyber Crime*, Abu Dhabi, 2010.

[55] S. Furnell, "The Problem of Categorising Cybercrime and Cybercriminals," in *2nd Australian Information Warfare and Security Conference.*, Perth, Australia, 2001.

[56] Australian Federal Police, *Fighting the Invisible,* Platypus: Journal of the Australian Federal Police 2, 2003.

[57] C. Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* U.S. Congressional Research Service, 2008.

[58] Foreign Affairs and International Trade, Canada, “Foreign Affairs and International Trade, Canada,” 2004. [Online]. Available: http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp. [Accessed 2 June 2015].

[59] M. McGuire and S. Dowling, “Cyber Crime: A review of the evidence. Research Report 75,” UK Home Office, 2013.

[60] S. Gordon and R. Ford, “On the definition and classification of cybercrime,” Springer, 2006.

[61] M. D. Goodman, “Why the police don't care about computer crime,” *Harvard Journal of Law and Technology,* vol. 10, no. 3, 1997.

[62] S. Ghernaouti, Cyberpower: Crime, Conflict and Security in Cyberspace, EPFL Press, 2013.

[63] S. Moitra, “Developing policies for cybercrime,” *European Journal of Crime Criminal Law and Criminal Justice,* vol. 13, no. 3, pp. 435-464, 2005.

[64] Council of Europe, “Chart of signatures and ratifications of Treaty 185,” [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=nuzO1lQv. [Accessed 02 july 2020].

[65] J. Corbin and A. Strauss, “Grounded Theory Research: Procedures, Canons and Evaluative Criteria,” *Qualitative Sociology,* vol. 13, no. 1, 1990.

[66] K. Charmaz, Constructing Grounded Theory. A practical Guide through Qualitative Analysis, Sage, 2006.

[67] T. Sõmer, R. Ottis, T. Lepik , M. Lagazio, B. Hallaq, D. Simms and T. Mitchener-Nissen, “The Economic Impacts of Cyber Crime, FP7-SEC-2013.2.5-2. D2.3 Detailed appendixes on cyber crime inventory and networks in non-ICT sectors.,” 2015.

[68] CERIS, "*Centre Européen de Recherches Internationales et Stratégiques” research guide,* Brussels, 2007.

[69] N. Schwarz, H. Bless and G. Bohner, “Mood and Persuasion: affective states influence the processing of persuasive communications,” *Advances in Experimental Social Psychology,* no. 24, pp. 161-199, 1991.

[70] K. Moser and G. Kalton, Survey Methods in Social Investigation, 1 ed., Routledge, 1971.

[71] V. Braun and V. Clarke, *Using Thematic Analysis in Psychology,* 2006.

[72] United Nations, *Cybercrime Study,* New York: United Nations, 2013.

[73] Oxford Reference Online, “Oxford Reference Online,” 2019.

[74] E. Filiol, “Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct,” in *Cyberwar and Information Warfare*, D. Ventre, Ed., Wiley, 2011.

[75] R. Broadhurst, P. Grabosky, M. Alazab, B. Bouhours and S. Chon, “Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime,” *International Journal of Cyber Criminology,* vol. 8, no. 1, pp. 1-20, 2014.

[76] L. Ablon, M. C. Libicki and A. M. Abler, “Markets for Cybercrime Tools and Stolen Data,” RAND Corporation, 2014.

[77] BAE Systems Detica and London Metropolitan University, “Organised Crime in the Digital Age,” London, 2012.

[78] European Police Office, “The internet Organised Crime Threat,” European Cybercrime Center, 2014. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014. [Accessed 5 september 2015].

[79] J. Hawkey, Exit Strategy Planning: Grooming Your Business for Sale Or Succession, Hampshire: Gower Publishing Limited, 2002.

[80] M. Castells, The Information Age: Economy, Society, and Culture. Volume I: The Rise of the Network Society, 2 ed., Wiley-Blackwell, 2010.

[81] A. Smith, An Inquiry into the Nature and Causes of the Wealth of Nations, Project Gutenberg, 2019.

[82] United Nations Office on Drugs and Crime, *The Globalisation of Crime: A Transnational Organized Crime Threat Assessment,* 2010.

[83] M. Iansiti and G. L. Richards, “The information technology ecosystem: structure, health and performance,” *Antitrust Bulletin,* vol. 51, no. 1, pp. 77-110, 2006.

[84] J. F. Moore, The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems, New York: Harper Business, 1996.

[85] J. Raab and B. Milward, “Dark Networks as Problems,” *Journal of Public Administration Research and Theory,* vol. 13, no. 4, pp. 413-439, 2003.

[86] O. Gross, “Eesti Päevaleht,” 03 February 2020. [Online]. Available: https://epl.delfi.ee/artikkel/92447271/kuidas-meili-teel-kaotada-20-aastat-kogutud-saastud-kuberkuritegevust-on-uha-rohkem?fbclid=IwAR1fsskxDDGTkhv1m0N4ALcSAU6SHL2glwZ7bixkbPLQRGXGTn1s822D43k. [Accessed 03 February 2020].

[87] R. Wasserstein, *George Box: A Model Statistitian,* 2010: Royal Statistical Society.

[88] MITRE Corporation, *ATT&CK Matrix for Enterprise,* MITRE Corporation.

[89] G. Bernard and P. Andritsos, “A Process Mining Based Model for Customer Journey Mapping,” in *International Conference on Advanced Information Systems Engineering*, 2017.

[90] Riigikantselei, “Riigikantselei innovatsioonitiim,” [Online]. Available: https://www.riigikantselei.ee/et/innovatsioonitiim. [Accessed 13 December 2019].

[91] M. Stickdorn, M. E. Hormess, A. Lawrence and J. Schneider, This Is Service Design Doing: Applying Service Design Thinking in the Real World, O'Reilly Media Inc., 2018.

[92] U.S. Department of Defense, “Joint Publication 3-60 Joint Targeting,” 2007. [Online]. Available: https://www.aclu.org/files/dronefoia/dod/drone_dod_jp3_60.pdf. [Accessed 25 September 2016].

[93] U.S. Department of Defence, “Joint Publication 3-13 Information Operations,” 2006. [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

[94] J. Tirpak, *Find, Fix, Track, Target, Engage, Assess,* Air Force Magazine 83, 2000.

[95] T. Sakuraba, B.-H. Chou, S. Domyo and K. Sakurai, “Exploring Security Countermeasures along the Attack Sequence,” in *2008 International Conference on Information Security and Assurance (isa 2008), 2008*, 2008.

[96] R. Willison and M. Siponen, *Overcoming the Insider: Reducing Employee Computer Crime through Situation-al Crime Prevention.*

[97] R. C. Schank and R. P. Abelson, "Scripts, plans, goals and understanding, an inquiry into human knowledge structures," Hillsdale, NJ, Lawrence Erlbaum Associates, 1977.

[98] H. Borrion, "Quality assurance in crime scripting," *Crime Science,* 2013.

[99] H. Brayley, E. Cockbain and G. Laycock, "The Value of Crime Scripting: Deconstructing Internal Child Sex Trafficking," *Policing: A Journal of Policy and Practice,* vol. 5, no. 2, pp. 132-143, 2011.

[100] B. Leclerc, "12 New developments in script analysis for situational crime prevention," in *Cognition and Crime: Offender Decision Making and Script Analyses*, 2013.

[101] P. Ekblom and M. Gill, "Rewriting the Script: Cross-Disciplinary Exploration and Conceptual Consolidation of the Procedural Analysis of Crime," *European Journal on Criminal Policy and Research,* vol. 22, pp. 319-339, 2016.

[102] H. Borrion, H. Dehghanniri and Y. Li, "Comparative Analysis of Crime Scripts: One CCTV Footage - Twenty-One Scripts," in *2017 European Intelligence and Security Informatics Conference (EISIC)*, Athens, 2017.

[103] R. P. Abelson, "Script processing in attitude formation and decision making," in *Cognition and social behavior*, Hillsdale, NJ: American Psychological Association, 1976.

[104] D. Cornish, "The procedural analysis of offending and its relevance for situational prevention," *Crime Prevention Studies,* vol. 3, pp. 151-196, 1994.

[105] M. Levi and M. Maguire, "Reducing and preventing organised crime: An evidence-based critique," *Crime Law and Social Change,* vol. 41, no. 5, 2004.

[106] N. Leontiadis and A. Hutchings, "Scripting the crime commission process in the illiscit online prescription drug trade," *Journal of Cybersecurity,* vol. 1, no. 1, pp. 81-92, 2015.

[107] N. Leontiadis and A. Hutchings, "Scripting the crime commission process in the illicit online prescription drug trade," *Journal of Cybersecurity,* vol. 1, no. 1, pp. 81-92, 2015.

[108] P. C. van Duyne and M. Levi, Drugs and Money: Managing the Drug Trade and Crime-Money in Europe, Abingdon, U.K: Routledge, 2005.

[109] J. Bertin, Graphics and Craphic Information Processing, Berlin: Walter de Gruiter, 1981.

[110] S. A. a. L. Shih, "Towards and Interactive Learning Approch in Cybersecurity Education.," in *Proceedings of the 2015 Information Security Curruculum Development Conference*, New York, 2015.

[111] Security Affairs, "Security Affairs," 2016. [Online]. Available: https://securityaffairs.co/wordpress/50680/cyber-crime/global-cost-of-cybercrime.html. [Accessed 20 January 2017].

Acknowledgements

Aristotle has been attributed to saying “the whole is greater than the sum of its parts”, but as philosophers after him have concluded: sometimes the sum of parts is greater than the whole. These wise words were an inspiration for my dissertation.

Writing this dissertation has been an exciting journey, beginning with a look at the whole, dismantling the whole to its parts and drawing on a number of people too great to mention. First of all, I would like to thank my supervisors, Dr. Rain Ottis and Dr. Patrick Voss de Haan. You both have been instrumental to the completion of this work and I thank you for your support, advice and inspiration. Thank you Dr. Tim Watson from the University of Warwick who provided valuable guidance, shared opinions and supported this journey as informal advisor. A special thank you also to you, Bil Hallaq for providing constructive criticism and feedback, and for your cheerful attitude and positive feedback when most needed. I am very grateful to those of a wide range of international background, who provided brainstorming and opinions – the different administrative systems, cultures and backgrounds of all of you made this journey more significant and enjoyable. Thank you also to Mika and Adrian, for providing support and positive thoughts when feeling insecure about this undertaking. And finally, special thanks go to my family and loved ones – I could not have done this without your support.

This work would not have started without funding from the E-CRIME project (FP7; GA no. 607775). And last but not least, the work could not have been completed without the support of ICT Development Fund of the Estonian Ministry of Economic Affairs and Communications, IT Academy study measure and the support of Estonian Police and Border Guard Board.

Abstract

Modelling financially motivated cyber crime

The development of information and communications technologies have greatly affected the way societies, economies and people operate. Worldwide internet usage has increased from 1.7 billion users in 2009 to more than 4.1 billion users in July 2019. In addition to people, internet connectivity today extends to digital devices, with more things connected than people. According to reports, the number of internet connected devices reached 18 billion in 2018 and will be close to 50 billion in 2030. The internet and related technologies have provided opportunities and benefits but has also made everyone vulnerable to those who wish to attack them. Hacker groups, lone criminals and criminal organisations worldwide have access to powerful, evolving capabilities, which they use to identify and target their victims and commit cyber crimes. The reasons for this vulnerability are two-fold: first, governments, societies, businesses and individuals are ever more dependent on cyberspace; and second, our understanding of cyber crime remains limited.

Cyber crime is a relatively new area of academic research, and has led to both theoretical and practical interest in the subject. Researchers agree in general on the scope and scale of cyber crime and acknowledge the extent of the problem. What we know about cyber crime is largely based upon empirical studies on mainly technical aspects, and recently more attention has been focussed on the human factor. However, far too little attention has been paid to cyber crime as a process, which would include both technical and non-technical aspects. Cyber criminals are not a willing population of research; therefore most research has used limited data sets and secondary sources of information. This dissertation is no exception in this regard. Today, the technical aspects of executing cyber attacks) have been researched widely, but understanding the dynamic and constantly changing process, or system, of cyber crime has not received as much attention. Utilising interdisciplinary approach and traditionally non-computer science methods to understand cyber crime provides a different view on how they happen, thereby providing better options to investigate such activities, and find or develop new countermeasures and awareness building measures.

This thesis is based on a collection of published and cited publications that explore cyber crime, related definitions and taxonomies. It proposes a definition and taxonomy to map financially motivated cyber crime, and introduces a Criminal JMAP model to provide understanding of financially motivated cyber crime as a process.

Cyber criminals are increasingly using new technologies, but also developing novel techniques, procedures and business models for their criminal purposes. Cyber crime is a mirror of our contemporary economic system, often not only mirroring but out-innovating legitimate economies. Cyber criminals operate in the same manner as legitimate commercial networks with clearly established business objectives and trusted supply chains for services or products that require outsourcing or development. The cyber criminals know what they are looking for, what objectives they want to achieve and how to achieve these goals – and they are willing to spend time to research and plan their actions. Crimes can be seen as a process where resources are required and decisions are made that together constitute the modus operandi of a crime. Conducting cyber criminal acts requires preparation, planning and making rational choices and decisions along the way. Contrary to legitimate corporations, business choices and decisions are not explicitly written down as policies or procedures, rather they happen on an ad-hoc

basis. Yet analysing the different cyber criminal acts provides a pattern of underlying associated decision points and business processes.

Central to the work of this dissertation is the construction of a general financially motivated cyber crime process model, the JMAP model. In conducting this research, existing definitions and taxonomies were analysed. Research showed that the term cyber crime embodies a multitude of concepts which are based on different aspects of crime and a generally accepted definition of cyber crime in general and financially motivated cyber crime in particular, is lacking. For this reason, and in order to develop a general financially motivated cyber crime process model, the author proposed a definition and developed a new taxonomy. The need for a taxonomy to respond to cyber crime is a practical measure: without an understanding of cyber crime, meaningful investigative or responsive measures cannot be developed. The basis for the proposed taxonomy is the underlying criminal process, which includes the stakeholders (perpetrator and victim), capabilities (attack vectors), and enablers (monetization of crimes and the cyber criminal ecosystem). The developed taxonomy provides a basis to analyse and develop a better understanding of cyber crime as a process, where criminals and victims interconnect with each other and where attack vectors, enablers and exit strategies are analysed in a systematic context. Using such taxonomy to model financially motivated cyber crime is significant because it not only helps to develop an understanding of cyber crime business processes, but also how the tactics, techniques and procedures utilised by criminals function. The resultant JMAP model will lead to identifying pinch points in the cyber crime processes, help conduct more effective investigations, find better countermeasures, and develop novel policy, investigative, or technical approaches in the fight against cyber crime.

Grounded Theory methodology approach was used, as this is one of the most practical ways to build theory even from incomplete data. This methodology was deemed most suitable as the current research on cyber crime is limited and there are no theoretical frameworks to analyse cyber crime processes. One advantage of Grounded Theory lies in its flexibility, while still being structured. Grounded Theory does not focus on testing hypotheses taken from existing theoretical frameworks, but instead promotes the development of a theory of an action, process or interaction grounded in data collected. A central characteristic of Grounded Theory is simultaneous data collection, analysis and writing which are considered interrelated processes and are conducted in iterative manner, thereby grounding the resultant work in more theory.

Grounded Theory Methodology was used to generate high abstract categories of cyber crimes, and customer journey mapping was used to explain criminal intent and actions within a crime cycle. The dissertation also used this methodology to look at potential application of the model in answering the main research question: how to model the process of financially motivated cyber crime. This emphasises the most important point identified in interviews with policy-makers, law enforcement officers and technical cyber security experts: the need for understanding the complete cyber criminal process.

The main contribution of this dissertation is to present a structured, systematic and interdisciplinary study on cyber crime as a complex system. The proposed Criminal JMAP model for financially motivated cyber crime is one which is explanatory and has flexibility. The JMAP model developed by the author is a practical mechanism, which can be used by various stakeholders in the cyber crime investigation and prevention process. It provides a step-by-step account of actions taken by the criminals throughout the crime.

It is not intended to be a rigid or linear process but a flexible tool to understand the key steps within a cyber crime process, allowing the identification of pinch points the criminals have to pass through. This has the potential to overcome the challenges in understanding cyber crime encountered by the range of authorities involved in the investigative process. The aim is to allow those investigating cyber crimes or developing countermeasures to quickly apply new crimes to the model and focus on the specific known (or unknown) pinch points in order to conduct their work more effectively.

The JMAP model developed by the author was inspired mainly from crime scripting used in criminology, phase-based approach used in the military, and customer journey mapping used in economics. As there are no standard rules or symbols for such modelling, the author developed her own. By graphically presenting the sequence of events constituting a cyber crime, forensic analysts, incident response teams and law enforcement agencies will be able to identify the specific stages that cyber criminals pass through in committing their crimes. By modelling and understanding both general and specific cyber crimes, better oversight of existing countermeasures and potential development of new innovative countermeasures and disruption techniques can be formulated. The developed Criminal JMAP model can provide a sense of processes and practices through which cyber crime occurs (including both technological and organisational pathways), and has flexibility for use in wide range of cyber crimes. Applying the Criminal JMAP model to conditional and consequential matrix enables to analyse macro and micro relationships of situations, thereby providing an overview of macro, meso and micro factors influencing financially motivated cyber crime.

The author is fully aware of the ethical issues this dissertation might rise, in the sense of serving as a manual for criminals, in allowing them to “know what we know” about them. However, as can be seen from the history of cryptography from its early days, there are certainly some criminals who will benefit from such knowledge, but majority of them know and use this already. The law enforcement authorities will benefit from such knowledge much more. As pointed out throughout this dissertation, the increased understanding of cyber crime processes together with developed specific knowledge and skills of law enforcement agencies will increase effectiveness of investigations. In conclusion, the developed Criminal JMAP model for financially motivated cyber crime serves as a visualisation of underlying principles of cyber criminal processes to law enforcement, rather than being a manual for cyber criminals.

Lühikokkuvõte
Rahaliselt motiveeritud küberkuritegevuse modelleerimine

Info- ja kommunikatsioonitehnoloogia areng on tugevalt mõjutanud seda kuidas riigid, ettevõtted ja inimesed maailmas tegutsevad. Internetikasutus maailmas on kasvanud 1,7 miljardilt inimeselt 2009 aastal enam kui 4,2 miljardi kasutajani 2019 aastal. Lisaks inimestele, on internetiga ühendatud seadmed: erinevatel hinnangutel oli aastal 2018 internetti ühendatud seadmeid 18 miljardit ja aastaks 2030 ennustatakse seda arvu kasvavat 50 miljardini. Kui internet ning info- ja kommunikatsioonitehnoloogias annavad meile palju kasu ja loovad uusi võimalusi, seonduvad nendega ka ohud. Ohtude põhjuseid on peamiselt kaks. Esiteks, riigid, ühiskonnad, ettevõtted ja üksikisikud on aina rohkem sõltuvad küberruumist, ja teiseks meie arusaam ründajatest ja küberkurjategijatest on piiratud.

Küberkuritegevus on üsna noor teadusliku uurimise valdkond, mis on pakkunud huvi nii akadeemilisteks uuringuteks kui ka praktiliseks tegevuseks. Teadlased ja praktikud nõustuvad, et küberkuritegevus on suur ja kasvav probleem, kuid selle probleemi tegelikku olemust ei teata. Meie praegune teadmine küberkuritegevusest põhineb peamiselt tehniliste aspektide uurimisel, ning viimasel ajal on rohkem tähelepanu pööratud ka inimlikele aspektidele. Samas on liiga vähe tähelepanu pööratud küberkuritegevusele kui komplekssele süsteemile, milles oleks kokku viidud tehnilised ja mittetehnilised aspektid. Küberkurjategijad arusaadavalt ei soovi et neid uuritakse, seetõttu on teaduslikud uuringud põhinenud piiratud ja sekundaarsetel andmetel. Käesolev väitekiri ei ole selles osas erand. Nagu eelnevalt öeldud, on küberkuritegevuse (ja küberrünnete) tehnilisi aspekte uuritud laialdaselt, kuid arusaamad selle dünaamilistest pidevalt muutuvatest protsessidest ja komplekssusest ei ole olnud piisavalt tähelepanu all. Väitekirjas kasutatakse interdistsiplinaarset lähenemist ja arvutiteadustes traditsiooniliselt mitte kasutatavaid, sotsiaalteaduslikke meetodeid küberkuritegevuse mõistmiseks. Selline lähenemine annab erineva vaate küberkuritegevuse toimumisest, mis omakorda pakub täiendavaid võimalusi kuritegude uurimiseks ja ennetamiseks, vastumeetmete välja töötamiseks või teadlikkuse suurendamiseks.

Väitekiri põhineb avaldatud ning tsiteeritud publikatsioonidel, mis uurivad küberkuritegevust, selle definitsioone ja taksonoomiaid. Töös pakutakse rahaliselt motiveeritud küberkuritegevuse mudeldamiseks uus definitsioon ja taksonoomia, ning välja on töötatud JMAP mudel küberkuritegevuse kui protsessi kirjeldamiseks.

Küberkurjategijad kasutavad mitte ainult uusi tehnoloogiaid vaid töötavad välja innovaatilisi protseduure ja ärimudeleid kuritegelike eesmärkide saavutamiseks. Küberkuritegevus peegeldab meie igapäevast majandusmudelit, tihtilugu mitte ainult peegeldamise vaid ka innovaatilisema lähenemise läbi äri- ja majandusmudelitele. Küberkurjategijad tegutsevad samade printsiipide alustel kui legaalse majanduse ettevõtted ja üksikisikud: püstitades konkreetseid eesmärke ja planeerides nende elluviimist. Kuritegevuse majandusharus kehtivad pakkumise ja nõudluse reeglid, usalduslikud tarneahelad, turundamine, jne. Küberkurjategijad teavad mida nad vajavad, mida soovivad saavutada ning kuidas seda kõige efektiivsemalt saavutada – ning on valmis investeerima vajalikku tegevusse, ettevamlmistusse ning planeerimisse. Küberkuriteod on protsessid, mis vajavad ressursse ning kus tehakse erinevatel etappidel otsuseid: oluline on teostada ettevalmistavaid tegevusi, planeerida terviklikku protsessi ning vastu võtta ratsionaalseid otsuseid. Vastupidiselt legaalsele majandusele, ei ole tegutsemis- ja otsustusprotseduurid konkreetselt kirja pandud, vaid toimivad tihti *ad hoc*

printsiibil. Samas, küberkuritegude analüüs näitab, et ka seal on olemas oma mustrid ning protseduurid, mis peegeldavad otsusekohti ja äriprotsesse.

Väitekirja keskseks teemaks on rahaliselt motiveeritud küberkuritegevuse protsessimudeli, JMAP mudeli, välja töötamine. Uurimistööd läbi viies analüüsiti küberkuritegevuse kohta olemasolevaid definitsioone ja kasutusel olevaid taksonoomiaid. Analüüs näitas, et küberkuritegevus kui termin katab palju erinevaid teemasid ning põhineb erinevatel aspektidel. Akadeemiliselt, poliitiliselt, juriidiliselt ega praktiliselt ei ole kokku lepitud ühtset definitsiooni küberkuritegevuse kohta laiemalt, või rahaliselt motiveeritud küberkuritegevuse kohta kitsamalt. Seetõttu on väitekirjas välja pakutud vastav definitsioon ja taksonoomia, mis on aluseks rahaliselt motiveeritud küberkuritegevuse JMAP mudeli koostamiseks. Vajadus taksonoomia järele on oluline ja praktiline – ilma küberkuritegevust mõistmata ja defineerimata ei ole võimalik relevantseid uurimis- või vastutegevuse meetmeid arendada. Välja töötatud taksonoomia aluseks on üldine küberkuritegevuse protsess, mis sisaldab endas kõiki protsessis osalejaid (kurjategija ja ohver), vajalikke võimekusi (ründevektorid ja protseduurid), ning võimendajaid (küberkuritegevuse ökosüsteem ja monetiseerimine). Välja töötatud taksonoomia paneb aluse küberkuritegevuse kui protsessi, kus kurjategijate ja ohvrite tegevus on seotud süsteemselt ründevektorite, võimendajate ja väljumisstrateegiatega. Sellise taksonoomia kasutamine on oluline mitte ainult protsesside mõistmise kontekstis, vaid ka küberkurjategijate kasutatava *modus operandi*, s.t. taktika ja protseduuride, kirjeldamiseks. Mudeldamise tulemusena on võimalik leida nõrku kohti ja otsustuspunkte terviklikus protsessis, viia uurimist läbi efektiivsemalt, leida erinevaid vastumeetmeid ning välja töötada küberkuritegevuse vastase võitluse uudseid poliitilisi, uurimislikke või tehnilisi lahendusi.

Töös kasutati põhistatud teooria metodoloogia lähenemist, kuna see metodoloogia võimaldab teooria välja töötamist kasutades algselt ebatäielikke andmeid. Kuna olemasolevad teaduslikud uuringud küberkuritegevusest on piiratud ning laialdaselt aktsepteeritud metodoloogiat kasutuses ei ole, peeti nimetatud metodoloogiat kõige paindlikumaks ja sobivamaks. Olles paindlik, on metodoloogia samal ajal siiski struktureeritud. Põhistatud teooria ei keskendu niivõrd olemasolevate hüpoteeside testimisele, kui pigem andmete põhisele uue teooria, tegevuse või protsessi välja töötamisele. Põhistatud teooria keskseks ideeks on samaaegne ja järjepidev andmete kogumine, analüüs ja kirjutamine; mis kõik on omavahel seotud protsessid ja mida viiakse läbi korduva protsessina ja lõpptulemuseks on teooria mis põhineb andmetel.

Põhistatud teooria metodoloogiat kasutati küberkuritegevuse abstraktsete kategooriate loomiseks ning kliendikogemuse kaardistamise metodoloogiat kasutati kurjategijate motivatsiooni ja tegevuse kirjeldamiseks kuriteo protsessis. Samuti kasutati metodoloogiat mudeli rakenduslike aspektide ja vajaduste uurimiseks, vastamaks uurimistöö põhiküsimusele: kuidas modelleerida rahaliselt motiveeritud küberkuritegevust. Rakenduslike aspektide kajastamine rõhutab ka töö käigus läbi viidud intervjuudes välja toodut: vajadust küberkuritegevuse kui protsessi mõistmiseks, et leida efektiivseid lahendusi poliitilisel tasandil, uurimisorganite tegevuses, või tehniliste lahenduste välja töötamisel.

Väitekirja peamine panus on struktureeritud, süstemaatiline ja interdistsiplinaarne lähenemine küberkuritegevusele kui kompleksele süsteemile ning selle tarbeks JMAP mudeli välja töötamine. Töö tulemusel välja töötatud JMAP mudel rahaliselt motiveeritud küberkuritegevusest on paindlik. Tegemist on praktilise tööriistaga, mida saavad kasutada küberkuritegude uurimise ja ennetamisega tegelevad erinevad

osapooled. JMAP mudel annab samm-sammulise lähenemise kuriteo protsessis toimuvatele tegevustele. Mudeli näol ei ole tegemist lineaarse protsessi kaardistamisega, vaid paindliku mehhanismiga, millesse saab integreerida erinevaid olulisi aspekte. Paindlikkus võimaldab leida küberkurjategijate võtmesammud ja –otsustuspunktid kuriteo ettevalmistamise ja läbi viimise protsessis. JMAP mudeli praktiline eesmärk on võimaldada uurimise ja vastumeetmete arendamisega tegelevatel ametivõimudel ja ettevõtetel efektiivsemalt ületada praeguseid väljakutseid, mis peamiselt tulenevad protsessi üksikute osade uurimisel põhinevast lähenemisest.

Väljatöötatud JMAP mudel põhineb kriminoloogias kasutusel oleval kuritegude skriptimise metoodikal ühelt poolt ning majanduses kasutatava kliendikogemuse kaardistamisel teiselt poolt. Samuti on töö teostamisel saadud inspiratsiooni sõjateadustes kasutatavast faasi- e. etapi-põhisest lähenemisest. Kuna selliseks mudeldamiseks ei ole standardiseeritud reegleid või sümboleid, on autor kasutanud enda omasid. Küberkuritegu kui tervikut moodustava sündmuste jada visuaalne esitlus võimaldab kriminalistidel, intsidentidele reageerimisüksustel ja õiguskaitseorganitel identifitseerida erinevad etapid kuriteo tsüklis. Samuti võimaldab JMAP mudel kiiresti leida nii teadaoleva kui mitte-teadaoleva informatsiooni kuriteo toimumise protsessist, lihtsustades seeläbi keskendumist mitte-teadaolevatele aspektidele kuritegude uurimises.

Autor on teadlik väitekirjaga tõusetuda võivatest võimalikest eetilistest aspektidest – võimalusest et seda kasutatakse kuritegevuse käsiraamatuna, või näitab kurjategijatele, mida me neist teame. Samas on võimalik tuua näiteid krüptograafia ajaloost, kus see ei ole nii. Võib eeldada, et kindlasti on mõned kurjategijad, kellel JMAP mudelist kasu on, kuid suurem enamus neist teab ja tegutseb vastavalt juba praegu. Õiguskaitseorganitel on JMAP mudelil baseeruvast teadmisest vaieldamatult suurem kasu. Nagu väitekirjas on läbivalt välja toodud, võimaldab küberkuritegevuse protsesside mõistmine ja lahtikirjutamine suurendada õiguskaitseorganite teadmisi ja oskusi, ning efektiivistada uurimis- ja ennetustööd. Seega võib kokkuvõtteks öelda, et mudel annab õiguskaitseorganitele küberkuritegevuse protsesside visualiseeringu, mitte ei ole käsiraamatuks küberkurjategijatele.

Annex 1

Feedback form
Mapping cyber criminal journeys

1. Do you think this kind of modelling will be useful for your work?

   YES ( ) NO ( ) NOT SURE ( )

   (a) In case of „yes“ answer: In which areas could you use this model in your work?

   TRAINING ( ) INVESTIGATION ( ) PREVENTION ( )

   OTHER (please specify) _____

   (b) In case of „no“ answer: Why would it not be useful?

2. In your opinion, is there any important points missing in the cyber criminal journeys? Please explain.

3. Do you have any proposals for improving this model (for better application in police work)? Please explain.

4. Any other comments you would like to add

Annex 2

Intro and presentation

Who am I, what is this interview about, etc

Tiia Sõmer. Doing my PhD research to develop a model for visualising financially motivated cyber crime. Here is the current version … (show + explain)

Expectations: to get your view on how best to model financially motivated cyber crime.

The goal with the interview is to get the interviewee's perspective on modelling financially motivated cyber crime, the issues related to studying it, training people on how cyber crime as a process takes place, how can investigation activities be improved, how to develop better countermeasures and find preventive actions. Gain additional views on the potential usage of the model.

Framework of the interview.

Time: the interview will be between 30-60 minutes long.

During the interview, notes will be taken. The interview and its data will be anonymised and treated confidentially. Everything used from the interview will be anonymized so it wont lead back to the interviewee at any point. If there is anything you have doubts about or do not understand during the interview you are free to ask at any point. I want to let you know that your participation is voluntarily and that you can always withdraw your consent. You can opt out of answering any question.

THEMES FOR THE INTERVIEW

Questions	Question	Lead answers
1. Interviewee	What is your background?	LEA, Academia, industry, other
	What kind of experience do you have with cyber crime (or other cyber attack-related things, e.g. warfare)	Investigation, prevention, modelling, procecuting, …
	Based on your experience, if you were asked to describe a cyber crime event, how would you describe it?	Expect: discuss tech details, discuss how cyber crimes are currently investigated (in case of academia: researched), can they share details?
	In your knowledge, how are new LEA officers trained on cyber crime?	Special short term courses, on-the-job-training, university, …
2. Modelling	Do you have experience in modelling? If yes, please expand	Find out, whether the interviewee has some kind of experience with modelling in general or modelling of cyber crime in particular
	In your opinion, how can modelling be useful?	Find out interviewee's view on usefulness of/ attitude towards modelling

3. C-JMAP model	Here is the model that has been developed (present the model). The main aim is to find an overarching model to visualise all types of cyber crime.	
	How does this look like to you?	
	Do you think this kind of modelling will be useful for your work?	Expect: some find it useful – ask further for more details. Some find it not useful, investigate why
	If yes, how/ in which areas	Expect: training, investigation, prevention, policy … ask how
	If no, why not?	Expect: they do not work directly with cyber crime
	In your opinion, is there any important points missing in the cyber criminal journeys? Please explain	Expect: motivation aspect – explain why not included. Any other- ask for expanding thoughts
	Do you have any proposals for improving this model (for better application in police work)? Please explain	Expect most answers to focus on application of model, ask for concrete proposals (examples). Might be some interesting new ideas.
	Any other comments you would like to add	
	Can you share information on real life examples/ provide insights?	Expect in case of LEA: not being able due to classification/ sensitivity.
	Which phase of cyber crime are you most familiar with (preparation, execution, monetization)?	Discuss this phase in more detail, ask for sharing of real life examples/ insights, if possible.
	Follow-on questions based on interviewee's field of expertise, experience and previous answers	
4. Concerns with the C-JMAP model	Which concerns do you have with the model as such?	
	Which concerns do you have with the potential application of model in: - Training - Investigation - Prevention - Cooperative activities	
	Do you see any threats with the use of models in LEA work?	Scepticism about use of models, model for model's sake (not for real work)

Appendix 1

Publication I

Somer, Tiia; Hallaq, Bil; Watson, Tim. Utilising journey mapping and crime scripting to combat cyber crime. In Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS 2016 : Universität der Bundeswehr, Munich, Germany, 7-8 July 2016

Utilising Journey Mapping and Crime Scripting to Combat Cyber Crime

Tiia Somer, Tallinn University of Technology, tiia.somer@ttu.ee
Bil Hallaq, University of Warwick, bh@warwick.ac.uk
Tim Watson, University of Warwick, tw@warwick.ac.uk

Abstract
Modern society is now reliant on digital communication and networks for conducting a wide array of tasks, ranging from simple acts such as browsing the web through to mission critical tasks such as the management of critical infrastructure and industrial controls. This reliance shows a growing emphasis on strategic importance of cyberspace (Sharma, 2010). While organisations and individuals are keenly exploiting the benefits of cyberspace, these same platforms have also opened new avenues for nefarious actors in the pursuit of their criminal activities to attack, disrupt, or steal from organisations and individuals. Criminal organisations and lone criminals worldwide have access to powerful, evolving capabilities which they use to identify and target their victims allowing for the perpetration of a wide variety of cyber crimes.

This paper discusses ways in which utilising methods from typically non-cyber disciplines – business and criminology – can successfully be applied to the cyber domain in order to help in the fight against and prevention of cyber crime. Through the provision of a visual representation, this paper clarifies how journey mapping and crime scripting can help in building an understanding of the steps criminals undertake during execution of a cyber crime. In essence, within our work we have deconstructed the lifecycle of a crime events and translated these into a visualisation map to show the full event process, highlighting key steps as well as positive and negative events. Such work is useful to several roles and organisation types as it can aid in their decision processes when undertaking steps in pursuit, prevention, preparation and protection.

Keywords
Cyber crime, criminal journey mapping, cyber crime scripting, cyber crime pathways, E-CRIME Project

Introduction

It is an established fact that the internet has greatly affected the way societies and people operate. Worldwide internet usage has increased to more than 3.5 billion users at the beginning of 2014 (Internet Usage and World Population Statistics, 2014). In addition to people, internet connectivity today extends to digital devices, with more things connected to the internet than people. Gartner predicts that the number of internet connected devices will reach 25 billion for 2020 (Gartner, 2014).

While organisations and individuals are quick to exploit the business and personal benefits of internet, they often give less consideration that cyberspace offers a plethora of benefits to those who wish to attack them. Hacker groups, criminal organisations and espionage units worldwide have access to powerful, evolving capabilities, which they use to identify and target their victims and commit cyber crimes.

This research was conducted as part of the Economic Impacts of Cyber crime (E-CRIME) project of the Seventh Framework Programme, funded by the European Union. The majority of this work has been conducted with the help of desktop research and insights from a group of experts; the conclusions drawn and statements made rely on the Deliverable 2.3. "Detailed appendixes on cyber crime inventory and networks in non-ICT sectors" of the E-CRIME project [67]. The work was conducted by means of a review of the existing literature and an evaluation of the published approaches, as well as by conducting expert interviews. Sources of information included journals and conference proceedings in the fields of law, criminology and information systems, reports published by think-tanks and law enforcement agencies as well as scholarly textbooks.

Interviews of experts were also undertaken as a further means of data collection with the main consideration being: even though cyber crime has been researched extensively, the specific criminal "journeys" and stepping stones the cyber criminals take within crime cycles have not been subject to such research methods previously to the best of the authors knowledge based on publically available information. An interview guide was prepared, which provided an informal grouping of topics to be covered during the interview. Once completed the results of the interviews provided extra data and some interesting nuances. The authors prioritized the interview results, since the main focus was the provision and mapping of criminal journeys.

The expert groups of interviews for this paper consisted of law enforcement operating at regional, national and international levels, industry based cyber security experts as well as experts from academia. The aim was to reach a common conclusion, and not to research single activities at the micro levels. Different focus groups each had specific expertise and points of view to the topic of the research – cyber crime – which with the method chosen allowed for analysis of the experiences and requirements of a wider audience.

Cyber crime

Cyber crime is increasing in both complexity and intensity, reflecting an increased level of sophistication. For the purposes of this work our focus on cyber crime includes different aspects and extensions of modern crime: from development and sale of attack tools, services to plan and execute attacks and culmination in the laundering of stolen or illegally obtained assets. Cyber criminals increasingly operate in the same manner as legitimate business networks with clearly established business objectives and trusted supply chains for services or products that require outsourcing or development. The cyber criminals know what they are looking for, what goals they want to achieve and how to achieve these goals – and they are willing to spend time to research and plan their actions (CISCO 2014).

Given the complex nature of cyber crime and in order to understand and take efficient measures against it, it is imperative to gain deep understanding of the mechanics of cyber crime, from preparation, or pre-crime stages, to exit strategies and monetization, including everything in between the two including the committing of the actual crime. For the purposes of this paper we have performed several journey mapping exercises to describe the events and experiences that cyber crime perpetrators go through during a crime, using crime scripting techniques as found in traditional "offline" criminology.

The research focus of this work has been on the crime itself, not the underlying causes of crime or the law enforcement actions following the crime. This mapping will help facilitate identification and testing of effective countermeasures, as well as facilitate further work in identification of possibilities to deter criminals and manage risks deriving from the perpetration of cyber criminal activities.

Three phases are critical to the development of our journeys from the perspective of the criminal:

1. Preparation phase
    a. Decision to engage in criminal activity
    b. Choosing a victim
    c. Choosing a method
2. Execution phase
    a. Conducting the crime
3. Monetization/Reward phase
    a. Exit

Cyber crime can be seen as a process where resources are required and decisions are taken at different stages in the process. The preparation phase includes pre-attack actions including committing to the initial decision to undertake a crime, deciding on the worthiness of an attack, identifying potential victims, and conducting targeted reconnaissance, but also a choice of an attack method including use of own means and abilities, or taking the decision to outsource respective capabilities. The execution phase includes drawing an attack plan and executing the attack itself, including entering the target system and conducting criminal activities within such systems. It also includes lateral movement and finding additional opportunities for criminal action. The monetization phase includes direct or indirect monetary gain for the cyber criminals(s) and exit strategy. It is important to note that throughout any one criminal journey, the perpetrator can loop back to an earlier step (if a chosen attack method fails, they need to find a new one, or they may 'accidentally' find unforeseen vulnerabilities to take advantage of), or they can repeat steps for example, defacing the same website multiple times, or they may just quit once they realise the efforts are not worth the results.

Various sources show the developments of global cyber crime and related threat landscape. The United Nations Comprehensive Study on Cybercrime of 2013 states that cyber crime globally shows a broad distribution across financially driven acts, computer-content related acts, but also attacks against the confidentiality, integrity and availability of data and computer systems (United Nations 2013) which is key to take into consideration in understanding cyber criminal journeys. The 2015 RSA outlook on the changing threat landscape of cyber crime states that the most important trend developing within the past few years, is the rapid advancement of cyber crime-as-a-service model. What this development means, is that more criminals can participate in the chain and that these criminal do not need to understand the complete chain of the crime nor how to conduct any specific part of it, for example spam, DDoS or phishing. Nor do they need to have the technical requirements in house to the conduct of the crime itself (RSA 2015). The ENISA Threat Landscape 2015 states that from cyber crime-as-a-service model, the most mature are botnet-related service models (ENISA 2015). ENISA also states that the most rapidly growing service is provision of ransomware-

related services. These points clarify the importance of journey mapping and crime scripting in order to provide those combatting cyber crime with a clear understanding of the complete crime cycle, including the various aspects and actors which may take part at different phases of a cyber crime.

Journey mapping

Journey mapping is a methodological tool that has been traditionally used in business to map customer experience, as well as in criminology generally under the name of crime scripts. Journey mapping is also often used by strategy consultancies and public organisations to shape customer strategies and public service transformational programmes. In criminology, crime scripts have been used to deconstruct complex crimes into component parts even from a relatively small data set. Within this work we have used such methods from these typically non-cyber disciplines and shown that they can be successfully applied to the cyber domain.

Crime scripting

The 'map'-style of output has been adopted and applied within a number of different disciplines where it is often referred to as a *script*. A script is a predetermined set of actions that define a well-known situation in a particular context (Borrion, 2013), or more specifically "[a] script is simply a sequence of actions which make up an event" (Brayley, 2011). Scripts are related to the concept of schema, i.e. "abstract cognitive representations of organised prior knowledge, extracted from experiences with specific instances". When the sequence of events being scripted encapsulates the conduct of a criminal activity (as in the case of cyber crime), the output is commonly referred to as a crime script (Borrion, 2013). Initially developed in psychology, scripts are now used in different fields from artificial intelligence to consulting.

Scripts can be used to present different crimes, but are believed to be of particular use for new or complex crimes (Brayley, 2011). It has also been suggested that crime scripts can be used as an innovative way to gain a more detailed understanding of complex forms of crime in a review of organized crime-reduction strategies (Levi, 2004). As previously stated in this paper, cyber crime is a rapidly developing field with an evolving trend of the cyber crime-as-a-service model. This will bring more participants into the cyber crime journey or cycle, making it more complex to understand for those dedicated to prevention and fight against cyber crime.

Why can criminal journey maps be useful?

By schematically representing an anticipated sequence of actions, scripts are able to provide us with a cognitive representation of how we believe a sequence of events has occurred and will occur (Borrion, 2013), including for our purposes, the steps a criminal takes to commit a cyber crime. In this situation, the value of crime scripting as a crime analysis mechanism is believed to be in its potential to assist in the fight against such crime (Borrion, 2013) through the identification of *pinch points*. For example, by graphically presenting the typical sequence of events for a crime that has been derived from many examples of that type of crime, analysts are able to identify specific metaphorical gates the criminal must pass through if their crimes are to succeed. Once these points are identified, the logic is that those seeking to prevent such crimes will now know where best to focus their energies, whether this be through legislative or regulatory

changes, the development of new technological countermeasures, development of general awareness campaigns, the behaviour change of potential victims, or increased monitoring by police forces so as to capture or deter the cyber criminals. As stated in many cyber crime related sources, cyber crimes are becoming more complex, involving more parties each conducting independent steps within various phases of any one crime (RSA 2015, ENISA 2015). The understanding of each step, however minor within this crime cycle, will become more vital. The journey maps developed provide a cognitive representation of how we believe a cyber crime takes place from preparation to monetization and exit.

Some crime scripts list a sequence of actions and don't draw a diagram, others draw a graphical representation showing a series of actions and decision points. In graphical presentations, scripts are usually drawn as series of boxes, linked by arrows indicating direction of flow (where boxes indicate actions or decisions). As the same crime can be committed in different ways, so can different routes/tracks co-exist on one script.

There are various levels of scripts and selection depends on the script's intended application (Brayley, 2011). For the purposes of the current work, we developed a high-level journey map detailing a general cyber crime cycle (Figure 1). This is a general depiction of a single cyber crime act, from which more detailed maps in different categories can been drawn. In order to be of practical use in understanding cyber crime, more detailed journey maps for different criminal journeys are needed, providing crime sequences from preparation to exit for these specific journeys.

Since there are no standard journey mapping rules or specific software for crime scripting (Brayley, 2011), we have used our own symbols and drawings. We grouped similar actions under broad terms: preparation, execution, and monetization. The journey maps developed provide a step-by-step high-level account of actions taken by the criminals throughout the crime. Crimes are a process which involves several steps leading to reaching an end-goal as identified by respective criminals. For example, the preparation phase includes various pre-attack actions, i.e. initial decision, deciding the worthiness of an attack, identifying victims, and conducting targeted reconnaissance. The preparation phase also includes the choice of an attack method, including the cyber criminal(s) undertaking an analysis of their own means and abilities and making the decision of outsourcing or buying solutions from external sources in case there is a resource or skills gap. The execution phase includes creating an attack plan and executing the attack, which comprises of entering or interfacing with target system and the actual criminal activities (i.e. distributed denial of service (DDoS), extortion, espionage, etc.) themselves. However, it is important to note that the tactics used by criminals do not always follow the above formalised decision points, meaning that in some instances decisions are made very quickly without conducting a full-scale analysis or creating a set of actual attack plans. A further important point to note, is that the criminal can loop back to any earlier phase as required by circumstances and in some instances they may choose to abort the undertaking for example in cases where the criminals might determine it is no longer cost-effective or the potential risk of getting caught is not worth the reward. The monetization phase includes a tangible payment in some form with laundering and/or mules often being utilised, although in some instances the criminals will not have a monetary objective which is discussed in the next section. The final result culminates in

a personal gain or fulfilment of end-results as set out in the initial stages for the criminal(s).

Mapping and scripting a general cyber crime journey

Figure 1 represents a high-level journey map detailing a general crime cycle from the criminal's perspective. This general cyber criminal journey and journeys for any follow-on specific crimes have been developed with the help of desktop research and insights from experts as part of the E-Crime 7th framework project as already mentioned in this paper. The benefits for investigators of producing this visual representation of the general cycle are that;

(a) By identifying the commonalities in the conduct of what may seem very different cyber crimes, we can expose the sequence of events that underpin the majority of these.

(b) By comparing detailed maps of multiple different cyber crimes against this general crime cycle, those tasked with preventing and/ or defending against such crimes can see best where to focus their resources for maximum effect.

c) Experiment via virtualised or desktop exercises the application of countermeasures at various points along the pathway with the goal of taking forward the most effective ones for application in real word scenarios.

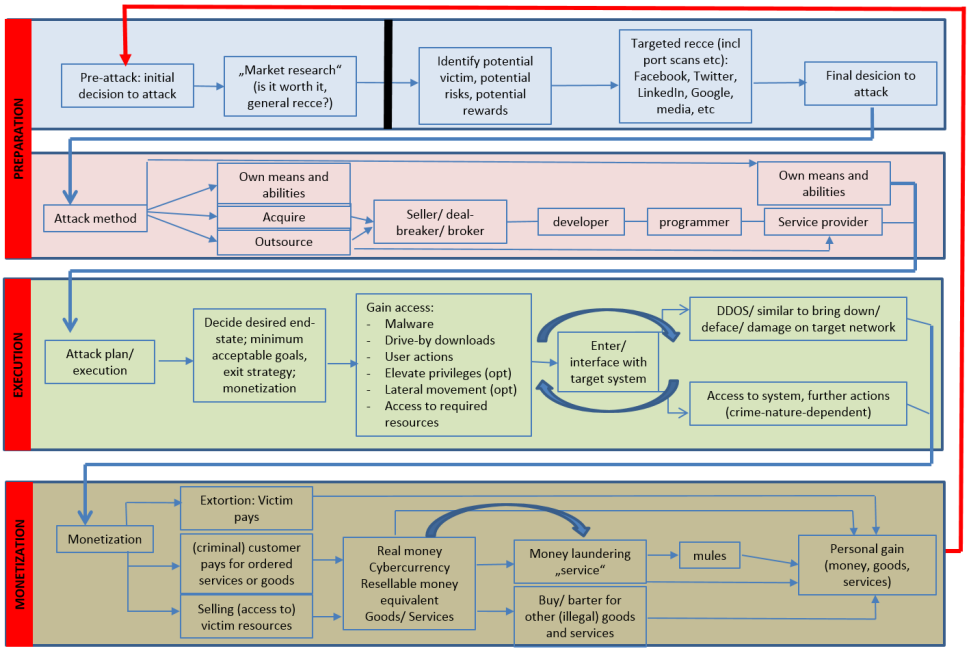

Figure 1: General cyber crime journey map

The preparation phase has two main components. Firstly the criminals need to decide whether or not to conduct the crime in the first place. This may be simply an opportunistic decision or it may include "market research" of some kind, in the sense of determining and weighing the costs and benefits of their options. The second component requires the identification of potential victims and attack methods, the conducting of

targeted reconnaissance and finally deciding to execute the criminal act. The attack itself can then be executed in three ways, either; (1) by using their own existing means and abilities. As an example in case they have access to their own botnet, malware or exploit already, they will use these and will not go through all the steps in the process but move to the execution phase directly. (2) By buying the respective means and/or capabilities from other criminals – this brings other sectors into the process (special markets, forums, stores, sellers, brokers, developers, etc.), or (3) Outsourcing the required criminal activities by paying another criminal to conduct it as a service (crime-as-a-service).

The execution phase starts with an attack plan. In the plan the criminal decides upon a desired end-state, their minimum acceptable goals, and monetisation and exit strategies. During the attack, the criminal gains access to victim's resources through any number of means, including malware, drive-by downloads, user actions via phishing techniques or other illicit activities. Once the criminal gains access to the victim's system, they will map the compromised network, often looking for further opportunities to exploit. Thereafter the criminal enters or interfaces with the target system and based on their desired and decided goals and end-states they take the commensurate actions. Within this phase of mapping the compromised network, the criminal may notice other vulnerabilities that may become useful in their reaching of stated end-results and will take advantage of these, i.e. committing different crimes which were not originally part of their attack plan.

The monetization phase involves obtaining tangible benefits. These benefits include direct monetary gain, for example where the victim's monetary assets are stolen, or the victim pays the criminal directly in cases of extortion, such as ransomware or DDoS extortion schemes. Or indirect monetary gain whereby the victim's resources can be turned to tangible assets which are traded or sold, for example selling access to the victim's machine to others. The payment can be conducted in real currency, crypto-currency, resalable money equivalents (such as gaming assets), or in goods and services (real or virtual, legal or illegal). In some cases money laundering services are used, in other cases other means such as setting up mules to withdraw cash from banks might be used. Clearly though in some cases the monetization phase is excluded, examples of such cases include Hacktivists or those with ideological or other motivations.
In any case the crime ends with an exit strategy as set out by the criminal culminating in some type of personal gratification be it monetary or otherwise.

Conclusion

Within this report, the authors have shown how traditional crime scripting can provide useful insights into understanding the lifecycle of a general cyber-criminal journey. It also shows how methods and techniques from typically non-cyber disciplines can be successfully applied to the cyber domain. Such mapping and scripting can be modified and further detailed for specific crime scenarios and graphically represented. By graphically presenting the sequence of events constituting a cyber crime, risk management teams, forensic analysts, incident response teams and law enforcement agencies will be able to identify the specific stepping stones and pinch points that cyber criminals pass through in committing their crimes. Such work can help to facilitate the identification and testing of effective countermeasures including mitigation at scale, early prevention and the development of proportional disruption techniques.

References

Brayley, H., Cockbain, E., Laycock, G., 2011. The value of crime scripting: Deconstructing Internal Child Sex Trafficking, Policing, Volume 5, Number 2, pp. 132–143

Borrion, H., 2013. Quality assurance in crime scripting, Crime Science 2013, 2:6. Available online at: http://www.crimesciencejournal.com/content/2/1/6

CISCO, 2014. Annual Security Report. Available online at: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

The Economic Impacts of Cyber Crime, FP7-SEC-2013.2.5-2. D2.3 Detailed appendixes on cyber crime inventory and networks in non-ICT sectors. T.Sõmer, R.Ottis, T.Lepik, M.Lagazio, B.Hallaq, D.Simms, T.Mitchener-Nissen. March 2015

ENISA Threat Landscape 2015. ENISA 2015. Available for download at: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015

Gartner, 2014. http://www.gartner.com/newsroom/id/2905717
Internet Usage and World Population Statistics, 2015. http://www.internetworldstats.com/stats.htm

RSA 2015. CYBERCRIME 2015: An Inside Look at the Changing Threat Landscape. Available online at: https://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf

Sharma, Amit, “Cyber Wars: A Paradigm Shift from Means to Ends”, Strategic Analysis, Vol. 34, No. 1, 2010, pp. 62-73. http://www.tandfonline.com/toc/rsan20/34/1

United Nations 2013. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013. Available online at: <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Appendix 2

Publication II

Somer, Tiia; Hallaq, Bil; Watson, Tim. Utilising Journey Mapping and Crime Scripting to Combat Cyber crime and Cyber Warfare Attacks. In Journal of Information Warfare (2016) 15.4: 39-49

Utilising Journey Mapping and Crime Scripting to Combat Cyber crime and Cyber Warfare Attacks

T Somer[1], B Hallaq[2], T Watson[3]

[1]*Tallinn University of Technology, Tallinn, Estonia*
tiia.somer@ttu.ee

[2]*University of Warwick, Coventry, United Kingdom*
bh@warwick.ac.uk

University of Warwick, Coventry, United Kingdom
[3]*University of Warwick*
tw@warwick.ac.uk

Abstract:
This paper discusses ways in which utilising methods from typically non-cyber disciplines, business and criminology, can successfully be applied to the cyber domain to aid the fight against and the prevention of cyber-attacks, including those used in cyber warfare. Through the provision of a visual representation, this paper clarifies how journey mapping and crime scripting can help build an understanding of the steps criminals or adversaries in general undertake during the execution of a cyber crime or cyber-warfare attack.

Keywords: *Cyber-attack, Cyber crime, Cyber Warfare, Journey Mapping, Crime Scripting, Cyber-attack Pathways, E-CRIME Project*

Introduction

Modern society is now reliant on digital communication and networks for conducting a wide array of tasks, ranging from simple acts, such as browsing the web, to mission-critical tasks, such as the management of critical infrastructure and industrial controls. This reliance reveals a growing emphasis on the strategic importance of cyberspace (Sharma 2010). While organisations and individuals are keenly exploiting the benefits of cyberspace, these same platforms have also opened new avenues for nefarious actors to attack, disrupt, or steal from organisations and individuals. Criminal organisations and lone criminals worldwide have access to powerful, evolving capabilities which they use to identify and target their victims allowing for the perpetration of a wide variety of cyber crimes. Cyber-attacks and the term ‘cyber warfare, which for the purposes of this paper involves the actions by a nation state or international organisation to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks, have been used more frequently and led to the emergence of a new class of weapons: software viruses, Trojan horses, logic

bombs, etc. Where such weapons exist, attackers exist also. The modus operandi of nation-state actors is not much different from that used by cyber criminals—with the exception of their end goals.

This paper discusses ways in which utilising methods from typically non-cyber disciplines, business and criminology, can successfully be applied to the cyber domain to aid the fight against and the prevention of cyber-attacks, including those used in cyber warfare. Through the provision of a visual representation, this paper clarifies how journey mapping and crime scripting can help build an understanding of the steps criminals or adversaries in general undertake during the execution of a cyber crime or cyber-warfare attack.

In essence, the authors have deconstructed the lifecycle of attack events and translated the steps within it into a visualisation map to show the full-event process and to highlight key steps as well as positive and negative events. Such work can be applied to the military defence area, as it can aid in the decision-making processes involved in pursuit, prevention, preparation, and protection. The end goals of criminal or military actors differ, but their tactics and techniques—reconnaissance for, preparation of, and execution of attacks—use the same modus operandi.

It is an established fact that the internet has greatly affected the way societies and people operate. Worldwide Internet usage has increased to more than 3.5 billion users at the beginning of 2014 (Internet Usage and World Population Statistics 2014). In addition to people, internet connectivity today extends to digital devices, with more things connected to the internet than people. Gartner (2014) predicts that the number of internet connected devices will reach 25 billion by 2020.

While organisations and individuals are quick to exploit the business and personal benefits of the internet, they often give less consideration to the fact that cyberspace offers a plethora of benefits to those who wish to attack them. Hacker groups, criminal organisations, and espionage units worldwide have access to powerful, evolving capabilities, which they use to identify and target their victims and to commit cyber crimes.

Methodology

This article is based on research conducted as part of the Economic Impacts of Cyber crime (E-CRIME) project of the Seventh Framework Programme funded by the European Union. The majority of this work has been conducted with the help of desktop research and insights from a group of experts; the conclusions drawn and statements made rely on the Deliverables 2.2. “Executive summary and brief: Cyber crime inventory and networks in non-ICT sectors” and 2.3. “Detailed appendixes on cyber crime inventory and networks in non-ICT sectors” of the E-CRIME project (Somer et al 2015). The work was conducted by means of a review of the existing literature and an evaluation of the published approaches, as well as by conducting interviews with experts. Sources of information included journals and conference proceedings in the fields of law, criminology, and information systems; reports published by think-tanks and law enforcement agencies, as well as scholarly textbooks. The “Cyber Kill Chain” introduced by Lockheed Martin (Hutchins et al 2011) provides a good base for understanding the

cyber-attack event chain. In the current discussion, however, the authors have attempted to simplify the process into as few steps as possible, with the aim of finding potential ways to combat cyber crime.

Interviews of experts were also undertaken as a further means of data collection with the main consideration being this: even though cyber-attacks and cyber crime have been researched extensively, the specific criminal 'journeys' and stepping stones the cyber criminals take within crime cycles have not previously been subject to such research methods, to the best of the authors' knowledge, which is based on publicly available information.

The interviews followed an interview guide, which provided an informal grouping of topics. Once completed, the results of the interviews provided extra data and revealed some interesting nuances. Since the main focus was the provision and mapping of criminal journeys, the authors prioritized interview results. The results, however, are relevant for cyber-attacks in general—that is, not only cyber crime—since attackers use certain patterns, tactics, and techniques, irrespective of whether they are criminals or nation-state actors.

The groups of expert interviews for this paper consisted of law enforcement operating at regional, national, and international levels; industry-based cybersecurity experts, as well as experts from academia. The aim was to reach a common conclusion, not to research single activities at the micro levels. Each different focus group had specific expertise and points of view regarding the topic of the research, which, with the method chosen, allowed for analysis of the experiences and requirements of a wider audience.

Cyber crime

Cyber crime is increasing in both complexity and intensity, reflecting an increased level of sophistication. For the purposes of this work, the focus on cyber crime includes different aspects and extensions of modern crime: from development and sale of attack tools, services to plan and execute attacks, and culmination in the laundering of stolen or illegally obtained assets. Cyber criminals increasingly operate in the same manner as legitimate business networks with clearly established business objectives and trusted supply chains for services or products that require outsourcing or development. The cyber criminals know what they are looking for, what goals they want to achieve, and how to achieve these goals—and they are willing to spend time to research and plan their actions (CISCO 2014).

Given the complex nature of cyber crime, understanding and taking efficient measures against it requires a deep comprehension of the mechanics of cyber crime, from preparation or pre-crime stages, to exit strategies and monetization, to everything between the two, including the committing of the actual crime. For the purposes of this paper, the authors have performed several journey-mapping exercises using crime-scripting techniques as found in traditional 'offline' criminology to describe the events and experiences that cyber crime perpetrators go through during a crime. The research focus of this work has been on the crime itself, not the underlying causes of crime or the law-enforcement actions following the crime. This mapping will help facilitate identification and testing of effective countermeasures, as well as facilitate further work

on the identification of possible ways to deter criminals and manage risks deriving from the perpetration of cyber-criminal activities.

Relevance to Cyber Warfare

Cyber-attack campaigns today use tactics and techniques similar to cyber criminals: denial of service attacks (Ottis 2008), information-gathering malicious software (Kaspersky 2015), new sophisticated targeted weapons such as Stuxnet (De Falco 2012), and espionage and infiltration into systems for the purpose of data exfiltration (Lancaster University 2014). The development of malware or denial of service attacks can have grave consequences by influencing command and control capabilities or systems to a great extent. Such activities can potentially change the course of power supremacy.

The difference between cyber crime and cyber war is vague (Denker 2011). The definitions are manifold, and discussions are ongoing whether cyber war is cyber crime or vice versa. The aim of this discussion is not to define the two, but rather to focus on how to best deconstruct the attacks: tactics, methodologies, and techniques used; targets and consequences—regardless of attribution. Two clear differences between cyber crime and cyber war are the underlying intent in the conduct of attacks and the end goals to be achieved (Trend Micro 2013). The intent of cyber criminals is to get personal gain (usually monetary); the intent of cyber warriors is to gain political supremacy using cyber means.

After analysing writings on cyber warfare (Bernik, 2013; PC World 2012; Clarke 2010) and on cyber crime (Goodman 2015; Olson 2013), the authors have concluded that even though the intent and end goals are different, the underlying attack cycle remains the same in both: preparing for the attack, executing the attack, and following an exit strategy.

The current discussion takes methods used in typically non-cyber disciplines—business and criminology—and applies these to the cyber domain in order to deconstruct attacks—criminal or military—and find ways to prevent attacks, fight against them, or find countermeasures.

Cyber crime Journey

Three phases are critical to the development of cyber crime journeys from the perspective of the criminal:

1. Preparation phase
    a. Deciding to engage in criminal activity
    b. Choosing a victim
    c. Choosing a method
2. Execution phase
    a. Conducting the crime
3. Monetization/Reward phase
    a. Exiting

Cyber-attacks related to crime and warfare can be seen as a process where resources are required and decisions are taken at different stages in the process. The preparation phase includes pre-attack actions including committing to the initial decision to

undertake a crime, deciding on the worthiness and/or reasons for undertaking an attack, identifying potential victims, and conducting targeted reconnaissance, but also choosing an attack method, including use of own means and abilities, or taking the decision to outsource respective capabilities. The execution phase includes drawing an attack plan and executing the attack itself, including entering the target system and conducting criminal activities within such systems. It also includes lateral movement and finding additional opportunities for criminal action. The monetisation phase includes direct or indirect gain for the cyber-attackers and culminates in an exit strategy. It is important to note that throughout any one criminal journey, the perpetrators can loop back to an earlier step (if a chosen attack method fails, if the perpetrators need to find a new one, or if they 'accidentally' find unforeseen vulnerabilities to take advantage of); or they can repeat steps, for example, defacing the same website multiple times; or they may just quit once they realise the efforts are not worth the results. As stated previously, this journey can be applied to cyber-attacks in general with the exception of the monetisation phase which in general is not relevant for nation-state actors.

Various sources show the developments of global cyber crime and related threat landscape. The United Nations Comprehensive Study on Cybercrime of 2013 states that cyber crime globally shows a broad distribution across financially driven acts, computer-content related acts, but also attacks against the confidentiality, integrity, and availability of data and computer systems (United Nations Office on Drugs and Crime 2013). This distribution is key to understanding cybercriminal journeys. The 2015 RSA outlook on the changing threat landscape of cyber crime states that the most important trend developing within the past few years is the rapid advancement of cyber crime as a service model. What this development means is that more criminals can participate in the chain and that these criminal do not need to understand the complete chain of the crime nor how to conduct any specific part of it (for example, spam, DDoS or phishing). Nor do they need to have the technical requirements in house to conduct the crime itself (RSA 2015). The ENISA Threat Landscape 2015 states that from among cyber crime-as-a-service model, the most mature are botnet-related cyber crime service models (ENISA 2015). ENISA also states that the most rapidly growing service is provision of ransomware-related services.

Other studies have been undertaken specifically for cyber warfare. Geol (2011) states, "Cyberwarfare is a potent weapon in political conflicts, espionage, and propaganda. Difficult to detect a priori, it is often recognized only after significant damage has been done".

Intelligence agencies can today gather large amounts of information that can then be used for any purpose, including a military one. In the military context, this broad information-gathering capability can create decisive information superiority. In discussing the Russia-Ukraine conflict in 2015, Weedon (2015) explains how this superiority can be achieved: preparing the ground for conventional military operations via cyber means and using denial and deception. Weedon shows the technical aspects of alleged Russian cyber operations in the Russia-Ukraine conflict, including samples of malware employed, tactics used by hackers, and results achieved.

Pakharenko (2015) has provided an overview of cyber-attacks that took place during the revolution in Ukraine. During the street demonstrations, actions were taking place in cyberspace as well: physical and logical attacks were being launched against opposition servers, smartphones, and websites. In Crimea, attacks were even more sophisticated: from severing network cables to influencing satellites. At the same time, cyber espionage operations were conducted in Eastern Ukraine using location data of mobile phones and Wi-Fi networks to target military units, and to isolate parts of the country from the rest on internet.

These points clarify the importance of journey mapping and crime scripting in order to provide those combatting cyber crime and cyber warfare with a clear understanding of the complete attack cycle, including the various aspects and actors which may take part at different phases of a cyber-attack.

Journey Mapping

Journey mapping is a methodological tool that has been traditionally used in business to map customer experience, as well as in criminology generally under the name of crime scripts. Journey mapping is also often used by strategy consultancies and public organisations to shape customer strategies and public service transformational programmes. In criminology, crime scripts have been used to deconstruct complex crimes into component parts even from a relatively small data set. Within this work, the authors have used such methods from these typically non-cyber disciplines and shown that they can be successfully applied to the cyber domain.

Cybercriminal scripting

The 'map'-style of output has been adopted and applied within a number of different disciplines where it is often referred to as a *script*. A script is a predetermined set of actions that define a well-known situation in a particular context (Borrion 2013), or more specifically "[a] script is simply a sequence of actions which make up an event" (Brayley 2011). Scripts are related to the concept of schema, i.e. "abstract cognitive representations of organised prior knowledge, extracted from experiences with specific instances" (Brayley 2011). When the sequence of events being scripted encapsulates the conduct of a criminal activity (as in the case of cyber crime), the output is commonly referred to as a crime script (Borrion 2013). Initially developed in psychology, scripts are now used in different fields, ranging from artificial intelligence to consulting.

Scripts can be used to present different crimes, but are believed to be of particular use for new or complex crimes (Brayley 2011). It has also been suggested that crime scripts can be used as an innovative way to gain a more detailed understanding of complex forms of crime in a review of organized crime-reduction strategies (Levi, Maguire 2004). As previously stated in this paper, cyber crime is a rapidly developing field with an evolving trend of the cyber crime-as-a-service model. This will bring more participants into the cyber crime journey or cycle, making it more complex to understand for those dedicated to the prevention of and fight against cyber crime.

Why can criminal journey maps be useful?

By schematically representing an anticipated sequence of actions, scripts are able to provide a cognitive representation of how people believe a sequence of events has

occurred and will occur (Borrion 2013), including, for the purposes of this discussion, the steps a criminal takes to commit a cyber crime. In this situation, the value of crime scripting as a crime analysis mechanism is believed to be in its potential to assist in the fight against such crime through the identification of *pinch points* (Borrion 2013). For example, by graphically presenting the typical sequence of events for a crime that has been derived from many examples of that type of crime, analysts are able to identify specific metaphorical gates criminals must pass through if their crimes are to succeed. Once these points are identified, the logic is that those seeking to prevent such crimes will now know where best to focus their energies, whether it be through legislative or regulatory changes, the development of new technological countermeasures, the development of general awareness campaigns, the behaviour change of potential victims, or an increase in monitoring by police forces so as to capture or deter the cyber criminals. As stated in many cyber crime-related sources, cyber crimes are becoming more complex, involving more parties each conducting independent steps within various phases of any one crime (RSA 2015; ENISA 2015). The understanding of each step, however minor within this crime cycle, will become more vital. The journey maps developed provide a cognitive representation of how analysts believe a cyber crime takes place from preparation to monetization to exit.

Some crime scripts list a sequence of actions and do not draw a diagram; others draw a graphical representation showing a series of actions and decision points. In graphical presentations, scripts are usually drawn as series of boxes, linked by arrows indicating direction of flow (where boxes indicate actions or decisions). As the same crime can be committed in different ways, so can different routes/tracks co-exist on one script.

There are various levels of scripts, and selection depends on the script's intended application (Brayley 2011). For the purposes of the current work, the authors developed a high-level journey map detailing a general cyber crime cycle (**Figure 1**, below). This is a general depiction of a single cyber crime act, from which more detailed maps in different categories can been drawn. In order to be of practical use in understanding cyber crime, more detailed journey maps for different criminal journeys are needed, providing crime sequences from preparation to exit for these specific journeys.

Since there are no standard journey mapping rules or specific software for crime scripting (Brayley 2011), the authors have used their own symbols and drawings. With similar actions grouped under broad terms (preparation, execution, and monetization), the journey maps developed provide a step-by-step, high-level account of actions taken by the criminals throughout the crime. Crimes are a process which involves several steps leading to reaching an end-goal as identified by respective criminals. For example, the preparation phase includes various pre-attack actions, including making the initial decision, deciding the worthiness of an attack, identifying victims, and conducting targeted reconnaissance. The preparation phase also includes the choice of an attack method, including the cybercriminal(s) undertaking an analysis of their own means and abilities, and making the decision of outsourcing or buying solutions from external sources in case there is a resource or skills gap. The execution phase includes creating an attack plan and executing the attack, which comprises entering or interfacing with target system and the actual criminal activities (that is, distributed denial of service (DDoS), extortion, espionage, etc.) themselves. However, it is important to note that the tactics

used by criminals do not always follow the above formalised decision points, meaning that in some instances decisions are made very quickly without conducting a full-scale analysis or creating a set of actual attack plans. A further important point to note is that the criminal can loop back to any earlier phase as required by circumstances; and in some instances, they may choose to abort the undertaking, for example, in cases where the criminals might determine it is no longer cost-effective or the potential risk of getting caught is not worth the reward. The monetization phase includes a tangible payment in some form with laundering and/or mules often being utilised. Although in some instances the criminals will not have a monetary objective (which is discussed in the next section). The final result culminates in a personal gain or fulfilment of end-results as set out in the initial stages for the attackers, regardless of their primary motivation.

Mapping and Scripting a General Cybercriminal Journey

Figure 1, below, represents a high-level journey map detailing a general crime cycle from the criminal's perspective. This general cybercriminal journey and journeys for specific crimes thereafter have been developed with the help of desktop research and insights from experts as part of the EU E-Crime 7th framework project as already mentioned in this paper.

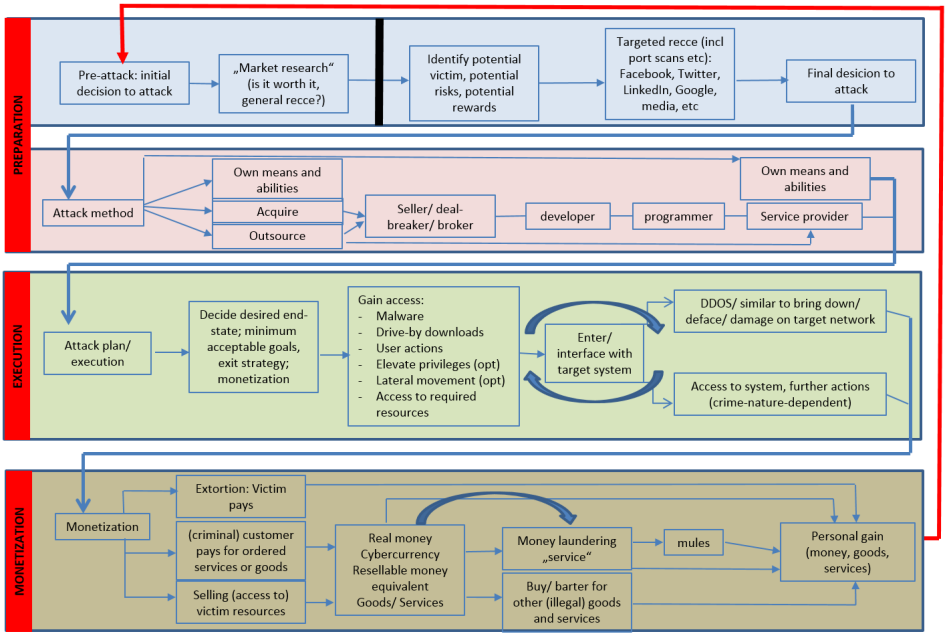

Figure 1: General cyber crime journey map

The benefits for investigators and defenders of producing this visual representation of the general cycle are as follows:

(a) By identifying the commonalities in the conduct of what may seem very different cyber crimes, the sequence of events that underpin the majority of these cyber crimes may be exposed.

(b) By comparing detailed maps of multiple and different cyber crimes against this general crime cycle, those tasked with preventing and/ or defending against such crimes can see best where to focus their resources for maximum effect.

c) By allowing for experimentation (via virtualised or desktop exercises) with the application of countermeasures at various points along the pathway, the goal of taking forward the most effective ones for application in real word scenarios may be achieved.

It is worth noting that the principles introduced with **Figure 1** (above) are usable for any cyber-attack, not only cyber crime.

Phases of the cyber crime journey

The preparation phase has two main components. Firstly the criminals need to decide whether or not to conduct the crime in the first place. This may simply be an opportunistic decision, or it may include 'market research' of some kind, in the sense of determining and weighing the costs and benefits of their options. The second component requires the identification of potential victims and attack methods, the conducting of targeted reconnaissance, and finally deciding to execute the criminal act. The attack itself can then be executed in three ways. First, the criminals may use their own existing means and abilities. For example, if they have access to their own botnet, malware, or exploit already, they will use these and will not go through all the steps in the process but, instead, move to the execution phase directly. Secondly, the criminals may buy the respective means and/or capabilities from other criminals, which would bring other sectors into the process (special markets, forums, stores, sellers, brokers, developers, etc.). Third, the criminals may outsource the required criminal activities by paying another criminal to conduct them as a service (crime-as-a-service).

The execution phase starts with an attack plan. In the plan, the criminals decide upon a desired end-state, their minimum acceptable goals, and monetisation and exit strategies. During the attack, the criminals gain access to victim's resources through any number of means, including malware, drive-by downloads, user actions via phishing techniques, or other illicit activities. Once the criminals gain access to the victim's system, they will map the compromised network, often looking for further opportunities to exploit. Thereafter, the criminals enter or interface with the target system. Based on the criminals' desired and decided goals and end-states, they take the commensurate actions. Within this phase of mapping the compromised network, the criminals may notice other vulnerabilities that may become useful in reaching their stated end-results and may take advantage of these vulnerabilities, for example, committing different crimes which were not originally part of their attack plan.

The monetisation phase involves obtaining tangible benefits. These benefits include direct monetary gain, for example, the victim's monetary assets are stolen or the victim pays the criminal directly in cases of extortion, such as ransomware or DDoS extortion

schemes. Or indirect monetary gain may be achieved if the victim's resources can be turned to tangible assets, which are traded or sold (for example, selling access to the victim's machine to others). The payment can be made in real currency, crypto-currency, resalable money equivalents (such as gaming assets), or in goods and services (real or virtual, legal or illegal). In some cases, money laundering services are used; in other cases, other means such as setting up mules to withdraw cash from banks might be used. Clearly, though, in some cases the monetization phase is excluded. Examples of such cases include Hacktivists or those with ideological or other motivations.

In any case, the crime ends with an exit strategy as set out by the criminals and culminating in some type of personal gratification, be it monetary or otherwise. As pointed out earlier, a difference between cyber crime and cyber warfare is the intent of attacks and the end goals to be achieved (Trend Micro 2013). While the intent of cyber criminals is to get some kind of monetary reward, the intent of cyber warriors is to gain political supremacy using cyber means. In order to gain political advantage, generation of revenue is not necessary: a successful outcome for hackers could be manipulation of data. As seen in the recent Russia-Ukraine conflict, physical and logical attacks against opposition servers, smartphones, and websites were conducted; as were cyber espionage operations to target military units and to isolate parts of the country from the rest on internet (Pakharenko 2015).

Conclusion

Within this report, the authors have shown how traditional crime scripting can provide useful insights into understanding the lifecycle of a general cyber-criminal journey. The article also shows how methods and techniques from typically non-cyber disciplines can be successfully applied to the cyber domain. Such mapping and scripting can be modified and further detailed for specific crime scenarios and graphically represented. In addition to cyber crime, such mapping can also be used for cyber-attacks of any kind—and not only for criminal purposes as shown here with cyber-warfare related attacks.

Graphically presenting the sequence of events constituting a cyber crime or attack will allow risk-management teams, forensic analysts, incident-response teams, government authorities, militaries, and law-enforcement agencies to identify the specific stepping stones and pinch points that cyber criminals (or attackers) pass through in committing their crimes. Such work can help to facilitate the identification and testing of effective countermeasures, including mitigation at scale, early prevention, and the development of proportional disruption techniques.

References

Bernik, I 2013, *Cybercrime and Cyber Warfare*. John Wiley and Sons, NJ, U.S.A. (accessed through Wiley online library Aug-Dec 2015)

Brayley, H, Cockbain, E & Laycock, G, 2011, 'The value of crime scripting: deconstructing internal child sex trafficking', *Policing*, vol. 5, no. 2, pp. 132–43.

Borrion, H 2013, 'Quality assurance in crime scripting', Crime Science 2013, 2:6. Available online at: http://www.crimesciencejournal.com/content/2/1/6, viewed 16 November 2015.

CISCO 2014, Annual security report, viewed 15 December 2015. <http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf>.

Clarke, R 2010, *Cyber war*, HarperCollins Publishers, New York, NY, U.S.A.

De Falco, M 2012, 'Stuxnet facts report: a technical and strategic analysis', NATO Cooperative Cyber Defence Center of Excellence, Tallinn, Estonia 2012, viewed 28 August 2016.
<https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf>.

Denker, K 2011, *Cyber war and cybercrime—implications of a vague difference*, viewed 28 August 2016 <https://www.inter-disciplinary.net/wp-content/uploads/2011/04/kaiwpaper.pdf>. Viewed 30 August 2016.

Somer, T, Ottis, R, Lepik, T 2015. "Executive summary and brief: Cyber crime inventory and networks in non-ICT sectors", *The economic impacts of cybercrime*, March 2015, FP7-SEC-2013.2.5-2. D2.2.

ENISA 2015, *ENISA threat landscape 2015*, viewed 18 August 2016. <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015>.

Gartner 2014, "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015", viewed 18 August 2016. <http://www.gartner.com/newsroom/id/2905717>.

Geol, S 2011, "Cyberwarfare: connecting the dots in cyber intelligence", *Communications of the ACM*, vol. 54, no. 8, pp. 132-40.

Goodman, M 2015, *Future crimes*, Random House, New York, NY, U.S.A.

Internet Usage and World Population Statistics 2014, Viewed 18 August 2016 <http://www.Internetworldstats.com/stats.htm>.

Kaspersky 2015, 'The Duqu 2.0.: technical details, viewed 03 September 2016, <https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf>.

Lancaster University 2014, Detecting and preventing data exfiltration, viewed 28 August 2016, <https://www.cpni.gov.uk/Documents/Publications/2014/2014-04-11-de_lancaster_technical_report.pdf>.

Levi, M., Maguire, M., 2004, 'Reducing and Preventing Organised Crime: An Evidence-Based Critique', *Crime, Law & Social Change*, vol. 41, issue 5, pp. 397–469

Hutchins, E.M, Cloppert, M.J, Amin, R.M., 2011. Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Viewed 18 August 2016, <http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>.

Olson, P 2013, *We are anonymous: inside the hacker world of Lulzsec, Anonymous, and the Global Cyber Insurgency*, Back Bay Books/ Little, Brown and Company, Hachette Book Group, New York, NY, U.S.A..

Ottis, R 2008, 'Analysis of the 2007 cyber-attacks against Estonia from the information warfare perspective', *Proceedings of the 7th European Conference on Information Warfare and Security*, Plymouth, UK, 2008, Academic Publishing Limited, Reading, UK, pp. 163-68.

Pakharenko, G 2015, "Cyber operations at Maidan: a first-hand account", ed. K Geers, Cyber war in perspective, NATO CCDCOE Publications, Tallinn, Estonia.

PC World 2012, 'When is a cybercrime an act of cyberwar?', viewed 28 August 2016, <http://www.pcworld.com/article/250308/when_is_a_cybercrime_an_act_of_cyberwar_.html>

RSA 2015, Cybercrime 2015: an inside look at the changing threat landscape, viewed 18 August 2016. <https://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf>.

Sharma, Amit 2010, "Cyber wars: a paradigm shift from means to ends", *Strategic Analysis*, vol. 34, no. 1, pp. 62-73, viewed 24 August 2016. <http://www.tandfonline.com/toc/rsan20/34/1>

Trend Micro 2013, 'When do we call a cyber-attack an act of cyber war?', viewed 10 September 2016. <http://blog.trendmicro.com/trendlabs-security-intelligence/when-do-we-call-a-cyber-attack-an-act-of-cyber-war/>.

United Nations Office on Drugs and Crime 2013, *Comprehensive study on cybercrime*, United Nations, February 2013, <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

Weedon, G 2015, "Beyond 'cyber war': Russia's use of strategic cyber espionage and information operations in Ukraine", *Cyber war in perspective*, ed. K Geers, NATO CCDCOE Publications, Tallinn, Estonia.

Appendix 3

Publication III

Somer, Tiia; Tiido, Anna; Sample, Char; Mitchener-Nissen, Timothy. Application of journey mapping and crime scripting to the phenomenon of trolling. Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018 : National Defence University, Washington DC, USA, 6-9 March 2018

Application of Journey Mapping and Crime Scripting to the Phenomenon of Trolling

Tiia Somer, Tallinn University of Technology, Estonia
Dr. Anna Tiido, University of Warsaw, Poland
Dr. Char Sample, ICF International
Dr. Timothy Mitchener-Nissen, Trilateral Research Ltd.

tiia.somer@ttu.ee
anna3399@gmail.com
charsample50@gmail.com
tim.nissen@trilateralresearch.com

Abstract: Cyber attacks and the terms “cyber warfare” and “information warfare” have entered everyday language, and as a result a new class of adversarial toolsets have emerged. Tactically speaking, cyber attack campaigns today follow techniques and patterns that are similar to those used by cyber criminals: DOS attacks (Ottis 2008), information gathering malicious software (Kaspersky 2015), sophisticated targeted weapons (De Falco 2012), and espionage and infiltration for data exfiltration (Lancaster University 2014). Having analysed writings on cyber warfare (Bernik, 2014, Clarke 2012, PC World 2012) and cyber crime (Goodman 2015, Olson 2013), we have concluded that, with the exception of the intent and end goals, the underlying attack cycle remains the same: attack preparation, attack execution and exit upon completion of goal.

This paper discusses how methods from typically non-cyber disciplines can be applied to the cyber domain. By providing a visual representation in the form of *criminal journeys* this paper clarifies how such mappings can assist in building understanding of the steps adversaries undertake, in addition to supporting in the identification and development of effective and proportional countermeasures.

Our work has deconstructed the lifecycle of cyber-attack events and translated these entries into a visualisation map, highlighting key steps an attacker takes during the lifecycle in the preparation and execution of trolling, where the authors have applied this

methodology. We apply the definition of Jalonen et al. (2016): “Trolling is a phenomenon that is experienced in the interactions between internet users, with the aim of changing behaviour, altering reasoning and values, or simply gaining a strong response from as many users as possible by using offensive, emotionally-charged content”. Our work focuses on the motivation and activities of human trolls, with particular interest in the so-called *hybrid-trolls*. We examine trolling by mapping this as a crime script, with specific interest placed on the activities of hybrid trolls supporting pro-Russian political agenda within Estonia.

Keywords: cyber crime, cyber warfare, journey mapping, crime scripting, attack visualisation, hybrid trolling, information warfare.

Introduction

While organisations and individuals are quick to exploit the business and personal benefits of internet, they often give less consideration that cyberspace offers the same benefits to those who wish to attack them. Wall states that the advancement in technologies enables the criminals to commit many smaller crimes instead of one large scale crime, bringing them more benefits in total, with lesser chances of getting caught (Wall, 2007). Hillman, Procyk and Neustaedter have argued that internet has brought crime to a “global business”, where anyone anywhere can commit crimes against anyone anywhere (Hillman, Procyk and Neustaedter, 2014).

Warren et al have used literature around science communication to deduce that developing a common language can potentially allow different parties involved in fighting cyber crime and in the criminal justice process to understand each other better (Warren et al, 2017). We believe that for cyber attacks this can be achieved by expanding on the concept of crime scripting used in criminology. This will allow combining technical aspects of conducting cyber attacks with psychological and economic aspects, such as intent, decision-making, business processes, behaviour, etc.

While there are numerous papers about crime scripts in criminology, academic works on utilising crime scripting for cyber crimes are lacking (Warren et al, 2017). The “Cyber Kill Chain” (Hutchins, Cloppert, and Amin, 2011) provides a good base into understanding

the cyber attack event chain, however, the current work attempts to simplify the process further. In criminology, crime scripts were first introduced by Cornish, turning a crime from single event to a process (Cornish 1994). Further, Levi has proposed that crime scripting is an important means to understand complex crimes (Levi 2008).

This paper proposes that the methodology of journey mapping and crime scripting can be used to deconstruct different types of cyber attacks including those related to trolling. Rather than focusing on solely technical elements, our work includes other aspects of the attack related to an attacker's intent, resources, interactions between all players in an attack process, preparation for and execution of an attack, their desired end state and exit strategy. This is significant as understanding the whole sequence of events in an attack is a critical component in finding weak points in the adversary's strategy and tactics. As a result, it can give a better oversight on where to best focus countermeasures. Some examples include but are not limited to policy initiatives, awareness campaigns, legislative/ regulatory changes, development of new technological applications, and/or behaviour modification of potential victims or even running relevant prevention campaigns to raise awareness and open dialogue with those who might wish to undertake malicious activity ahead of planning and execution.

Journey mapping

The exponential growth of cyber attacks, including those with an information warfare component, has provided enormous challenges to law enforcement authorities, militaries, forensic experts, but also policymakers at different levels. By leveraging the literature around science communication, Warren et al., have concluded that the act of developing a *common language* is an important step in enabling those different parties involved in (a) fighting cyber crime and (b) the wider criminal justice process, to better understand each other. We assert that this common language can be achieved without completely reinventing the wheel, but by using a multi-disciplinary approach, drawing on existing knowledge from economics, criminology and sociology. In so doing, the technical aspects of conducting cyber crime with psychological, sociological and economic aspects can be better understood. Economic aspects include business processes and cost-benefit analyses, while behavioural aspects include values, desires and intent. Combined together, these aspects support the decision-making processes of the cyber attackers.

Journey mapping is a methodological tool that has traditionally been used in business to map customer experience, as well as in criminology, generally under the name of crime scripts. Journey mapping is also often used by strategy consultancies and public organisations to shape customer strategies and public service transformational programmes. In criminology, crime scripts have been used to deconstruct complex crimes into component parts even from a relatively small data set.

A script is a predetermined, stereotyped sequence of actions that define a well-known situation in a particular context (Schank and Abelson 1977, Borrion 2013), or more succulently "[a] script is simply a sequence of actions which make up an event" (Brayley et al 2011, p.133). Scripts are related to the concept of schema, i.e. "abstract cognitive representations of organised prior knowledge, extracted from experiences with specific instances" (Fiske et al 1980, Borrion 2013). As opposed to the "Cyber Kill Chain" introduced by Lockheed Martin (Hutchins, Cloppert, and Amin, 2011) – which provides a good base into understanding the cyber attack event chain – the current work attempts to simplify the process into as few steps as possible while still including all the mandatory phases an attacker must pass through to complete their intended attack. In criminology, crime scripts were first introduced by Cornish (Cornish 1994), turning a crime from single event to a process. Following this, crime scripting has been identified as an important means to understand complex crimes (Levi 2008).

Developing journey maps for schematically representing cyber attacks provides a visual picture of an anticipated sequence of events comprising an attack. Warren et al., further note that a good crime script must not only explain the whole crime process, but should also identify critical pinch points where countermeasures can be effectively utilised. The value of journey mapping as an attack analysis mechanism lies in exactly those aspects – the identification of pinch points and the ordered steps an attacker takes in conducting attacks. These pinch points become counter measure entry points enabling: legislative/ regulatory changes, new technological protections, counteractions, behaviour modification, and/or increased monitoring.

Ideally, data from multiple attack campaigns should be collected and observed to identify common events and behavioural (both human and machine) responses. These commonalities allow for more robust problem modelling leading to more resilient solutions. Additionally, this process can lead to the more accurate identification of pinch points.

We have previously applied journey mapping to firstly deconstruct, and then overlay, multiple cyber crime types with the aim of understanding and constructing/ mapping (a) specific cyber crimes, as well as producing a master script that can encompass the whole attack process for any attack (E-CRIME, 2015). In addition to their application in the cyber crime and forensics contexts, this methodology has the potential to find effective countermeasures (from policy, military, technical to law enforcement perspectives) for different stages of attacks. Journey mapping is an effective method for understanding the activities an attacker takes during different attack phases, while also showing different players involved in an attack. Rather than focusing solely on technical elements, journey mapping will show other aspects of the attack related to an attacker's intent; resources; interactions with and between all players in the attack process; preparation for and execution of an attack; and their desired end state and exit strategy.

While journey mapping has developed good practices (see Borrion, 2013), neither standardised rules for visualising the journey nor specific crime scripting software currently exists (Brayley, 2011). As a result, we have used our own symbols and drawings when constructing our maps. We grouped similar actions under broad terms: intent, preparation, execution, and exit strategy. Having analysed related literature on cyber warfare (Clarke 2010) and cyber crime (Goodman 2015, Olson 2013), we have concluded that even though the intent and end goals are different, the underlying attack cycle, as well as toolsets and methods remains largely the same: starting with attacker's intent, preparations for the attack, executing the attack, and ending in exit strategy.

Description of a general attack process

Cyber attacks related to crime and warfare can be viewed as a process where resources are required and decisions are taken at different stages in the process. This general attack

process has been developed by using literature review, interviews with experts and studying real-life cyber attacks. Four phases are critical to the development of our journeys from the perspective of the perpetrator: intent, preparation, execution and exit phases.

Any attack will start with an intent phase. When developing a script for a specific pre-selected crime, the intent phase is often omitted. This is justifiable as, beyond the initial decision/intent to commit a specific offence, the criminal's intention will often not modify, or otherwise exert meaningful influence upon, the following phases of the selected crime. For example, when developing a crime script for pickpocketing, the initial starting point is that the criminal intends to steal items being carried in the pockets of victims without their awareness. In this situation, the intention of the attacker (theft with subterfuge) largely pre-dictates the subsequent decisions to be taken in the preparation, execution and exit phases. Furthermore, for *crimes of opportunity* the attacker may not have held any pre-existing intention to commit a crime before the situation presented itself.

However, for certain attack types the intentions of the attacker are important as they directly influence their choices within the subsequent phases. For example, in the case of cyber crime where there exists a wide suite of potential attack forms, the motivations of the attacker act as a filter by narrowing the range of attack types available to the rational attacker. For example, when the attacker's motivation is financial reward, a rational attacker will employ appropriate attacks that achieve their intention, such as: ransomware/ransomworms; CEO fraud; and other well documented cyber crime types. Conversely, an activist attacker motivated by some cause or personal ideology may wish to disrupt the operation of their target, thus employing DDoS attacks, hacking and defacing websites, etc.

Note that as stated above, the attackers *intention* can influence their decision-making in the subsequent phases. Nevertheless, possessing the intention to commit an attack does not mean the potential attacker will actually *decide* (or possess the necessary

capabilities) to commit that attack – the decision to commit the attack occurs during the preparation phase and is influenced by multiple factors.

The preparation phase includes pre-attack actions: making a decision to attack, analysing the worthiness and/or reasons for undertaking an attack, identifying potential victims/targets, conducting targeted reconnaissance, and potentially conducting a risk/benefit analysis based on anticipated rewards. The reconnaissance phase provides the information necessary for attack planning. In this stage, the attacker chooses an attack method (potentially influenced by the intention phase as discussed above). An analysis their own means and capabilities leads to a decision point of self or outsource required attacking capabilities. Should the attacker decide to outsource any or part of the operation additional decisions are made and steps taken, but that discussion is out of scope for this study; however those actions are all part of this reconnaissance phase.

The execution phase commences with drawing an attack plan and executing the attack. Execution goals are typically to deny, destroy, deceive or disrupt. The execution includes entering the target system and conducting criminal activities in support of the goals. In the case of certain intentions/motivations, lateral movement within the target system to find additional opportunities for action/exploitation may be necessary and/or beneficial. In other cases, such as where the intention is disruption or denial, lateral movement may not be necessary.

The exit phase includes direct or indirect gain for the cyber attackers and culminates in an exit strategy. At this the authors feel it is important to point out that the existence of an exit strategy is contrary to the Cyber Kill Chain model of persistence. This is relevant since the longer an attacker exists in the compromised environment the greater their chance of discovery (SANS Institute 2016). One additional note is that within a specific crime journey, the perpetrator can:

a) loop back to an earlier step where required (for example, if a chosen attack method fails such that they need to employ a different strategy/attack-method, or if they “accidentally” discover additional unforeseen vulnerabilities to take advantage of);
b) repeat steps where necessary; or

c) quit their attack once they realise the efforts are not worth the risk or potential benefits.

As stated previously, this methodology can be applied to cyber attacks in general, keeping in mind the specificities of crime, cyber and information warfare.

Trolling

It can be said that the phenomenon of trolling is difficult to define. It has been used a lot in recent media accounts, and is a term widely discussed without a precise definition. Merriam-Webster (2017) defined the term trolling as “to antagonize (others) online by deliberately posting inflammatory, irrelevant, or offensive comments or other disruptive content”. This definition defines the behaviour, but places no limits on the contextual environment. Trolling has a long history, and even though it has not been equated as such, for as long as chat-rooms and other discursive environments have existed, people have had fun posting deliberately irritating comments to solicit the annoyance of others. The research outlined in this paper focusses primarily with online trolling in the context of pro-Russian trolling operations in Estonia.

Furthermore this research uses the online trolling definition from Jalonen et al., (2016). According to this, “trolling is a phenomenon that is experienced in the interactions between internet users, with the aim of changing behaviour, altering their reasoning and values, or simply gaining a strong response from as many users as possible by using offensive, emotionally-charged content”. There have been many publications concerning the types of trolls from the psychological viewpoint. For example, Stanford University research (Cheng et al 2017) came to a conclusion that mood can influence the trolling behaviour of an ordinary citizen.

In the political context, mainstream media largely addresses the trolling phenomenon in connection with international politics, speaking about "troll armies" employed by governments. This is the specific type of trolling that has a unique role in information warfare discussions and represents the area of interest in our paper. These equate to the so-called hybrid or government trolls, who are either paid by, or volunteering to support, the state in furthering an ideological purpose. According to Spruds et al. (2015), hybrid trolls are those employed for information warfare and do not act on their own accord.

Where classic trolls act with no apparent overarching strategy or purpose, hybrid trolls communicate to discredit a particular ideology and operate under the direction and orders of a particular state or state institution (NATO STRATCOM COE, 2014). While out of the scope of current work, we acknowledge the existence of so-called robotrolling; i.e., the coordinated use of fake accounts on social media (NATO STRATCOM COE, 2017). Social media platforms by virtue of becoming news sources without journalistic standards of veracity and reliability (Vasterman, 2005), have become tools of social control. According to Bradshaw and Howard, the trolls who use social media in this manner, are a part of cyber troops; defined as government, military or political-party teams committed to manipulating public opinion over social media (2017). Cyber troops actively engage with users by commenting on posts that are shared on social media platforms. The interactions can be either negative, positive or neutral. (Bradshaw and Howard 2017). Cyber troops can be subdivided into: government-based troops (public servants tasked with influencing public opinion); politicians and parties; volunteers; and paid citizens (Bradshaw and Howard 2017).

Russian trolling in Estonia

"Trolls" act as the instruments to aid in the implementation of a pro-Russian propaganda system. They are a technique of information of information warfare: these recruited commentators distribute the messages of Russia's political leaders online. The role of such trolls has been widely documented (Pomerantsev & Weiss, 2014; Jaitner & Mattsson, 2014; Smoleňová 2015; Volodymyr, 2016; Bradshaw & Howard, 2017). The Russian investigative journalist Garmazhapova, who went undercover in a pro-Putin social media commenting office in St Petersburg in 2013, dubbed the commentators "trolls" and their office a "troll factory" (Aro 2016). The research has shown that trolling is used to support a pro-Russian narrative that is initially disseminated by state-controlled traditional media (NATO STRATCOM COE 2014). Thus, the trolling operations are very much designed to support the Russian disinformation machine and spread fake news (Pomerantsev & Weiss, 2014; Jaitner & Mattsson, 2014; Smoleňová 2015; Volodymyr, 2016; Bradshaw & Howard, 2017).

These trolls comment on political issues, for example events in Ukraine (Volodymyr, 2016), and their disinformation is designed to manipulate the receiver's feelings; a form

of perception management. Younger and more visually-oriented people are lured in with memes, caricatures and videos (Volodymyr, 2016). On the one hand, the creation of trolls' memes is not simplistic: both targeting and memes-wording are carefully crafted to achieve the intended goals. On the other hand, the messages themselves are sometimes simple in nature: i.e., Western political leaders are often depicted as "Nazis" or "fascists", images of corpses and alleged war crimes committed by Ukrainian soldiers are distributed, as well as photos of Ukrainian teenage girls wearing t-shirts with Nazi symbols on them, however it would appear from the literature that such images have been edited in Photoshop (Aro 2016).

In Estonia, research from Mattiisen, Zurawski and Supinska (2017) reveals that the operations in social media have intensified after the occupation of Crimea and the war in eastern Ukraine. One of the ideas behind these tactics seems to be the destabilization of Western societies (Pomerantsev & Weiss, 2014; Jaitner & Mattsson, 2014; Volodymyr, 2016). Among the themes are: the violation of human rights of Russian speaking minorities; anti-NATO rhetoric; and instigating the fear of immigrants and refugees. NATO is usually depicted as being provocative, and surrounding Russia by troops (Mattiisen, Zurawski and Supinska 2017).

On Facebook, there also exist Russian-friendly communities operating in both Estonian and Russian languages. The main discussions developed there are the likes of "Putin's greatness" substantiated by his capability to deal with homosexuals and immigrants (Mattiisen, Zurawski and Supinska 2017).

The reasons behind trolling activities can be varied. There are certainly politically minded citizens in the Russian community of Estonia who do trolling and the spreading of fake news on their own free will. This equates to the simple malicious use of social media platforms. However, state-sponsored trolling, that exploits the same free speech mechanisms, can be viewed as cyber crime; thus, our methodology of journey-mapping can be applied. In this case, the desire is rather connected to the policy of the state, and the executers are merely applying different strategies.

We concentrate on the analysis of trolling in Estonian media, the usual topics which provoke trolling (strong emotional response) are:

1) The alleged discrimination of Russian minority, rescue of discriminated Russians (e.g. Russian language education);
2) The history of the World War II, Victory Day dividing the communities' understanding of history;
3) The presence of NATO troops, Western threat to Russia;
4) The attacks on the Western way of life, e.g. LGBT issues, the concentration on Western problems such as refugees, migrants.
5) Attacks on perceived native cultures by Western countries and institutions such as the internet (Ristolainen 2017)

Trolling can also be automated, one example was researched recently by NATO STRATCOM Center of Excellence (2017). The research concentrated on the mentioning of Baltic states, Poland and NATO troops in Twitter. The majority of postings (around 70%) in the Russian language on these topic were made by bots (NATO STRATCOM COE, 2017).

Application of journey mapping to trolling

As cyber crime is a quickly evolving field, academic literature on specific aspects of it is relatively scarce. We therefore relied on experts and practitioners in the field of information security, law enforcement and other relevant authorities, as well as independent researchers as the key sources of information on cyber crimes. Based on the review of existing literature and expert interviews we concluded that cyber crimes usually take place in three stages: preparation, execution and monetisation and grouped those similar actions under broad terms.

Our previous work (E-CRIME, 2015) developed eight cyber criminal journeys:

- Building a botnet;
- Extortion (ransomware);
- Espionage (APT/ APA);
- Malware development/ zero-day exploit development;
- Cryptocurrency mining;

- DRM cracking;
- VoIP attacks;
- Click Fraud

This selection of journeys was based on commonalities between different crimes as provided for in existing literature and the results of expert interviews. For each script, a mapping was conducted in three principal phases of cyber crime: preparation, execution and monetization. Since there are no standard rules or specific software for crime scripting (Brayley 2011), we have used our own symbols and drawings. These journeys have been validated in the EU FP-7 E-CRIME project's validation workshop, held in Rome on January 19-20, 2015.

Having scripted the eight different types of cyber crime as stated above, a general crime script has been developed. This work has deconstructed the lifecycle of crime events and translated these into a visualisation map to show the full event process. These scripts help identify the cyber criminals' *modus operandi*, an account of how they operate within a crime cycle from preparation to monetization and exit. It will also provide a sense of the processes and practices through which cyber crime occurs.

Based on literature review and expert insight, we have mapped the phenomenon of trolling on a crime script journey (Figure 1). The underlying intent behind trolling is usually of political nature, i.e. influencing the activities and actions within a state - in our case influencing the agenda in Estonia according to from a pro-Russian agenda.

In preparation of trolling activities an initial decision to engage in influencing a state's agenda is taken, followed by risk assessment and final decision to launch operations. Thereafter, trolling is chosen as an attack method - often times accompanied with activities using methods of traditional information warfare. For trolling, two possible avenues are possible - using existing means and capabilities, or recruiting trolls. Trolls can be recruited by means of regular job advertisements, "compatriot organisations" may be used, or the operations may be executed using "useful proxies". The means used for trolling could be fake accounts, identity theft, influence operations, information operations or troll armies.

In the beginning of execution phase, the desired end state, minimum acceptable goals and an exit strategy in the form of attack plan are formulated. There are various options to implement trolling. One of those is purchasing or Influencing media outlets, or alternatively by broadcasting own media in target state. Other options include spreading disinformation, spreading provocative information or manipulating existing information, or influencing user actions. Trolling can take place on most popular social media platforms, in traditional media, newsgroups or forums in the form of providing comments, or in blogs/ vlogs. Trolling may use text, still imagery, video or audio online to distribute hate speech, harassment, disinformation, incite violence, provoke distrust in authorities, or simply conduct propaganda operations.

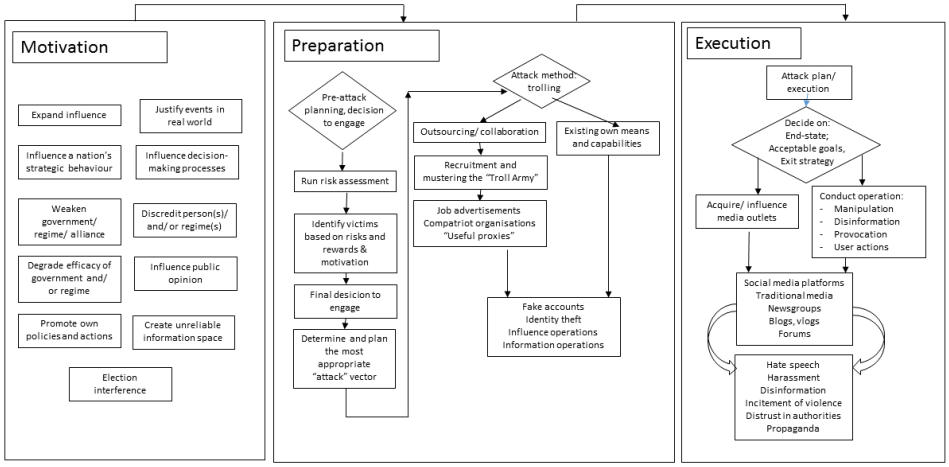

Figure 1. Mapping trolling on a cyber attack journey

Potential application of trolling journey: developing countermeasures

Having mapped trolling on the cyber criminal journey gives opportunities to map and develop potential countermeasures (Figure 2).

Various options are possible - in the intent phase, most of the countermeasures are policy-oriented. These can be actions of government authorities in the national and international arenas, diplomacy-related activities, as well as countering adversary activities in the influencing of public opinion and creating own reliable information space.

Where the trolling activities are politically motivated, the hand-off between those planning or mandating the action to those responsible for the execution and delivery is a potential pinch-point.

In the preparation phase and with the intent of influencing Russian-speaking population, the national authorities should mainly focus on "useful proxies" and compatriot organisations to distribute own agenda, countering that of the adversary. The use of fake accounts can be countered by cooperation with social media platforms so that the creation and use of fake accounts can be discovered well in advance. This may include the development of relevant technical capacities. Identity theft can be countered by increasing awareness among general population on this. Information and influence operations can be fought using traditional and non-traditional capabilities of information warfare.

The execution phase could be countered by making the operations as difficult as possible. The ownership of traditional media can probably not be influenced in our Western societies, but potential avenues for this should be explored. Counteractions can include provision of more support to public media outlets. Information operations can be countered by counteroperations, and the means used in these information options would reflect the means used in countering these and could be adjusted according to the nature of such operations.

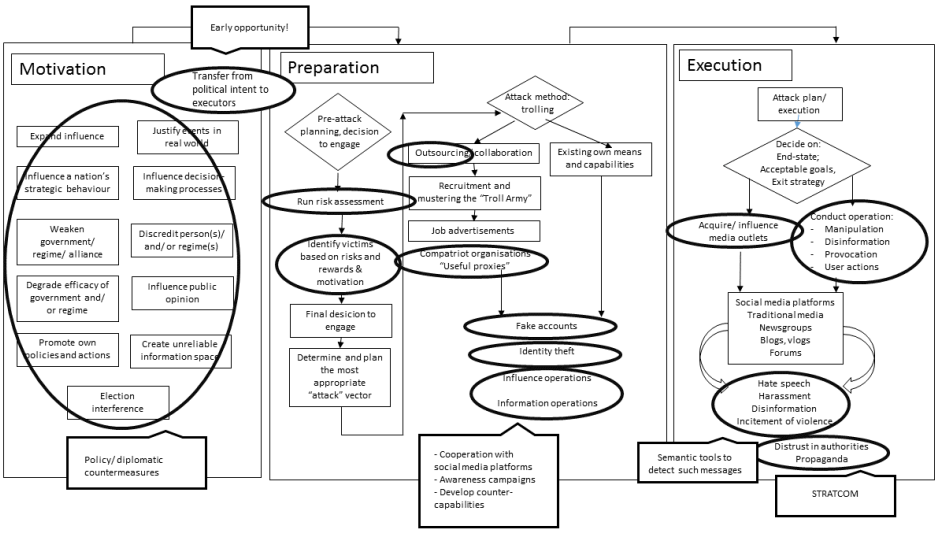

Figure 2. mapping potential high-level countermeasures to trolling on an attack journey

Conclusion

Within this article, the authors have shown how traditional crime scripting can provide useful insights into understanding the lifecycle of a general cyber attack journey. The article also shows how methods and techniques from typically non-cyber disciplines can be successfully applied to the cyber domain. Such mapping and scripting can be modified and further detailed for specific scenarios and can then be represented graphically. In addition to cyber crime, such mapping can also be used for cyber attacks of any kind – and we have applied it to the phenomenon of trolling.

Graphical presentation of the sequence of events constituting a cyber crime or attack will allow different authorities to identify the specific stepping stones and pinch points that cyber attackers pass through in the conduct of operations. Such work can help to facilitate the identification and testing of effective countermeasures, as shown for the case of trolling. Only high-level countermeasures are shown in the current work. Our future work will go further, and look at more specific countermeasures that include – but are not be limited to – mitigation at scale, early prevention, and the development of proportional response or disruption techniques.

Cyber attacks can be seen as a process, where resources are required and decisions are taken, constituting the modus operandi of a crime. In the current work, we provide a script for trolling, developed on the basis of previous work on a general cyber crime cycle. The work undertaken is based on literature reviews and expert interviews.

This work is useful to several organisations as it shows how cyber attacker mapping can help to facilitate the identification and testing of effective countermeasures. This is significant because understanding the whole sequence of events in an attack can help in finding weak points in the adversary actions. As a result, it can give a better oversight on where to best focus our own actions in the fight against cyber attacks: high-level policy initiatives, counteroperations, awareness campaigns, legislative/regulatory changes, development of new technological applications, and/or increased monitoring by relevant authorities.

Bibliography

Bernik, I. (2014) “Cybercrime and Cyberwarfare”, John Wiley & Sons, Inc., Hoboken, USA.

Borrion, H. (2013) “Quality assurance in crime scripting”, Crime Science 2013. Available online at: http://www.crimesciencejournal.com/content/2/1/6

Brayley, H., Cockbain, E., Laycock, G. (2011) “The value of crime scripting: Deconstructing Internal Child Sex Trafficking”, Policing, Volume 5, Number 2, pp. 132–143

Cheng, J., Bernstein, M., Danescu-Niculescu-Mizil, C., Leskovec, J. (2017) “Anyone Can Become a Troll -Causes of Trolling Behavior in Online Discussions”. Available online at: http://cs.stanford.edu/~jure/pubs/trolling-cscw17.pdf

Clarke, R. (2012) Cyber War. New York, HarperCollins Publishers, 2012.

Cornish, D.B. (1994) “The procedural analysis of offending and its releavnce for situational prevention”. Crime Prev. Stud. 3, 151-196 (1994)

De Falco, M. (2012). “Stuxnet Facts Report. A technical and Strategic Analysis”. NATO Cooperative Cyber Defence Center of Excellence, Tallinn, 2012. Available online at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf

The Economic Impacts of Cyber Crime (2015) FP7-SEC-2013.2.5-2. D2.3 “Detailed appendixes on cyber crime inventory and networks in non-ICT sectors”. Sõmer, T., Ottis, R., Lepik, T., Lagazio, M., Hallaq, B., Simms, D., Mitchener-Nissen, T.

Fiske, S., Linville, P. (1980) „What does the Schema Concept Buy us?“ Personality and Social Psychology Bulletin. Vol 6, No 4, Available online at: http://journals.sagepub.com/doi/pdf/10.1177/014616728064006

Goodman, M. (2015). Future Crimes. New York, Random House

Hillman, S., Procyk, J., Neustaedter, C. (2014). “Tumblr fandoms, community and culture”. In: Proceedings of the Companion Publication of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing, pp285-288. ACM, February 2014

Hutchins, E., Cloppert, M., and Amin, R. (2014). Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Available online at: https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Jaitner, M., and Mattsson, P.A., (2014). Russian information warfare 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, NATO CCD COE Publications, Tallinn

Jalonen, H.,Paavola, J., Helo, T, Huhtinen, A.-M. (2016). “Understanding the Trolling Phenomenon: The Automated Detection of Bots and Cyborgs in Social Media”. Journal of Information Warfare, Vol 15, No 4.

Kaspersky (2015) “The Duqu 2.0. Technical details”, available online at: https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

Lancaster University (2014) “Detecting and Preventing Data Exfiltration”. Available online at: https://www.cpni.gov.uk/Documents/Publications/2014/2014-04-11-de_lancaster_technical_report.pdf

Levi, M. (2008) “Organized fraud and organizing fraud. Unpacking research on networks and organizations”. Criminol. Crim. Justice 8 (4) 389-419

Merriam-Webster, Inc, (2006) “Webster's ninth new collegiate dictionary”. Merriam-Webster https://www.merriam-webster.com/dictionary/troll

NATO StratCom Center of Excellence (2014) “Analysis of Russia’s Information Campaign Against Ukraine”. http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine

NATO StratCom Center of Excellence (2017) “Robotrolling”. www.stratcomcoe.org/robotrolling-20171

Olson, P. (2013) “We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency”. Hachette Book Group

Ottis, R. (2008) “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective”. Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited, pp 163-168.

PC World (2012) “When Is a Cybercrime an Act of Cyberwar?” Available online at: http://www.pcworld.com/article/250308/when_is_a_cybercrime_an_act_of_cyberwar_.html

Pomerantsev, P. Weiss, M. (2014). „The menace of unreality: How the Kremlin weaponizes information, culture and money“. The Interpreter, 22.

Ristolainen, M. (2017). „Should 'RuNet2020' be taken seriously? Contradictory views about cybersecurity between Russia and the west“, Proceedings of the 16th European Conference on Cyber Warfare and Security, Dublin, Ireland, pp. 391 - 400.

Sans Institute (2016) Incident Response Capabilities 2016, available online at: https://www.sans.org/reading-room/whitepapers/analyst/incident-response-capabilities-2016-2016-incident-response-survey-37047

Schank, R. C., & Abelson, R. P. (1977) „Scripts, plans, goals, and understanding“. Hillsdale, NJ: Lawrence Erlbaum Associates, 1977

Spruds, A., Rožukalne, A., Sedlenieks, K., Daugulis, M., Potjomkina, D., Tölgyesi, B., Bruge, I. (2015) “Internet Trolling as a Hybrid Warfare Tool. The Case of Latvia”. Available at: http://www.stratcomcoe.org/download/file/fid/3345

Volodymyr, H., (2016). “The “Hybrid Warfare” Ontology”. Фахове видання з економічних, філософських, політичних наук Затверджено постановами Президії ВАК України від 26 січня 2011 р. № 1

Wall, D. (2007) “Cybercrime the Transformation of Crime in the Information Age”, Polity, Cambridge vol.4.

Warren S., Oxburgh G., Briggs P., Wall D. (2017) “How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?” In: Tryfonas T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science, vol 10292. Springer, Cham

Appendix 4

Publication IV
Somer, Tiia. Taxonomies of Cyber crime: an overview and proposal to be used in mapping cyber criminal journeys. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019 : University of Coimbra, Portugal, 4-5 July 2019

Taxonomies of Cyber crime: an overview and proposal to be used in mapping cyber criminal journeys

Somer, Tiia. Tallinn University of Technology, Department of Software Sciences
Tiia.Somer@taltech.ee

Abstract: Is cyber crime different from „traditional crime"? Is there such a thing as cyber crime? There are several proposals for definition of cyber crime, and several analyses and proposals for a taxonomy. This paper presents an overview of currently available taxonomies and considers how useful these could be in mapping cyber criminal journeys. In order for individuals, enterprises and states to be informed about the motivations, methods and modi operandi of cyber criminals and thereby begin to protect themselves, it is useful to understand how a cyber crime takes place from its initial stages of motivation and intent, until exit. This paper uses the methodology of journey mapping as a basis for proposing a four-level taxonomy of cyber crime. This is significant because a common framework and taxonomy will help to more effectively analyse, as well as find targeted preventive and awareness-building measures in the fight against cyber crime.

Keywords: taxonomy, cyber crime, journey mapping

1. Introduction

In order to better understand cyber crime, its processes, and tactics, techniques and procedures used by cyber criminals, we need a robust framework. This paper reviews a number of well-known taxonomies and approaches used currently, and analyses if these can be used to understand cyber criminal journeys. Cyber crime is a vast and growing problem internationally. Cybercriminal revenues have reached 1,5 trillion USD annually in 2018 (McGuire 2018). The main goal of cyber criminals is to gain some kind of personal benefits: often times it is financial, but not only. Other goals might be curiosity, thrill, distribution of illegal material, harassment, influencing populations, espionage, stealing of intellectual property, etc.

2. Existing taxonomies

Currently there does not exist a universally accepted definition of cyber crime, and this is reflected in the taxonomies that have been developed. Some of the definitions and classifications follow the logic used for "traditional crimes", others use approaches based on technology, adversaries or threats, for yet others law is the basis. Common points do exist among these taxonomies, but there are differences in structure, definitions and content. There is a clear distinction between the approaches using technical nature of cyber crime as basis on one hand and those using impacts of crime as basis on the other hand. Researchers have studied aspects of crime, such as technical (e.g. malware types and prevention of these) aspects of execution of crimes, or human aspects (human error, victimisation, etc.), but understanding of cyber crime as a process and system remains less developed. The current approaches to studying cyber crime are based on law, impacts, victims, methods and attack vectors, criminals/ attackers, motivations of perpetrators and criminal gain.

Current taxonomies and approaches to building a taxonomy are based on one of the following:

- Approaches based on criminology
- Approaches based on technologies, adversaries and threats
- Two dimension taxonomies
- Three dimension taxonomies
- Proposals by international bodies

2.1. Approaches based on criminology

Approaches based on criminology are built on traditions of criminal justice and they see cyber crime as regular crime, where computers are a tool which are enablers for "traditional" crimes. Brenner (2006) states that the definition of cyber crime as "a crime committed on a computer network" should reflect existing legal frameworks, both national and international. Brenner also discusses differences between cyber crime and cyberterrorism, and notes that crimes are in general committed for personal gain or personal revenge. Terrorism has different motives, but may use the same methods, and the same applies to cyber warfare where the techniques used may be identical to cyber crime.

Wall (2007)	Three different types of crime	- Traditional crimes, committed through use of ICT - Partially new crimes, modified crimes - New crimes, enabled by ICTs

Table 1. Taxonomy based on criminology

2.2. Approaches based on technological aspects, attackers, attack vectors or threats

A different approach has technological aspects, attackers, attack vectors or threats as a basis, or the aspects of computer and network infrastructure as targets. These proposals use the nature of computer security flaws as a basis, look at existing data on security incidents, look at adversaries and attacks, or impacts.

Landwehr et al (1994)	The nature of computer security flaws as a basis	- Flaws by genesis (how the flaw arises) - Flaws by time of introduction - Flaws by location (hardware and software)
Howard (1997); Howard and Longstaff (1998)	Based on existing data on security incidents	- Attackers (hackers, criminals, terrorists, vandals) - Tools (scripts, toolkits, user commands) - Access (implementation or design vulnerabilities, access permissions) - Results (corruption, deletion or disclosure of data, theft of resources, denial of service) - Objectives (intellectual challenge, peer status, financial gain, damage)

Hansman and Hunt (2005)	Four-category model	- Attack vectors (the means by which the target is reached) - Targets (hardware, software, network, data) - Specific vulnerabilities and exploits (security flaws) - Payload (the outcome and effects)
Kjaerland (2005, 2006)	Built on earlier work and added a quantitative component	- Source sectors (top level domains) - Method of operation (resource theft, social engineering, malware, denial of service) - Impact (disruption, distortion, destruction, disclosure) - Target services (commercial or governmental)
Meyers et al. (2009)	Based on attack vectors	- Viruses; - Worms; - Trojans; - Buffer overflows; - Denial of service; - Network attacks; - Physical attacks; - Password attacks/user compromise; and - Information gathering
Simmons et al. (2014)	AVOIDIT taxonomy	- Attack Vector - Operational Impact - Defence - Information Impact - Target
Rogers (1999, 2001, 2006)	Adversaries	- Script kiddies, newbies, novices; - Hacktivists, political activists; - Cyberpunks, crashers, thugs; - Insiders, user malcontents; - Coders, writers; - White hat hackers, old guard, sneakers; - Black hat hackers, professionals, elite; - Cyberterrorists

Table 2. Taxonomy based on technological aspects, attackers, attack vectors or threats

2.3. Two-dimension and three-dimension taxonomies

Some authors have proposed two dimension taxonomies to classify cyber crime into two categories, and others have proposed three-dimensional taxonomies of cyber crime.

Furnell (2001), Koenig (2002), the Australian High Tech Crime Centre (2003), Lewis (2004), and Wilson (2008), Foreign Affairs and International Trade of Canada (2004)	Two-dimensional classification of crimes	- crimes committed using computers and networks (hacking, viruses); - traditional crimes that are facilitated by the use of computers (illegal pornography, online fraud)
Alkaabi et al. (2010)	Two-dimensional classification of crimes	- Type I crimes, where the computer, computer network, or electronic device is the target of the criminal activity - Type II crimes, where the computer, computer network, or electronic device is the tool used to commit or facilitate the crime
Wall (2007)	Three- dimensional classification of crimes	- Computer integrity crimes (hacking, cracking and denial of service attacks, activities that prevent legitimate access to systems or modify, corrupt or delete software and data). - Computer-assisted crimes (virtual robberies, scams and thefts). - Computer content crimes (digital storage and communication of pornography, violence and offensive materials)
Goodman (1997)	Three types of cyber crime	- crimes in which the computer is the end target - crimes where the computer is the tool - crimes where there is an incidental presence of computer equipment
Ghernaouti (2013)	Distinguished cyber crime from cyberconflicts, wars and terrorism	- Cyber crimes against people (including activities affecting their dignity and integrity, frauds, identity crimes and privacy related offences); - Cyber crimes against assets (including the theft of data, the theft of services and resources, counterfeiting, software piracy, surveillance and espionage, manipulation of information, fraudulent acquisition of intellectual property); and - Cyber crimes against states (including destabilization, information warfare, and attacks on critical infrastructures)

Table 3. Two-dimension and three-dimension taxonomies

2.4. Taxonomies proposed by international bodies

Another set of taxonomies are those proposed by international bodies. These are significant because of their visibility and influence in shaping policies and providing a framework for legislation. The best known among these are the Council of Europe Convention on Cybercrime, The UN Manual on the prevention and control of computer related crime (1999) and a three domain taxonomy proposed by INTERPOL.

Council of Europe Convention on Cybercrime		- Offences against the confidentiality, integrity and availability of computer systems and data - Computer related offences (forgery, fraud) - Content related offences - Offences related to infringements of copyright and related rights - Dissemination of racist and xenophobic materiel, and threats and insults motivated by racism or xenophobia, through computer systems
The UN Manual on the prevention and control of computer related crime (1999)	Proposed to address the problems of international cooperation in computer crimes and criminal law	- Fraud by computer manipulation - Computer forgery - Damage to or modification of computer data or programs - Unauthorised access to computer systems and services - Unauthorized reproduction of legally protected computer programs
INTERPOL	Three domain taxonomy	- Attacks against computer hardware and software (botnets, malware and network intrusion) - Financial crimes (online fraud, penetration of online financial services and phishing) - Abuse (especially of young people, in the form of grooming or 'sexploitation')

Table 4. Taxonomies proposed by international bodies

The review of taxonomies and approaches shows that while there is agreement on the importance and growing significance of cyber crime, there is no consensus on a common definition or taxonomy.

Some proposals for the definitions and classifications follow the logic used for "traditional crimes", others use approaches based on technology, adversaries or threats, yet others use law to base their proposals on. The main difference in these taxonomies arises from the basic definition: what is cyber crime? Some authors consider any crime, involving computers at any stage, a cyber crime (pure cyber crimes, cyber-enabled and cyber-dependent crimes), others consider only "pure cyber crimes" or "cyber-

dependent" crimes as cyber crimes. There are common points in all of these taxonomies, but the structure, definitions and content differ. There is a clear distinction between the approaches which use technical nature of cyber crime as basis on one hand and those using impacts of crime as basis on the other hand. Researchers have studied aspects of crime, such as technical aspects (e.g. malware types and prevention of these) of execution of crimes, or human aspects (human error, victimisation, etc.), but understanding of cyber crime as a process and system remains less developed.

The cyber crime ecosystem is dynamic, and constantly evolving (McGuire 2018), therefor it is not easy to apply any of the existing taxonomies to thoroughly understand cyber crime.

3. Cyber criminal journey mapping

Cyber crimes can be seen as a process where resources are required and decisions are made, which together constitute the modus operandi of a crime. In order to understand cyber criminal modi operandi, we have in our previous work undertaken an exercise to map cyber criminal journeys – how a crime is conducted, from the criminal view. Journey mapping is a method which utilises methods from various disciplines – criminology, information security, military science, economics – with the aim to understand how a crime takes place. In our work, we have explained a crime in four principal stages: intent/ motivation; preparation; execution; and monetization and exit. This work is significant as it allows us to understand cyber crime as a process, and can provide different stakeholders involved in investigation, fight against, and prosecution of cyber crimes a common platform for understanding cyber crimes.

In our effort to model cyber criminal processes we have used phase-based approach, customer journey mapping and crime scripting. Phase-based approach has been used in the armed forces (U.S. Department of Defence, 2007) to find capability shortfalls and make decisions on the development of new capabilities (Tirpak, 2000). Mapping is also used in business to map customer satisfaction, and crime scripting is used in criminology to map criminal journeys throughout a crime cycle. Given the complex nature of cyber crime, it is valuable to gain deep understanding of the mechanics of it. We analysed several crimes and took them apart, thereafter made generalisations for similar types of crime (DDOS, Malware development, DRM cracking, VoIP attacks, extortion, espionage, IP theft, crypto cracking). In essence, our mapping used attack vectors, providing a sequence of actions making up a crime event, generalised from a number of known crimes.

In analysing different types of cyber crime, it has been difficult to come up with a usable taxonomy that would let us best break the crime down to small parts. The schematic representation of sequence of actions provides us with a cognitive representation of how we believe a sequence of events will occur (Abelson 1981, Borrion 2013), e.g. the steps a criminal makes in an attempt to commit cyber crime. Such scripting can be used to present different crimes, but are believed to be of particular use for new or complex crimes (Brayley et al 2011). Levi and Maguire (2004) have suggested, in their review of organised crime reduction strategies, that such scripts could be used as an innovative way to get a more detailed understanding complex new crimes. Our initial analysis of cyber crime was based on attack vectors. Having modelled these, it became apparent

that the steps criminals pass in different phases for the different attack vectors do not differ between themselves too much. In our modelling it became evident that there are four main aspects that need to be considered: criminal, attack vectors, victim, and criminal gain. Also it became clear that there is a need for a taxonomy.

4. Proposed taxonomy for mapping cyber criminal journeys

The main difficulty in creating a taxonomy of cyber crime is the definition of crime, which is a legal issue. Crimes exist when they are identified as such in legislation, and this is done in specific national contexts. Cyber crime is an international phenomenon, and this makes its study even more difficult and creates additional problems of terminology and taxonomy.

In our approach, we have not considered cyber-enabled crime as cyber crime, rather such crimes are enablers of cyber crime. We have defined cyber crime as "pure" and "cyber-dependent" cyber crimes, i.e. such crimes, that would not happen without the use of ICTs. The aim of mapping cyber criminal journeys is to understand how a crime takes place from the criminal's point of view. Important aspects in this process are the criminal, his/ her motivations, victim, impacts on him/her, attack vectors and methods, and criminal gain, or exit from crime journey. Schematically this can be represented as follows:

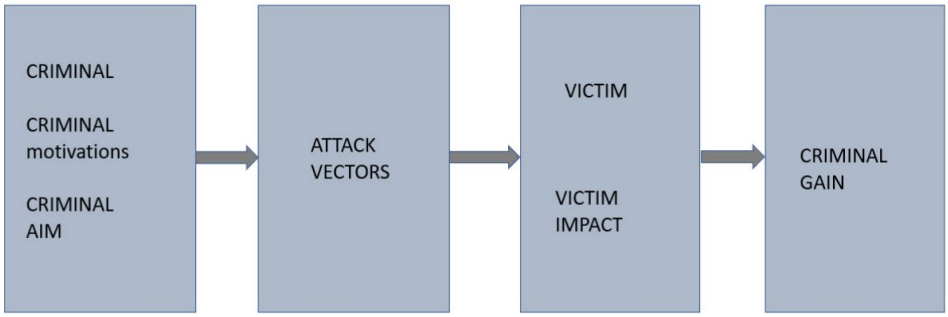

Figure 1: Actors and aspects in a cybercriminal cycle/ journey

A robust taxonomy is seen as an essential starting point to addressing these questions. The need for a taxonomy to respond to cyber crime is a practical measure: without an understanding of cyber crime, meaningful responsive measures cannot be developed (Moitra 2005). Any taxonomy created can not be a static or complete document. This is so due to the connected digital world that we live in, the ever-evolving nature of cyber crime, ever-evolving cyber criminal ecosystem, and the varied legal frameworks.

The principal objective in conducting cyber criminal journey mapping is to understand how a cyber crime takes place. Therefore we propose to use an appropriately generic taxonomy, that can be further sub-divided as the processes, actors, tactics, techniques and systems change. After researching various crime types, the cyber criminal ecosystem, victimology and cyber criminal business models, we propose a four-dimensional taxonomy:

- Perpetrator, including their motivation and aim, business models, ecosystem and preparation to conduct the crime;

- Attack vector, including enabling capabilities to conduct the crime;
- Victim, including the impact of crime on victim;
- Exit, including monetization of crime.

The basis for the proposed taxonomy is the underlying crime cycle, or crime journey, i.e. the stakeholders (perpetrator and victim), capabilities (attack vectors, but also preparation for crime), and enablers (monetization of crimes, but also the cyber criminal ecosystem). This classification covers all aspects in a crime and each can be further sub-divided as depicted on Figure 2 and explained below.

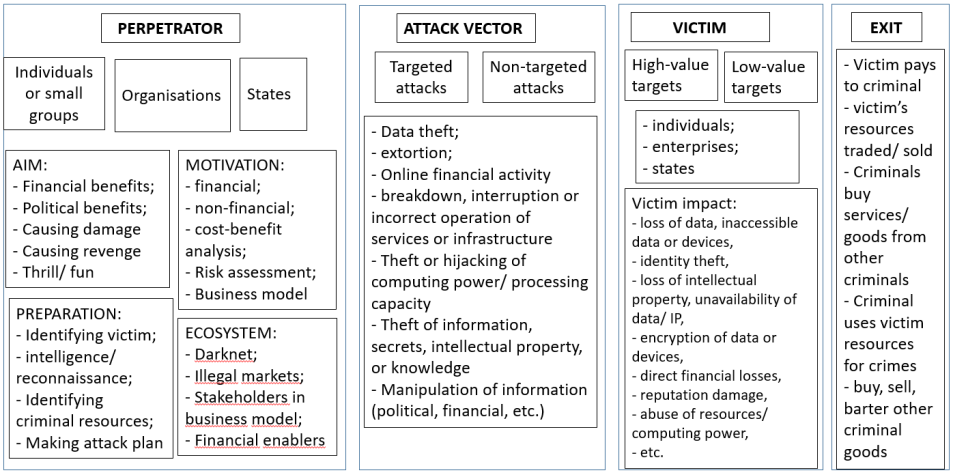

Figure 2. Four-dimensional taxonomy proposed for cyber criminal journey mapping

4.1. Perpetrator

In quite short time cyber crime has moved from low volume crime performed by individuals to being high volume crime, which is organised and industry-like (UN 2013). Published evidence on cyber crime is based on a small number of case studies or interviews, and mostly focus on the methods of the crime (McGuire, Dowling 2013). Research from five or more years ago suggested that the cyber criminal world was not highly organised, however research published within the last few years suggests otherwise. Now there are estimates that more than 80% of cyber crime acts use some kind of organised activity (UN 2013, Broadhurst et al 2014). The UN cyber crime study states that cyber crime often requires a "high degree of organisation to implement, and may lend itself to small criminal groups, loose ad hoc networks, or organised crime on a larger scale", and that the typology of cyber criminal groups reflect that of the conventional world. It also notes that many cyber crime acts require high levels of organisation and considers it likely that conventional organised crime groups are also active in cyber crime. (UN 2013).

Bearing this in mind, cyber criminals can be broadly classified into four general types of players and/or groups, often interacting amongst each other:

1. Individuals and small criminal groups (opportunistic or planned attacks),
2. International criminal organisations,
3. States (i.e. foreign intelligence agencies),
4. Legitimate organisations.

4.1.1. Perpetrator motivations

Criminal motivation, or intent, is where the potential criminal makes a conscious decision to engage in a criminal act. In spite of it being a conscious decision, it doesn't have to be well-reasoned, rational, or completely thought through; and timeframes for decision-making are very short. Having said that, there is an element of rationality, with cost-benefit analysis, risk assessment, etc. interplaying with the decisions to commit a crime. In general terms, perpetrator motivations can be:

1. Satisfaction, peer-approval, publicity, status, revenge, etc.,
2. Challenges, having fun,
3. Organisational/ community obligations (hacktivism, working on behalf of a government organisation or individuals acting on a sense of pride or obligation),
4. Direct or indirect monetary gain.

Based on the above, we propose the following classification for perpetrators:

- Actor (individual, small groups, international (criminal) organisations, states),
- Aim (get financial benefits, get political benefits, cause damage, cause revenge, thrill/ fun,
- Motivation (financial or non/financial, cost-benefit analysis, risk assessment),
- Preparation for conduct of crime (identifying victim, intelligence/ reconnaissance, identifying criminal resources, making attack plan)

4.2. Victim

People and organisations/ enterprises usually fall victim to cyber crime through either their actions or non-actions. One can fall victim during the course of their use of information technology, i.e. using e-mail, browsing the web, using removable media, or by not taking appropriate action to keep their systems or use of systems secure, i.e. bad password management; not updating or poor management of systems, software or hardware. Once falling victim to cyber crime, the victim will face damages.

The impacts of, or damages from, cyber crime can be loss of data, hijacked accounts, loss of intellectual property, unavailability of data/ IP, inaccessible data or devices, encryption of data or devices, identity theft, direct financial losses, reputation damage, abuse of resources, abuse of computing power, etc.

Victims can be either high or low value targets. Adopted from Ghernaouti (2013), victims of cyber crime can broadly be classified into three general categories:

3) individuals (identity crimes, privacy related offences, direct financial crimes, extortion, etc);
4) enterprises (theft of data or intellectual property, theft of services and resources, counterfeiting, economic espionage, etc;
5) states (destabilization, information or cyber warfare, attacks on critical infrastructures).

4.3. Attack vectors

Typical attacker modus operandi is gaining or blocking access to a victim's data, device, or functionality (European Police Force, 2014). The overview of current taxonomies and approaches to cyber crime presented earlier in this paper, show two approaches in presenting attack vectors: 1) concrete technical means of conducting attacks (viruses, worms, Trojans, denial of service, network attacks, user compromise, etc.); 2) general attack methods (unauthorised access, malicious codes, interruptions of services, theft or misuse of data/ devices).

For discussing attack vectors in the journey mapping context we propose to use a general approach of attacks (such as theft of data, extortion, etc.), which can be further sub-divided into enablers (such as malware, botnets, ransomware, etc). Attacks can further be subdivided to be either targeted or non-targeted attacks. The attack vectors proposed are the following:

- Data theft
- Extortion
- Online financial activity
- Breakdown, interruption or incorrect operation of services or infrastructures
- Theft or hijacking of computing power/ processing capacity
- Theft of information, secrets, intellectual property, or knowledge
- Manipulation of information (political, financial, etc)

4.4. Exit strategies

In general, the gain from cyber crime can be divided into two: financial gain or non-financial gain. An exit strategy is a "means of leaving one's current situation, either after a predetermined objective has been achieved, justifying premises or decision makers for any given operational planning changed substantially, or as a strategy to mitigate imminent or possible failure". In the case of financially motivated crime, monetization as a separate phase will come into the picture. In cases of hacktivism, or state-sponsored actions, the monetization phase is (often, but not always) excluded.

A financially-motivated attacker must decide who and what to attack, attack successfully and then monetize access. In general, there are five options to generate income:

- Victim pays to criminal directly (e.g. extortion);
- Victim's resources are turned to tangible assets (i.e. victim's resources will be sold and traded);
- Criminal pays for goods and/or services to another criminal (real money, cryptocurrency, re-sellable money equivalents, or goods and services);
- Criminal gets access to victim resources and uses these for other (criminal) actions;
- Buying, selling or bartering other (sometimes illegal) goods and services.

In terms of cyber crime, an exit strategy will let the criminal decide when to leave the crime scene, either for the risks or costs overweighing the benefits, for not being able to make enough profit, or simply for risks of getting caught by law enforcement authorities.

The exit strategy will also cover hiding one's tracks and analysing law enforcement agencies' abilities to infiltrate crime rings or their capabilities of investigating crimes.

5. Future work

Future work to validate this taxonomy will be undertaken in the form of case studies with real-life cyber crime cases in the second half of 2019, in cooperation with police forces from Estonia, Germany and the U.K.

6. Conclusion

Cyber crime as being a vast and growing problem is acknowledged widely. Even so, the understanding of cyber crime as a complete system or process is not studied in detail, and to a big extent this is influenced by the lack of appropriate taxonomy. Any taxonomy to be used in mapping cyber criminal journeys should be appropriately generic and based on stakeholders and actions interacting within a cyber crime cycle. Therefor we propose a four-dimension taxonomy:

- Perpetrator, including their motivation and aim, business models, ecosystem and preparation to conduct the crime;
- Attack vector, including enabling capabilities to conduct the crime;
- Victim, including the impact of crime on victim;
- Exit, including monetization of crime.

The basis for the proposed taxonomy is the underlying crime cycle, or crime journey, i.e. the stakeholders (perpetrator and victim), capabilities (attack vectors, but also preparation for crime), and enablers (monetization of crimes, but also the cyber criminal ecosystem). This classification covers all aspects in a crime and each is further sub-divided.

We believe that this generic taxonomy will allow us to analyse and develop a better understanding of cyber crime as a process and system, where criminals and victims interconnect with each other and where attack vectors, enablers and exit strategies from crime are analysed in a systematic context. This is significant because it would help develop an understanding of how cyber crime business processes, but also tactics, techniques and procedures utilised by criminals function. This could potentially lead to identifying pinch points in the cyber crime processes, find better countermeasures, and develop novel policy or technical approaches in the fight against cyber crime.

References

Alkaabi A, Mohay G, McCullagh A, Chantler A. (2010). Dealing with the problem of cybercrime. Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime. Abu Dhabi

Australian High Tech Crime Centre (AHTCC). (2003). Fighting the Invisible. Platypus Mag J Aust Fed Police. 2003;80:4–6

Brenner SW. (2006). Cybercrime, cyberterrorism and cyberwarfare. Rev Int Droit Penal. 77(2006/3):453–71

Borrion, H. (2013). "Quality assurance in crime scripting", Crime Science 2013, 2:6. http://www.crimesciencejournal.com/content/2/1/6

Brayley, H, Cockbain, E, Laycock, G. "The value of crime scripting: Deconstructing Internal Child Sex Trafficking", Policing, Volume 5, Number 2, pp. 132–143

Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime

Clarke, Ronald R. (ed.). (1997). Situational Crime Prevention: Successful Case Studies. Second Edition. New York: Harrow and Heston

Council of Europe Convention on Cybercrime (2001).

Foreign Affairs and International Trade Canada. (2004). Available from: http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp

Furnell S. (2001). The Problem of Categorising Cybercrime and Cybercriminals. 2nd Australian Information Warfare and Security Conference. Perth, Australia; 2001. p. 29–36

Ghernaouti S. (2013). Cyberpower: Crime, Conflict and Security in Cyberspace. EPFL Press
Goodman M. (1997). Why the Police Don't Care about Computer Crime. Harv J Law Technol. 1997;10(3):465–94

Hansman S, Hunt R. (2005). A taxonomy of network and computer attacks. Comput Secur. 2005;(21):31–43

Howard J. (1997). An analysis of security incidents on the internet, 1989-1995. Carnegie Mellon University; Available from: http://www.cert.org/archive/pdf/JHThesis.pdf

Howard J, Longstaff T. (1998). A common language for computer security incidents. Sandia National Laboratories; 1998. Report No.: Technical Report SAND98- 8667. Available from: http://www.cert.org/research/taxonomy_988667.pdf

Interpol (2014). Available from: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Kshreti N. (2006). The Simple Economics of Cybercrimes. IEEE Secur Priv. 2006;4(1):33–9 Landwehr C, Bull A, McDermott J, Choi W. (1994). A taxonomy of computer program security flaws, with examples. ACM Comput Surv. 1994;26(3):211–54

Kjaerland M. (2005). A classification of computer security incidents based on reported attack data. J Investig Psychol Offender Profiling. 2005;(2):105–20.

Kjaerland M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. Comput Secur. 2006;(25):522–38

Koenig D. (2002). Investigation of Cybercrime and Technology-related Crime.

Levi, M. and Maguire, M. (2004). "Reducing and Preventing Organised Crime: An Evidence-Based Critique", Crime, Law & Social Change

Lewis B. (2004). Preventing of Computer Crime Amidst International Anarchy [Internet]. 2004. Available from: http://goliath.ecnext.com/coms2/summary_0199- 3456285_ITM

McGuire, M. (2018). Into the Web of Profit. Understanding the Growth of Cybercrime Economy. Bromium

Meyers C, Powers S, Faissol D. (2009). Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches. Lawrence Livermore National Laboratory; 2009 Apr. Report No.: LLNL-TR-419041

Moitra S. (2005). Developing Policies for Cybercrime. Eur J Crime Crim Law Crim Justice. 2005;13(3):435–64.

Rogers M. (1999). A new hacker taxonomy. University of Manitoba.

Rogers M. (2001). A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study. University of Manitoba.

Rogers M. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. Digit Investig. 2006;(3):97–102

Simmons C, Shiva S, Bedi H, Dasgupta D. (2014). AVOIDIT: A Cyber Attack Taxonomy. Proceedings of the 9th Annual Symposium on Information Assurance (ASIA '14). Albany, NY, USA; 2014.

Tirpak, J. (2000). Find, Fix, Track, Target, Engage, Assess. Air Force Magazine, 83:24–29, 2000. URL http: //www.airforce-magazine.com/MagazineArchive/Pages/2000/July%202000/0700find.aspx

United Nations manual on the prevention and control of computer-related crime (1999). United Nations

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime

U.S. Department of Defense (2006). Joint Publication 3-13 Information Operations, February 2006. URL http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Wall D. (2007). Cybercrime. Cambridge: Polity Press

Williams L. (2008). Catch Me If You Can: A Taxonomically Structured Approach to Cybercrime. Forum on Public Policy

Wilson C. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and policy issues for congress.

Appendix 5

Publication V

Somer, Tiia. Modelling financially motivated cyber crime. to be published in Proceedings of the 16th International Conference on Cyber Warfare and Security, ICCWS 2021 : Tennessee Tech University and the Oak Ridge National Laboratory USA. 25-26 February 2021.

Modelling financially motivated cyber crime

Somer, Tiia. Tallinn University of Technology, Department of Software Sciences
Tiia.Somer@taltech.ee

Abstract: Development of information and communications technologies have greatly affected the way societies, economies and people operate. Worldwide internet usage has increased from 1.7 billion users in 2009 to more than 4.1 billion users in July 2019. The internet and ICT-s have provided opportunities and benefits to governments, businesses and people. On the other hand, it has also made everyone vulnerable to those who wish to attack them. Lone criminals and criminal organisations worldwide have access to powerful capabilities, which they use to identify and target their victims and commit cybercrimes. The reasons for this vulnerability are two-fold: first, governments, societies and businesses are ever more dependent on cyberspace; and second, our understanding of cybercrime remains limited. Cybercrime is a relatively young area of academic research, which has risen both theoretical and practical interest. Yet very few published studies have researched cybercrime as a process, which includes both technical and non-technical aspects. Cyber criminals are increasingly using new technologies, but also developing novel techniques, procedures and business models for their criminal purposes. This paper proposes a process model for financially motivated cybercrime, a practical tool which can be used by various stakeholders in the cybercrime investigation and prevention process; one which is explanatory and has flexibility. The model developed provides a step-by-step account of actions taken by the criminals throughout the crime. It is not intended to be a rigid or linear model but a flexible tool to understand the key steps within a cybercrime process, allowing us to identify major decision points the criminals pass through. By modelling and understanding cyber criminal processes, better oversight on investigations, countermeasures and disruption techniques can be formulated. This has the potential to overcome the challenges in understanding cybercrime across various players involved in the cybercrime investigation process. The aim is to allow those investigating cybercrimes or developing countermeasures to quickly apply new crimes to the model and focus on the specific known (or unknown) decision points in order to conduct their work more effectively.

Keywords: cyber crime, modelling, ecosystem, cyber crime process

Introduction

Cyber crime is a relatively young area of academic research, and very few published studies have researched cyber crime as a process, which includes both technical and non-technical aspects. Technical factors of executing cyber attacks (including crime) have been researched to a large extent, but understanding the dynamic and constantly changing process, or system, of cyber crime has not

received as much attention. Developing a model for financially motivated cyber crime has the potential to provide a different view on how cyber crime happens, thereby providing better options to investigate such crimes, find or develop new countermeasures or develop awareness building measures.

A successful cyber crime means the criminal has to take a series of consecutive steps [23]. In modelling, these steps are combined into logical groupings and further into phases, thereby creating a process. The cyber criminal processes are often referred to as cyber kill chains or cyber-attack life cycles, consisting of a number of phases. They are practical representations, which describe cyber crimes or attacks from different stages.

Cyber crime as a process

Maimon and Loderback [23] divided successful hacking acts into four stages: initial stage (preliminary investigation on potential targets' vulnerabilities and intelligence gathering); second stage which makes use of results of initial stage and infiltrates the target asset; third stage, elevating privileges and conducting the actual crime; and final stage where the criminals cover up evidence [23].

Hutchins et al [20] proposed the widely acknowledged Cyber Kill Chain concept, which defined intrusion as an end-to-end chain process, consisting of seven steps: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

Hewlett-Packard's Attack Life Cycle [21] consists of 10 stages: reconnaissance, attack delivery, exploitation, installation, command and control, regional seizure, internal exploration, elevation of privilege, channel creation, and information theft. HP's approach is different from LM in one aspect: the stage after the attacker has penetrated the target system is further subdivided into internal search, elevation of privilege, and information theft, and their proposed life cycle does not include weaponization.

MITRE corporation has proposed ATT&CK Matrix, which is a "knowledge base of adversary tactics and techniques based on real-world observations" [88]. It is essentially adversary behaviour model reflecting attack life cycle. The ATT&CK Matrix divides adversary actions to 12 steps: initial access, execution, persistence, privilege escalation, defence evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact; each step is divided into techniques utilised by adversaries [88]. A PRE ATT&CK model has also been proposed to reflect actions prior to the actual attack, i.e. in finding targets and taking preparatory steps.

Early theoretic script approach is illustrated by what is commonly known as Restaurant script [96], describing a customer perspective of eating in a restaurant. This is comprised of four phases: entering the restaurant, ordering a meal, eating the meal and leaving the restaurant, each phase consisting of explicit steps [97]. Customer journey mapping allows businesses to "understand

customers' experiences when they interact with the steps involved in a service" (called touchpoints), in order to provide better services [108]. Customer journey mapping has not only been applied to sales, but to other areas from health care to library science [108]. Journey mapping is also often used by strategy consultants and public organisations to shape customer strategies and public service transformational programmes.

Crime scripts are used as "an increasingly popular method for understanding crime by turning a crime from a static event into a process, whereby every phase of the crime is scripted" [66]. In crime scripting, "a script is considered a predetermined, stereotyped sequence of actions that define a well-known situation in a particular context" [97]. Crime scripts are schematic representations explaining "how knowledge is organised about how to understand behavioural processes" [97], or how we believe a sequence of events will occur [102]. As scripts alone could not explain how an event happens, they were described in a broader framework to include goals and plans; based on the idea that goals are achieved by a sequence of events [96]. It has been argued that crime scripts are effective in helping to understand criminal's behaviour and routines during the crime process [10].

Crime scripting is a systematic methodology [3] that generally relies on qualitative data and behavioural decision-making. It classically involves breaking down the actions of the criminal into four main stages - preparation, pre-activity, activity, and post activity, with each stage concentrating on the main elements of a crime. Classically, the most important information gathered is how the criminal conducts the crime and what decisions they make along the way. There are numerous papers about crime scripts in criminology, there is almost none about utilising crime scripting for cyber crimes [10].

In modelling financially motivated cyber crime, it is concluded that the crime scripting approach of preparation and pre-activity come together as preparation phase, activity is the execution phase and post-activity means exit phase, as depicted on Table 12.

Crime scripting	**Modelling financially motivated cyber crime**
1. Preparation 2. Pre-activity	1. Preparation
3. Activity	2. Execution
4. Post-activity	3. Exit

Table 12. Adapting crime scripting methodology to modelling financially motivated cyber crime

Figure 31 presents the financially motivated cyber crime as a process model. The model is a result of generalisation after analysing several cyber crime types. It must be noted that the emphasis of different phases differs according to crime type. For example, in crimes which are more socially focussed (i.e. CEO fraud, ransomware attacks, payment scams, romance scams, etc.) the main emphasis is on the preparation phase, whereas the more technical cyber crimes (where cyber systems are targets) the main emphasis is on the execution phase. In developing the model the specific crimes were deconstructed and modelled, then specific models were generalised to develop a general process model. As cyber crime is constantly innovating both in terms of business models and technological approaches, it is clear that any process model can not be exhaustive. The aim of current modelling approach is to present a general process model, which can be used to deconstruct cyber crime and improve general understanding of the modus operandi of criminals. The model does not intend to build a linear process, steps can be omitted, any previous steps can be reverted back to as needed, or when a course of action taken presents another criminal opportunity. The model is intended to be a guide for identifying criminal actions and decision points throughout a crime cycle. In investigating cyber crime, the analysts can use the model to quickly understand which steps in the crime process are known or unknown and which need more detailed investigations. In the efforts to prevent cyber crime, the model can help to identify where preventive actions should be focussed: for awareness-building of potential targets or developing additional technical countermeasures. Organised (cyber) crime relies heavily on processes, which can be explained by the developed model. In the efforts to develop legislative countermeasures, it can provide an understanding of decision points within a crime cycle. This, in turn, can provide guidance in efforts to adapt or develop legislative measures in targeting the criminal processes and decision points. The general model can also be effectively used for training law enforcement authorities as a quick understanding of this phenomena.

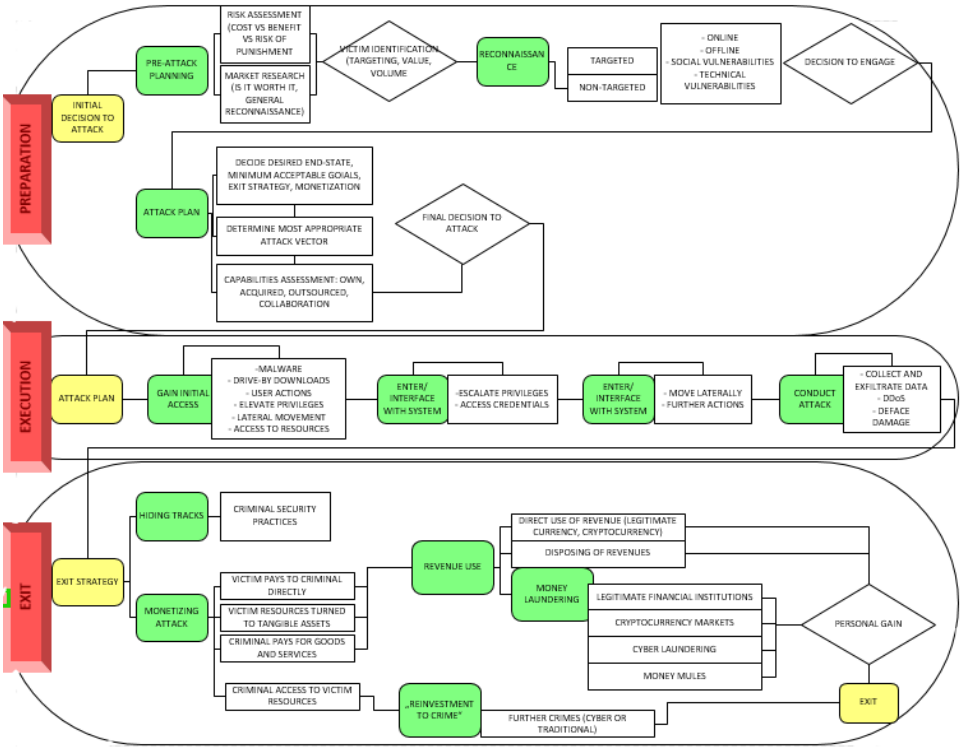

Figure 31. Cyber crime as a process model

Preparation phase of a crime

Victims can in general be divided to two groups: high-value targets and low-value targets. The criminal in general has two options in conducting the crime: victim-oriented (targeted) or attack method oriented (opportunistic, non-targeted) approach. In the case of victim-oriented approach, the victim is identified first. High-value targets are specifically chosen for their personal or business significance. The criminals may want to attack a specific company or person, or to gain access to the data of a specific individual. In following attack method oriented approach, the criminal wants to use a specific method of attack, and the identity of victim is not important. Such victims can be identified as low-value targets, where criminals cast a "wide net" of attack vectors (spam, malware, etc.) hoping that someone will "take the bait". The criminals may want to exploit victims that share a common property (language, age, occupation, etc.). In terms of planning for the crime the basic steps in the two approaches are the same. For example, in cases of extortion (socially constructed extortion, or attacks using ransomware) will be prepared the same way. The difference is on emphasis of separate steps: for targeted or victim-oriented approach the role of reconnaissance will play a more significant role than in attack-method oriented approach, where reconnaissance will play a less significant role.

The preparation phase is concerned about the planning of the crime, identifying victim and conducting reconnaissance on the victim, making an attack plan with choice of attack vector(s), and assessing existing capabilities. This is an iterative process of getting ready to conduct the crime. In case the reconnaissance step shows other potential criminal avenues, the criminal may abandon their preliminary idea and change focus, or they may decide to conduct multiple crimes instead.

The preparation phase has two main components:

- Decision to conduct crime. They perform “market research”, determine and weighing the risks, costs and benefits of options. This is a major decision point within a crime cycle: if the risks or costs outweigh benefits, they may decide not to conduct the crime. on the other hand, the criminals may also act opportunistically, with no serious consideration of potential outcomes of their actions.
- Identification of potential victims, investigating their technical and social vulnerabilities. This is done by conducting both online and offline reconnaissance. Here the criminals, based on their intelligence-gathering on targets, look into capabilities needed and decide if they have their own capabilities, if they should purchase the capabilities from another criminal, or if they should outsource the conduct of the crime. Final conscious decision is made to execute the criminal act, and attack methods and tactics to be used are decided.

The two components of preparation phase can further be translated into four major steps: pre-attack planning, reconnaissance, attack plan, and capabilities assessment, further sub-divided as depicted on Figure 32. The phase ends with the criminal being ready to engage and move on to the next stage of a crime, execution phase. Some form of preparation phase always precedes execution and usually determines how it will be implemented.

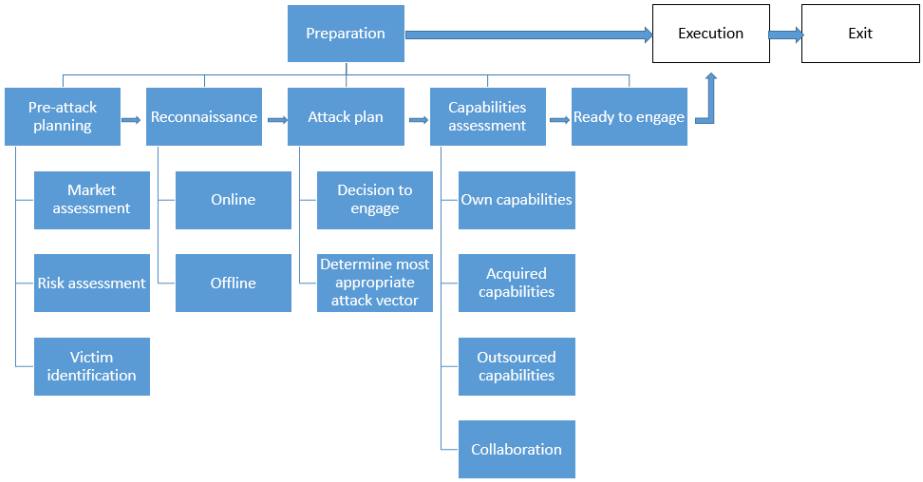

Figure 32. Elements of preparation phase of cyber crime

The pre-attack planning step concerns mostly around the question “Is it worth it?”. Market assessment is conducted in the case of enabling capabilities (CaaS, Botnet development, Malware development, etc.). Risk assessment usually deals with weighing the potential benefits against the risk of getting caught and punishment. At the end of this step, target victim is identified. In the case of a targeted attack, victim is identified first, then risk assessment conducted; and market assessment will not be of significant importance.

The aim of reconnaissance step is to find weaknesses in chosen victim: people-related, organisation-related or technology-related. An important part in many cases of cyber crime is the conduct of a simple social or technical information gathering and weakness identification. Social information gathering uses simple internet search of social media or traditional media, other websites, social or professional relationships. Technical information gathering will attempt to find critical technical elements and includes, among others, network architecture, IP space, network services, email format, and (security) procedures. In identifying technical weaknesses, the reconnaissance will attempt to find vulnerabilities in victim systems. The research of target is not relevant in some cases of more technically-focussed cyber crime (developing malware, botnets, other relevant capabilities, or in cases of non-targeted attacks).

Having conducted pre-attack planning and reconnaissance, the criminal will develop an attack plan. This will include the final decision to conduct a criminal act and determining the most appropriate attack vector. The criminals do not necessarily write down or are even not aware of this step, but it will always be present.

In capabilities assessment step, the criminal will identify if they have the capabilities (or ability to develop such capabilities) needed for the crime themselves, or they have to acquire capabilities, outsource the crime itself, or collaborate with other criminals to conduct a wider crime. Upon completion of the preparation phase, the criminal will be ready to engage and the crime process will move to next phase: execution.

It must be noted that the criminal may also move laterally within this phase, when additional opportunities present themselves during any one of the steps identified. The process model for preparation stage is depicted on Figure 33.

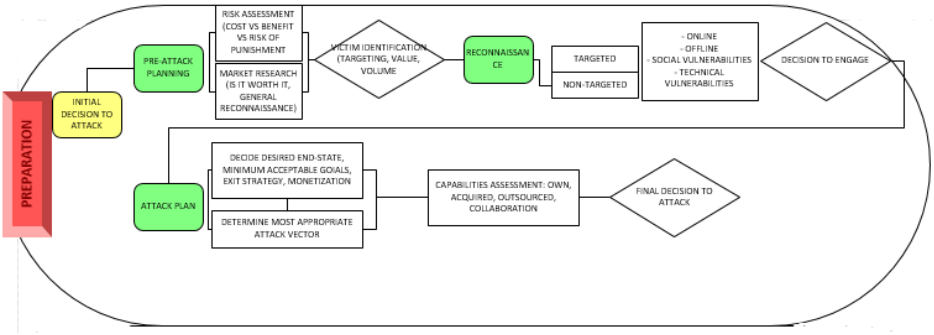

Figure 33. Process model of preparation phase of a cyber crime

Execution phase

The execution phase starts with an attack plan. In the plan the criminals decide upon their desired end-state, minimum acceptable goals, monetization and exit strategies [49] [50] [53]. The attack can be executed in three ways [49]:

- The criminal can use his own means and abilities. In this case the criminal moves to the Execution phase directly. In case he does not possess required capabilities, he will choose one of the two options outlined below,
- The criminal can acquire required means and capabilities from another criminal. In this case there are other criminals involved in the process: a seller/ broker/ deal-breaker, developer and programmer, etc. Any combination of the latter results in the provision of service to the crime originator. There are specific forums, markets and online stores where such “goods” are traded,
- The criminal can outsource the crime. This is the Crime-as-a-service model, where the criminal pays another criminal to conduct the crime. This also takes place on specific forums, markets and online stores.

Following the choice of victim, the attacks can be targeted or opportunistic. The aim of executing the attack could be data theft; extortion; online financial activity; breakdown, interruption or incorrect operation of services or infrastructure; theft or hijacking of computing power/ processing capacity; theft of information, secrets, intellectual property, or knowledge; or manipulation of information, etc.

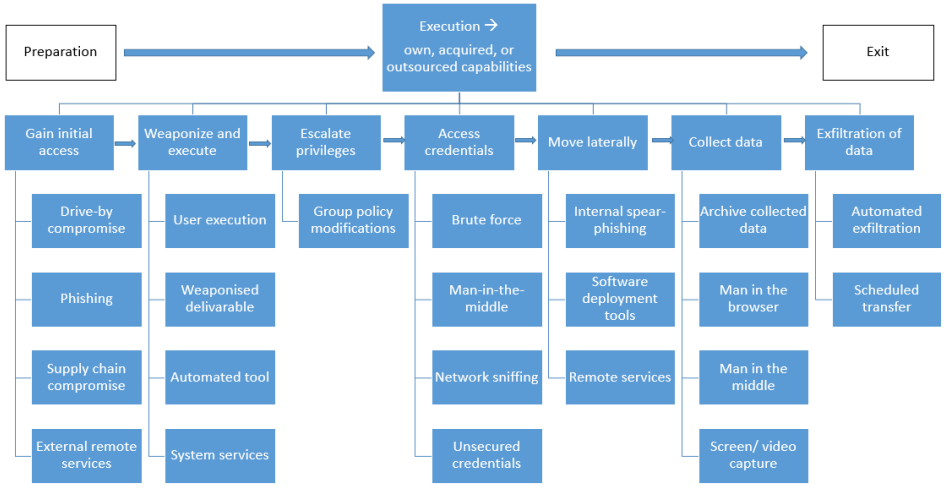

Figure 34. Elements of execution phase of cyber crime

The steps involved in execution phase are (see Figure 34):

- Gaining access to target systems. This can be achieved by using different attack vectors (malware, drive-by downloads, user actions, etc.) or social engineering. The choice of attack vector will become apparent upon the conduct of reconnaissance in the previous (preparation) phase depending on specific vulnerabilities: either people-related, organisation-related or technology-related;
- Entering/ interfacing with target system. Once the criminal gains access to victim system, he will map the compromised network, escalate privileges, and access credentials. This will allow the criminal to enter or interface with target system and based on their desired and decided goals and end-states take actions;
- Accessing target system. Having accessed the target system the criminal may move laterally within this phase, when additional opportunities present themselves during the conduct of the original actions;
- Conducting the attack/ crime. This will be the final step in the execution phase with the aim of collecting and exfiltrating data, DDoS, defacement, or otherwise damaging the victim.

The execution phase is complex and will consist of an operational sequence of many actions: gaining initial access, execution, privilege escalation, credential access, lateral movement, data collection, and exfiltration [88]. Each of these actions will have sub-actions, which will again have sub-actions. These technical aspects of executing an attack have been studied by scholars and practitioners at length (see [49] [20] [23] [44] [47] [88] [104] [50] [46] [53]), and will not be discussed here as the purpose of current modelling of financially motivated cyber crimes is to present a sense of processes the crime goes through.

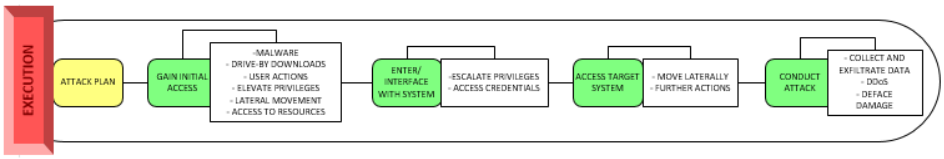

Figure 35. Process model of execution phase of cyber crime

Exit phase

Financial gain is the principal aim for all cyber crime, and the only aim for financially-motivated cyber crime, but knowledge about revenue generation is limited and fragmented [14]. Revenues are generated from illicit online markets, sale of IP and trade secrets, data trading, crimeware and CaaS, malware, botnets, etc. The exit phase of a cyber crime consists of three principal steps: monetising the attacks, hiding tracks, and using revenues.

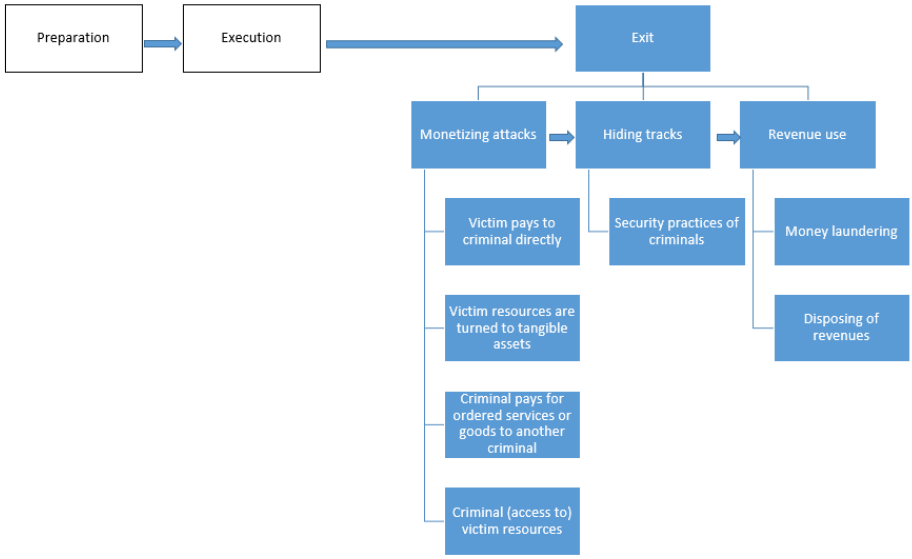

Figure 36. Elements of exit phase of a cyber crime

Attacks can be monetised in one of following ways:

1. Victim pays to criminal directly. This can take place in cases of extortion, such as ransomware or DDoS extortion schemes;
2. Victim resources are turned to tangible assets, and victim resources can then be traded and sold;
3. Criminal is paid for (criminal) goods and/or services by another criminal. Payment can be conducted in real currency, crypto currency, resellable money equivalents (i.e. gaming assets, loyalty points), or in goods and services (real or virtual, legal or illegal);
4. Criminal (access to) victim resources, where the criminal can sell access to victim resources to other criminals. Similar to above, payment can be in real currency, crypto currency, resellable money equivalents (gaming money, loyalty points, etc.), or in goods and services (real or virtual, legal or illegal);
5. Buying, selling or bartering other (legal or illegal) goods and services at dark markets (operations within the cyber criminal ecosystem, supporting further cyber- or traditional criminal activities).

After conducting a successful attack, the criminals must hide their tracks in order to avoid being caught and prosecuted by law enforcement authorities. In order to achieve this, the criminals use several security practices [19], focussed on (but not limited to) protection and anti-forensics.

Having obtained revenues from crime is only one aspect of generating income for criminals. They must convert this revenue into tangible assets or currency

they can use. Money laundering has been a problem for criminals in the offline world for a long time, methods for this have been in use for as long as crime has existed, and new methods brought about by the emergence of digital economy have come to use [14]. Cyber criminals use traditional money laundering means, such as the legal banking system, fake businesses, investments into assets, gambling and casinos, wire transfers, money mules or cash drops [14]. The digital economy has given rise to new forms of money laundering, sometimes referred to as cyber-laundering – involving digital payments, cryptocurrencies, mobile payments, etc.

In addition to money laundering, the criminals spend their profits. There is not a lot of reliable data available on this [14]. McGuire [14] analysed available data (interviews, as well as dark web and open web sources) and concluded that there are five broad categories where cyber criminals use their proceeds: spending on immediate needs (paying bills, buying food, etc.), hedonistic spending (buying drugs, luxury items, prostitution), calculated spending (luxury items to gain status), investments (property, finance, art, etc.), or reinvestment in crime.

Turning cyber crime proceeds into real assets of value, or tangible currency, is challenging for criminals. In order to do so, the criminals are using special enablers brought about by the emergence of digital economy: cryptocurrencies, and specialised web portals offering the sale of property, cars, luxury items, etc. for cryptocurrencies.

By the end of the exit phase, and the overall financially motivated cyber criminal cycle, the criminals have hidden their tracks and ended up with financial gain of some kind, and the cyber criminal process has come to a close. However, the criminals may also reinvest their proceeds into further crime, which will be the start of another process of crime.

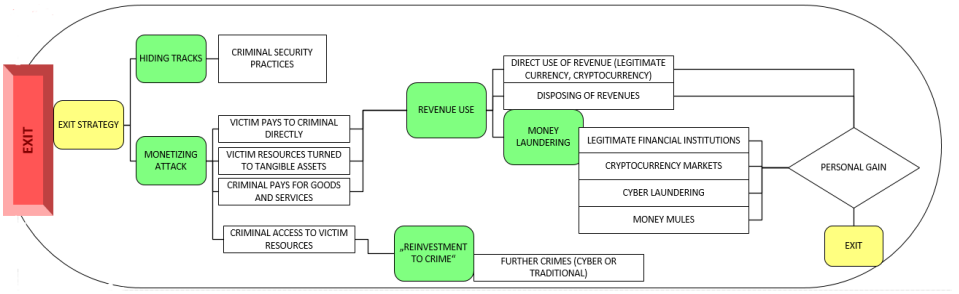

Figure 37. Process model of exit phase of cyber crime

Expert assessment

Expert assessment to the methodology was sought in two ways: validation events (workshops and trainings); and interviews. In total, four workshops and

training events were conducted, all followed by feedback survey on the usability of the proposed methodology. Validation of the methodology and expert feedback was undertaken with police officer training during several training events in Estonia, Germany and the UK. These events were both national and international in nature. These countries were chosen as they are different in size, administrative systems and law enforcement systems. Additional step in validation was undertaken with Cyber Security MSc students at TALTECH. To prove the methodology and developed model were applicable, the following steps were undertaken, using both qualitative and quantitative methods, according to principles of Grounded Theory Methodology:

1. Validation workshops and pilot group training. This was performed on six separate occasions, held between 2015-2019 in the three countries and organisation types. Pilot group trainings offered opportunity to make useful observations, these were followed by a select number of interviews with participants in the training,
2. A post event survey to determine the practical usability of the methodology and model for LEA operations. The survey used closed Likert scale questions with a few open-ended questions at the end,
3. Interviews with academics and practitioners on the usability and applicability of the methodology and model. Once completed the results of the interviews provided extra data and some interesting nuances,
4. Data analysis in order to determine the usability of journey mapping methodology and model. The aim of validation was to reach a common conclusion, and not to research single activities at micro levels. Different organisations and individuals each had specific expertise and points of view on the topic, and provided valuable insight in terms of validating the methodology and model of journey mapping.

Pilot group training

The pilot group training (a total sampling size of 250 persons) was based on the journey mapping methodology and model prepared during previous work. Principles of the training program were the same for all events, differing in details based on focus group's background and expertise. According to Grounded Theory Methodology, feedback from previous rounds of workshops and training were included in subsequent training events. In total, six events were held. The main goal was to confirm that that the journey mapping model is applicable to our stated purposes, is usable for practitioners and corresponds to real life. While the LEA and police oriented events looked in more detail at the potential use of the tool for investigation of cyber crimes, the student focus group aimed to identify if cyber security professionals could use the tool for their everyday work in preventing and responding to attacks. One training event focused on understanding the criminal mind in order for the defenders to be able to use defensive actions better.

Post event survey

Pilot group training and validation workshops (a total sampling size of 250 persons) were followed by post-event survey. The main goal was to get objective and quantifiable confirmation that the journey mapping model was applicable. The survey started with an introduction, stating also that it will be anonymised. The survey used Likert scale and had closed Likert-style questions in the beginning and a few open-ended questions in the end. In designing the survey, the aim was for it to not be too extensive – taking the survey should not take more than 10 minutes, as it would be taken at the end of classroom training within a limited timeframe.

Interviews

The qualitative aspects of the model were assessed by conducting interviews in different countries as above and different organisation types: LEA, police academies, investigators, prosecutors and academics. Semi-structured interviews were a method of choice because these allowed for establishing the main goals of the interview and fix core questions, but still gave freedom to ask additional follow-up questions [27].

The focus was on law enforcement operating at regional and national levels, industry based cyber security experts as well as experts from academia. The interview results were anonymised foremost for ethical reasons, not to reveal the identity of those working with cyber crime. Researchers and journalists writing about cyber crime have been threatened by cyber criminals, and in some cases cyber criminals have even used physical violence against police officers investigating cyber crimes [19]. The focus of these interviews was on requirements and needs at both individual and organization levels.

The interviews resulted in more thorough data collection and the identification of interesting nuances. Academics, law enforcement and cyber security specialists all had their unique views on real cyber crimes and/ or incidents, which provided useful input into the design of the model.

Data analysis

The aim data analysis and conclusions from validation was to determine the usability of journey mapping model at both individual and organization levels and include feedback in such a way which would allow its use in analysis according to the principles of Grounded Theory methodology. This stage also drew conclusions of the entire validation process and outcomes. The aim of the validation was to reach a common conclusion, and not to research single activities at micro levels.

As cyber criminals are not exactly willing subjects of research and so little is known about the process of cyber crime, or how a crime takes place from its initial preparatory stages through to exiting the crime cycle, this methodology was useful in considering inputs from cyber security professionals, LEA representatives and academia. It is clear that people with different background or area of expertise have different focus on a part of crime, which made the integrated approach relevant to all stakeholders, as post-event surveys showed. The integrated approach and resultant inclusion in the model using GT methodology principles resulted in more thorough data collection and the identification of interesting nuances. After conducting several rounds of data collection and feedback inclusion, a validated model for financially motivated cyber crime was developed. Since cyber crime is a quickly evolving and agile field of study, such exercise should be re-taken on a regular basis, to ensure the model remains relevant and updated as the business models, or tactics-techniques-procedures of cyber criminals change and adapt to the changing cyber security environment.

Conclusion

Very few published studies have researched cybercrime as a process, which includes both technical and non-technical aspects. This paper proposes a process model for financially motivated cybercrime, a practical tool which can be used by various stakeholders in the cybercrime investigation and prevention process. The model developed provides a step-by-step account of actions taken by the criminals throughout the crime. It is not intended to be a rigid or linear model but a flexible tool to understand the key steps within a cybercrime process, allowing us to identify major decision points the criminals pass through. By modelling and understanding cyber criminal processes, better oversight on investigations, countermeasures and disruption techniques can be formulated. This has the potential to overcome the challenges in understanding cybercrime across various players involved in the cybercrime investigation process. The aim is to allow those investigating cybercrimes or developing countermeasures to quickly apply new crimes to the model and focus on the specific known (or unknown) decision points in order to conduct their work more effectively.

References

Abelson, R. P., 1976. Script processing in attitude formation and decision making. In: Cognition and social behavior. Hillsdale(NJ): American Psychological Association.

Bernard, G. & Andritsos, P., 2017. A Process Mining Based Model for Customer Journey Mapping. s.l., s.n.

Borrion, H., 2013. Quality assurance in crime scripting. Crime Science.

Clarke, R. V., 1997. Situational crime prevention: successful case studies. s.l.:Harrow and Heston.

Hansman, S. & Hunt, R., 2005. A taxonomy of network and computer attacks. Computers and Security, Volume 24, pp. 31-43.

Hewlett Packard Enterprise, 2016. HPE Attack Life Cycle Use Case Methodology. Technical White Paper. s.l.:HPE.

Howard, J. D., 1997. An analysis of security incidents on the internet, 1989-1995, Pittsburgh, Pennsylvania: Carnegie-Mellon University.

Hutchins, E. M., Cloppert, M. J. & Amin, R. M., 2011. Intelligence-Driven Computer Network Defense Informed by ANalysis of Adversary Campaigns and Intrusion Kill Chains. s.l.:Lockheed Martin Corporation.

Kjaerland, M., 2005. A classification of computer security incidents based on reported attack data. Journal of Investigative Psychology and Offender Profiling, 2(2), pp. 105-120.

Levi, M. & Maguire, M., 2004. Reducing and preventing organised crime: An evidence-based critique. Crime Law and Social Change, 41(5).

Maimon, D. & Louderback, E. R., 2019. Cyber-Dependent Crimes: an Interdisciplinary Review. Annual Review of Criminology, pp. 191-216.

McGuire, M., 2018. Into the Web of Profit: Understanding the Growth of the Cybercrime Economy. s.l.:Bromium, Inc.

MITRE Corporation, n.d. ATT&CK Matrix for Enterprise. s.l.:MITRE Corporation.

Raudla, R., 2019. Lecture series “Research Methods in Social Sciences”. Tallinn: Tallinn University of Technology.

Rogers, M., 1999. A new hacker taxonomy. s.l.:University of Manitoba.

Rogers, M., 2006. A two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigation, 3(2), pp. 97-102.

Schank, R. C. & Abelson, R. P., 1977. Scripts, plans, goals and understanding, an inquiry into human knowledge structures. In: Hillsdale, NJ: Lawrence Erlbaum Associates.

Simmons, C. B., Shiva, S. G., Bedi, H. & Dasgupta, D., 2014. AVOIDIT: a cyber attack taxonomy. Albany, New York, s.n.

Van de Sandt, E., 2019. Deviant Security: The Technical Computer Security Practices of Cyber Criminals. Bristol: University of Bristol.

Warren, S., Oxburgh, G., Briggs, P. & Wall, D., 2017. How Might Crime-Scripts Be Used to Support the Understanding and Policing of Cloud Crime?. s.l., Springer.

Curriculum vitae

Personal data

Name:	Tiia Sõmer
Date of birth:	16 April 1974
Place of birth:	Tallinn
Citizenship:	Estonia

Contact data

E-mail:	tiia.somer@taltech.ee

Education

2015–2021	Tallinn University of Technology, PhD studies
2012–2014	Tallinn University of Technology, MSc, Cyber Security
2005–2010	Euro University, BSc, International Relations
1981–1992	Tallinn Secondary School no 13

Language competence

Estonian	native speaker
English	fluent
French	satisfactory
Swedish	satisfactory
Finnish	basic
Russian	basic

Professional employment

2014– …	Tallinn University of Technology, junior researcher
1994–2019	Estonian Defence Forces, officer

Elulookirjeldus

Isikuandmed

Nimi:	Tiia Sõmer
Sünniaeg:	16.04.1974
Sünnikoht:	Tallinn
Kodakondsus:	Eesti

Kontaktandmed

E-post:	tiia.somer@taltech.ee

Hariduskäik

2015–2021	Tallinna Tehnikaülikool, PhD
2012–2014	MSc Küberkaitse, Tallinna Tehnikaülikool
2005–2010	BSc Rahvusvahelised suhted, Euroülikool
1981–1992	Keskharidus, Tallinna 13. Keskkool

Keelteoskus

Inglise keel	kõrgtase
Prantsuse keel	kesktase
Rootsi keel	kesktase
Some keel	algtase
Vene keel	algtase

Teenistuskäik

2014– …	Tallinna Tehnikaülikool, nooremteadur
1994–2019	Eesti Kaitsevägi, ohvitser

ISSN 2585-6901 (PDF)
ISBN 978-9949-83-801-1 (PDF)