

NATIONAL DEFENSE UNIVERSITY

INTELLIGENCE ACQUISITION METHODS IN CYBER DOMAIN

Examining the Circumstantial Applicability of Cyber Intelligence
Acquisition Methods Using a Hierarchical Model

Master's Thesis

Lieutenant (Navy)

Karri Wihersaari

Master of Military Sciences Course 4
Navy

April 2015

Kurssi Sotatieteiden maisterikurssi 4	Linja Merisotalinja
Tekijä Yliluutnantti Karri Wihersaari	
Opinnäytetyön nimi <i>Tiedustelumenetelmät kybertoimintaympäristössä: kybertiedustelumenetelmien olosuhderiippuvaisen käyttökelpoisuuden tarkastelu hierarkkista mallia käyttäen</i>	
Oppiaine, johon työ liittyy Sotateknikka	Säilytyspaikka Maanpuolustuskorkeakoulun kurssikirjasto
Aika Huhtikuu 2015	Tekstisivuja 63 Liitesivuja 30
<p>TIIVISTELMÄ</p> <p>Kybertoimintaympäristön ilmiöt, erityisesti yksityisyyteen ja turvallisuuteen kohdistuvat uhat, ovat laajasti julkisuudessa käsitelty aihe sekä Suomessa että kansainvälisesti. Kybertiedustelusta on kuitenkin laadittu vain vähän tutkimusta.</p> <p>Opinnäytetyön päättökysymyksenä oli: missä määrin kybertiedustelumenetelmien käyttökelpoisuus on tilanneriippuvaista?</p> <p>Tutkimus toteutettiin käyttäen laajalti kirjallisuuslähteitä itse kybertiedustelun käsitteen määrittämiseen ja siihen vaikuttavien lainalaisuuksien tunnistamiseen. Näkökulmaa kehitettiin edelleen 15 asiantuntijahaastattelulla, jonka jälkeen kybertiedustelun menetelmistä muodostettiin hierarkkinen malli. Haastatelluista neljä vastasi mallin perusteelta luotuun AHP-kyselyyn.</p> <p>Tutkimuksessa päädyttiin siihen johtopäätökseen, että kybertiedustelu on kaikkia tavanomaisia tiedustelun lajeja poikkileikkaava tiedustelun ala, jolla on paljon erityispiirteitä suhteessa muihin tiedustelun lajeihin. Päättökysymykseen tehtiin johtopäätös että kybertiedustelumenetelmien käytettävyys riippuu olosuhteista osin.</p> <p>Avainsanat: Tiedustelu, kybertiedustelu, kybertoimintaympäristö, AHP</p>	

Course Master of Military Sciences Course 4	Branch Navy
Author Lieutenant (Navy) Karri Wihersaari	
Title <i>Intelligence Acquisition Methods in Cyber Domain: Examining the Circumstantial Applicability of Cyber Intelligence Acquisition Methods Using a Hierarchical Model</i>	
Area of study Military Technology	Repository National Defense University Course Library
Date April 2015	Text pages 63 Appendixes 30
<p>ABSTRACT</p> <p>Phenomena in cyber domain, especially threats to security and privacy, have proven an increasingly heated topic addressed by different writers and scholars at an increasing pace – both nationally and internationally. However little public research has been done on the subject of cyber intelligence. The main research question of the thesis was: To what extent is the applicability of cyber intelligence acquisition methods circumstantial? The study was conducted in sequential a manner, starting with defining the concept of intelligence in cyber domain and identifying its key attributes, followed by identifying the range of intelligence methods in cyber domain, criteria influencing their applicability, and types of operatives utilizing cyber intelligence. The methods and criteria were refined into a hierarchical model. The existing conceptions of cyber intelligence were mapped through an extensive literature study on a wide variety of sources. The established understanding was further developed through 15 semi-structured interviews with experts of different backgrounds, whose wide range of points of view proved to substantially enhance the perspective on the subject. Four of the interviewed experts participated in a relatively extensive survey based on the constructed hierarchical model on cyber intelligence that was formulated in to an AHP hierarchy and executed in the Expert Choice Comparison online application. It was concluded that Intelligence in cyber domain is an endorsing, cross-cutting intelligence discipline that adds value to all aspects of conventional intelligence and furthermore that it bears a substantial amount of characteristic traits – both advantageous and disadvantageous – and furthermore that the applicability of cyber intelligence methods is partly circumstantially limited.</p>	
<p>Keywords Intelligence, Cyber Intelligence, Cyber Domain, AHP</p>	

ESIPUHE

Viime vuosien aikana 'kyber' on noussut yhä voimakkaammin julkisuuteen. Erityisen kärjistettyä keskustelu on ollut kybermenetelmin tapahtuvan tiedonhankinnan vaikutuksista niin yksityishenkilöiden yksityisyyteen kuin organisaatioiden turvallisuuteenkin. Ajatus kybertoimintaympäristössä tapahtuvaa tiedustelua käsittelevästä pro gradu -työstä kehkeytyi keväällä 2013 käytyjen alustavien keskusteluiden perusteella. Sotatieteiden maisteriopintojeni alettua tutkimuksen näkökulmaksi valikoitui kybertoimintaympäristössä tapahtuvan tiedustelun tarkastelu laajasti ja yleisellä tasolla.

Aiheeseen perehdyttyäni havahduin siihen, että aiheen käsitteistö ei ole yksiselitteistä, vaan riippuvaista paljolti tarkastelunäkökulmasta. Tämän vuoksi työssä on pyritty luomaan eri lähteitä ja näkemyksiä yhdistelemällä kvalitatiivisesti tasapainoinen käsitteellinen perusta kybertoimintaympäristössä tapahtuvan tiedustelun luonteesta ja lainalaisuuksista, ja edelleen tarkastelemaan aihetta kvantitatiivisesti hierarkkisen mallin avulla.

Arvioitavaksi jättämisen jälkeen olen havainnut työn muotoseikoissa puutteita, jotka olen korjannut julkaistavaan versioon. Tutkimuksen asiasisältöön tahi tutkimustuloksiin en ole tehnyt muutoksia.

Haluan kiittää työn ohjaajia, professori Jouko Vankkaa sekä insinöörikapteeni Jouni Flyktmania kirjoitustyön aikana saamastani ohjauksesta, palautteesta ja neuvoista. Tutkimuksen aikana haastattelemilleni ja AHP -kyselyyn osallistuneille asiantuntijoille haluan esittää kiitoksen heidän tutkimukseni eteen näkemästään vaivasta. Rannikkosisarten säätiötä ja Maanpuolustuskorkeakoulun Sotatekniikan laitosta haluan kiittää tutkimuksen tekemiseen saamastani taloudellisesta tuesta. Lisäksi haluan kiittää vaimoani Katia tuesta ja ymmärtäväisyydestä etenkin työlään ja aikaa vievän kirjoitusprosessin aikana, vanhempiani tutkimusaiheesta ja tutkimuksen tekemisestä käymistämme keskusteluista sekä yliluutnantti Joona Hämäläistä kielellisestä ja sisällöllisestä vertaispalautteesta.

Helsingissä, 30.7.2015



Yliluutnantti Karri Wihersaari

FOREWORD

In past years, 'cyber' has become increasingly publicly prominent. The discourse regarding implications of information gathering by cyber means to privacy of individuals as well as security of organizations has been particularly aggravated. The idea of writing a thesis on intelligence in cyber domain emerged based on preliminary communications in autumn of year 2013. After starting my master's degree studies the focus of the study was further refined to examining intelligence activities in cyber domain broadly and on a general level.

After further familiarizing with the subject I came to discover that the conceptual base is not unequivocal, but much dependent on context and point of view. This is why I have pursued to establishing qualitatively a balanced conceptual base through synthesizing a range of different sources and views, which after the subject is further examined quantitatively through utilizing a hierarchical model.

After submitting the thesis for evaluation, I have noticed a number of technical mistakes in the work, which I have corrected in the published version of the thesis. The subject matter or findings of the study have not been altered.

I want to express my gratitude to the supervisors of my thesis, Professor Jouko Vankka and Captain (Engineering) Jouni Flyktman for their guidance, feedback and advice. Furthermore, I want to thank the experts interviewed for the thesis and those who took part in the AHP survey for the effort and time they put into supporting my thesis. I am also thankful to Rannikkosisarten säätiö foundation and the Department of Military Technology for their financial support to my research. Moreover, I want to thank my wife Kati for her support and understanding especially during the laborious and challenging writing phase of the research, my parents for the helpful discussions regarding conduct of the research as well as the subject matter, and Lieutenant (Navy) Joonas Hämäläinen for his peer feedback regarding both content and linguistic matters.

In Helsinki, 30.7.2015



Lieutenant (Navy) Karri Wihersaari

CONTENTS

1	INTRODUCTION	1
1.1	Foreword	1
1.2	A Brief History of Intelligence in Cyber Domain	3
1.3	Existing Research on Cyber Intelligence	6
1.4	Framework and Research Problem	7
1.5	Perspective, Scope and Exclusions	8
1.6	Key definitions	9
2	METHODOLOGY	11
2.1	Methodological Framework and Conduct of the Research	11
2.2	Research Methods	12
2.2.1	Literature Review	12
2.2.2	Interview	13
2.2.3	AHP	13
2.3	Source Criticism	15
2.3.1	Literature	15
2.3.2	Interviewees	16
2.3.3	AHP	16
3	INTELLIGENCE IN DECISION-MAKING	17
3.1	Intelligence as a Discipline	17
3.2	Intelligence as an Element in Decision-making	19
3.2.1	The OODA Cycle	19
3.2.2	The Intelligence Cycle	20
3.2.3	The Intelligence Cycle as a Situation Awareness Process	21
4	INTELLIGENCE IN CYBER DOMAIN	23
4.1	Defining Cyber Intelligence	23
4.2	Characteristics of Cyber Intelligence	28
4.3	Cyber Intelligence as an Extension of Conventional Intelligence	30
4.4	Operatives of Cyber Intelligence	31

5	A HIERARCHICAL MODEL OF INTELLIGENCE IN CYBER DOMAIN	33
5.1	Identifying Cyber Intelligence Methods	34
5.2	Identifying Evaluating Criteria	40
5.3	Identifying the Operative Types	42
5.4	A Hierarchical Model of Cyber Intelligence	43
5.5	Composing the Survey Based on the AHP-model	45
6	CIRCUMSTANTIAL APPLICABILITY OF CYBER INTELLIGENCE ACQUISITION METHODS	46
6.1	Overview of the Results	46
6.2	Assessment on the Survey Results	47
6.3	Analysis of Results Acquired from the Survey	50
6.3.1	Weights of Criteria	50
6.3.2	Overall Priorities	52
6.3.3	Performance	53
6.3.4	Capability	54
6.3.5	Risk	55
7	CONCLUSIONS, DISCUSSION AND SUGGESTIONS	56
7.1	Overview of the Research Process	56
7.2	Summary of Results	57
7.3	Validity and Reliability	60
7.4	Discussion	61
7.5	Future Work	62
	BIBLIOGRAPHY	
	ANNEXES	

TABLES

Table 1 Elements of the Hierarchical Model of Intelligence in Cyber Domain	43
Table 2 Standard Deviations of Participants' Assessments	48
Table 3 Standard Deviations of Participants' Normalized Assessments to criteria weights	48
Table 4 Sensitivity Analysis of Criteria Weights	50
Table 5 Local Weights of Evaluating Criteria	51

ANNEX 3

Table A3.1 Elements of the AHP Model on Intelligence Acquisition Methods in Cyber Domain	3
--	---

ANNEX 5

Table A5.1 Unnormalized Criteria Weights Submitted to Scenarios 1–3	1
Table A5.2 Method Assessments Submitted to Scenarios 1–3	2

ANNEX 6

Table A6.1 Criteria Weights and Method Priorities for Scenario 1	2
Table A6.2 Criteria Weights and Method Priorities for Scenario 2	3
Table A6.3 Criteria Weights and Method Priorities for Scenario 3	4

FIGURES

Figure 1 Structure of the Research and Thesis	11
Figure 2 Principle of Application of AHP in the Research	14
Figure 3 Example of AHP Hierarchy	14
Figure 4 CIA Triad	18
Figure 5 The OODA Cycle	19
Figure 6 The Intelligence Cycle	21
Figure 7 The Intelligence Process as the SA Process of the OODA Cycle	22
Figure 8 Relation Between CNO and CNE	23
Figure 9 Finnish Classification of Military Intelligence Disciplines	25
Figure 10 SWOT-analysis of Cyber Intelligence	30
Figure 11 Cyber Intelligence as an Endorsing Parallel of Physical Domain Intelligence	31
Figure 12 The Hacking Process	34
Figure 13 AHP-hierarchy in Expert Choice Comparison Suite	44
Figure 14 The Principle of Assessing Intelligence Methods Using an AHP Hierarchy	44
Figure 15 Arithmetically Averaged Priorities of Cyber Intelligence Acquisition Methods	47
Figure 16 Priorities of the Intelligence Methods With Respect to All Assessment Criteria	52
Figure 17 Priorities of the Intelligence Methods With Respect to Performance	53
Figure 18 Priorities of the Intelligence Methods With Respect to Capability	54
Figure 19 Priorities of the Intelligence Methods With Respect to Risk	55
Figure 20 Hierarchical Model for Evaluating Circumstantial Applicability of Cyber Intelligence Methods	58
ANNEX 3	
Figure A3.1 Example of an AHP Hierarchy	2

ANNEX 4

Figure A4.1 Description of the Scenario and Overview of the Survey	1
Figure A4.2 Weighing the Main Criteria	3
Figure A4.3 Weighing the Sub-criteria of Performance	4
Figure A4.4 Weighing the Sub-criteria of Capability	4
Figure A4.5 Weighing the Sub-criteria of Expertise	5
Figure A4.6 Prioritizing Sub-criteria of Risk	5
Figure A4.7 Evaluating Alternatives Against Speed	7
Figure A4.8 Comment Page	8
Figure A4.9 End Page of the Survey	8

ACRONYMS

a_i	Ratio score for the alternative on the i th objective
AHP	Analytic Hierarchy Process
AIJ	Aggregate Individual Judgment
C2	Command and Control
C4	Command, Control, Communications and Computers
C5	Command, Control, Communications, Computers and Cyber
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT-FI	Computer Emergency Response Team Finland
CIA	Central Intelligence Agency
CIA	Confidentiality, Integrity, Availability
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COMINT	Communications Intelligence
Comnet	Communications and Networking
CYBERINT	Cyber Intelligence
DCPD	Direction-Collection-Processing-Dissemination
Dr. Sc.	Doctor of Science
Dr. Sc. (Mil.)	Doctor of Military Sciences
ELINT	Electronic Intelligence
FBI	Federal Bureau of Investigation
FICORA	Finnish Communications Regulatory Authority
FIRE	Finnish Intelligence Research Establishment
g_i	Global priority score for the the i th objective
GCHQ	Government Communications Headquarters
GEOINT	Geospatial Intelligence
GIAC	Global Information Assurance Certification
HUMINT	Human Intelligence
IMINT	Imagery intelligence
INSA	Intelligence and National Security Alliance
MD	Managing director

M. Sc.	Master of Science
n	Number of objective
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
NCSC-FI	National Cyber Security Centre Finland
OODA	Observe-Orient-Decide-Act
OSINT	Open-source Intelligence
Ph. D.	Doctor of Philosophy
SA	Situational Awareness
SIGINT	Signals Intelligence
T	Total priority
σ_{max}	Maximum value of standard deviations
σ_{mean}	Mean value of standard deviations
σ_{med}	Median value of standard deviations
σ_{min}	Minimum value of standard deviations

INTELLIGENCE ACQUISITION METHODS IN CYBER DOMAIN

Examining the Circumstantial Applicability of Cyber Intelligence Acquisition Methods Using a Hierarchical Model

1 INTRODUCTION

1.1 Foreword

The rapid technological advancement of the latest century, let alone the latest decades has fundamentally transformed everyday lives in ways that in retrospect seemed incomprehensible. The gap between sci-fi and reality has narrowed, as new technology has increasingly proven to bedazzle people in ways earlier only wildest fiction could. Consequently, the relationship not only to communication, but information itself has transformed: new technology – high-speed wireless Internet, social networking, internet telephony, e-mail, cloud services etc. – enables one to carry and access all of his/hers personal data virtually everywhere, having uploaded it to the cloud and utilizing a smartphone with required data connections, and connect with practically anyone in the world for no price at all. Many argue that this development has made life easier and both work and personal life more flexible. On the other hand, however, it has made man reliant on ancillaries and his private data vulnerable for exploitation – willfully, albeit not comprehending the implications.

Phenomena associated with the digital realm of cyber domain have proven both inspiring and controversial. ‘Cyber’ phenomena – especially nasty-sounding military and criminal implications such as cyber espionage, cyber warfare, cyber theft, cyber terrorism etc. – has just begun to be comprehended by the masses. Nevertheless, “cyber is inevitably becoming the fifth war domain after land, sea, air and space” [144]. Furthermore, implications of threats in cyber domain can easily be appreciated in governmental, military or industrial context, but the understanding of the real-life implications of actions in cyberspace is not considered to be

of much personal importance. One commonly weighs ease and comfort of modern technology applications over trouble and awkwardness non-customary security measures bring, self-deceivingly not thinking one's personal data would be of any interest to anyone.

From an authoritative (military, police, government etc.) perspective, the cyber domain appears as a vast medium of both new opportunities and trouble. On one hand, the assisting, work-facilitating and expediting qualities observed in personal applications translate to professional ones as well – even more meaningfully than in recreational context – but on the other hand cyber vulnerabilities are fundamentally more difficult to identify let alone to protect or eliminate than real-life ones. Furthermore, exploitation of them is often hard to detect and skillful perpetrators virtually impossible to identify, but the effects of actions in cyberspace “will affect us every day more physically than virtually” [144].

When perceiving from a cyber-security point of view, “cyber espionage, theft of intellectual property, and a wide variety of criminal activities in cyberspace pose real and serious threats to all states, as well as to corporations and private individuals” [128, p. 4]. On the other hand, from an intelligence point of view the emergence of cyber domain as a growing global medium for a wide variety and vast amount of activities has brought forth a completely new and unforeseen set of opportunities – not only does it render physical proximity a negligible factor, it provides fundamentally novel ways of intelligence acquisition.

In military terms, “intelligence assists the commander in visualizing his battlespace, organizing his forces, and controlling operations to achieve the desired tactical objectives or end-state. [...] The most important purpose of intelligence is to influence decisionmaking. Commanders must receive the intelligence, understand it (because it is tailored to the commander's requirements), believe it, and act on it. Through this doctrinal concept, intelligence drives operations.” [17] The dual purpose of intelligence – military and otherwise – is to stay informed in order to be able to carry out analysis when needed and serve as a continuous source of balanced, verified information enlightened decision-making needs. Until recently, almost all branches of intelligence have been founded on primary observations made of real-world objects based on real-world indicators (visual, sound, electromagnetic etc.) and secondary observations of recordings (written form, photos etc.) of the former. Adding the cyber intelligence into the picture, only little imagination is required to fathom the dramatic increase in resources it brings to all-source intelligence.

1.2 A Brief History of Intelligence in Cyber Domain

Whereas other forms of intelligence are conducted in real world, characteristic to cyber intelligence – like other ‘cyber’-phenomena – is that it by definition requires the man-made environment of interconnected computer systems [97]. Intelligence has been a crucial to mankind ever since the earliest humans began to process information and have drawn conclusions influence everyday decisions. Furthermore, computers have been utilized for intelligence purposes ever since the construction of Colossus Mark 1, operational by January 1944 [71], that was “the world's first semi-programmable electronic computer” [53]. However, the first concept and infrastructure that would suffice for a cyber domain was the ARPANET, that initially in late 1969 comprised four host computers that were connected together [101], and through gradual developments grew into the Internet [101]. Until year 1990, the Internet was a network of a limited community – science and defense. In late 1989, Tim Berners-Lee documented what was to become the World Wide Web (WWW) and in 1993, CERN made it available on a royalty-free basis. [27]

With much of the cyber intelligence methodology building upon hacking – especially when perceiving intelligence as a general phenomenon – the origins of intelligence acquisition in cyber domain can be traced to MIT’s computer-enthusiasts of 1960’s. The earliest hacks were “simply shortcuts developed to bypass or improve the operation of systems” [21], meaning in essence finding and exploiting vulnerabilities in the systems. The introduction of ‘personal’ computers in the 1980’s was a turning point in hacker history, because computers became available to anyone for their own purposes, as opposed to being limited to hardcore hobbyists and business users. Modems were also more widely available and significantly extended the hacker’s reach [67], enabling the use of for example BBS systems (invented in 1978) [23; 124], IRC (invented in 1988) [32] for communicating. The latter is still perhaps the most popular means of communication in the hacker community [83].

The first publicly known case of cyber domain facilitated intelligence – or espionage – was discovered in the late 1980’s: Clifford Stoll, computer administrator at Berkeley, received an “apparently mundane job of tracking down an accounting discrepancy on the LBL computers” [98], which eventually lead to him uncovering a KGB spy ring based in West Germany. The craker, Marcus Hess, had compromised the security of the university’s computer network and had used it as an access point to a vast number of government, military and defense industry networks, and exploited the situation by passing sensitive information on to the KGB. Hess

was tried and convicted in 1989. [56, p. 97; 98] Now, “it’s estimated that 30,000 websites are hacked every single day, ranging from small company blogs to social media behemoths” [21].

Another central component in the cyber intelligence toolbox is malware. Much like hacking, for a long time malware was a phenomenon causing nuisance rather than compromising confidentiality, but the core nature of software being deliberately created for malicious purposes has been present from the emergence of first malware. First malware, the ‘Creeper Virus’, was created in 1971. The first Trojan, ANIMAL, was released in 1978, and the first virus, the ‘Elk Cloner’, in 1981. These did not, however, amount to causing damage to computer systems. [24] The first destructive virus to have a global impact was the Jerusalem virus released in 1987 [16], and since then, computer malware has explosively evolved in complexity, finesse, severity, number, and impact – financial as well as security. Until 1999, however, computer malware did not pose a threat to confidentiality of data. First occurrence of spyware took place in 1999, when Elf Bowling and other seemingly harmless leisure were discovered to be reporting user data back to their developers [25; 26], consequently also raising an issue of inadequateness of existing legislation to address the problem [70]. Interestingly, some of the code of Regin, a multi-staged, modular threat remote access Trojan (RAT) [5] discovered in 2014 and suspected to have been used for spying purposes by government entities [143], has been found to date back to 1999 [110]. The first malware incident F-Secure assessed to be involved in state-sponsored cyber espionage took place in 2003 [81].

Originally denoting exclusively nation-state level cyber espionage [3] and still assessed to being mainly within reach of only nations, the concept of advanced persistent threat (APT) was first coined in the US Air Force 2006, defining something fundamentally different from ‘ordinary’ cyber espionage that typically relies on mass-exploitation of vulnerabilities: targeted, long-lasting, low-profile cyber espionage that incorporates multiple methods [49]. Typically to espionage-related phenomena that is veiled with secrecy, APT actors are assessed to have been around much before their public discovery: for example, Equation group, a sophisticated APT actor, has been active since 2001, perhaps even since 1996 [13].

Later on, cyber espionage incidents have been discovered at a growing rate. In 2011, a trojan named Duqu that is believed to be designed to gather intelligence from industrial control-systems was discovered [12], and soon discovered to have many similarities with the infamous Stuxnet [57]. In 2013, Red October, a large scale cyber-espionage network that targeted mainly Eastern-European and Central-Asian diplomatic service agencies, was discovered in 2013 and suspected to have been active since 2007 [42]. The same year, Edward Snowden, a former National Security Agency (NSA) contractor acquired up to 200,000 classified documents, fled to Hong Kong and handed them over to journalists of *The Guardian* [93; 119], which after a vast amount of documents have been published. The documents have unveiled numerous, massive surveillance programs on online communication, run by many government agencies, most prominently the NSA and QCHQ¹. Reported surveillance methods used range from back door access to Google, Apple, Facebook and other databases, tapping fiber optic communication cables, circumventing encryption technologies, intercepting phone calls, diverting and modifying computers en route to customer... [76; 88; 93; 104]

To date, cyber espionage – or intelligence – has emerged as an increasingly potent and especially reaching intelligence gathering discipline. Whereas most ‘traditional’ intelligence methods are strongly sanctioned and thus within reach of only those with jurisdiction, many cyber intelligence acquisition methods have proven to be within reach of virtually anyone with the mere will to exploit them, given of course the capacity to learn and utilize the tools available. Albeit laws do condemn infringements of confidentiality, in cyber domain even noticing encroaching on confidential information, let alone identifying the perpetrator, can be beyond reach of any surveillance, and in case of discovery laws may be incapable of combating the threat [114]. Thus far – over a period of mere decades – a wide, almost incomprehensible range of methods of intelligence acquisition in cyber domain has been discovered – and yet there is something new and unforeseen to come [92].

¹ Government Communications Headquarters

1.3 Existing Research on Cyber Intelligence

Phenomena in cyber domain, especially threats to security and privacy, have proven an increasingly heated topic addressed by different writers and scholars at an increasing pace – both nationally and internationally. Approach angles and points of view of existing research and literature on cyber phenomena fall mainly into one of two categories: cyber security and cyber offensive. From these two perspectives, the role and manifestation of intelligence differ fundamentally. In the former, cyber intelligence is perceived from a threat awareness and vulnerability management perspective, whereas in the latter, cyber intelligence – or intelligence in general – is treated as an enabling and target designating element.

Cyber intelligence per se, however, is directly less covered in existing literature and research. Most writers discuss intelligence – or reconnaissance or espionage – as an interphase of a greater process or from a narrower point of view. Albeit cyber phenomena has been extensively – perhaps even overwhelmingly – discussed in literature, intelligence in cyber domain has not been addressed comprehensively as a phenomenon of its own. Consequently, the definition of intelligence in cyber domain as well as its attributes – scope, methodology, strengths and shortcomings – call for in-depth scrutiny.

1.4 Framework and Research Problem

Defining cyber warfare is far from a straightforward task. It can even be argued that “definitions for Cyber and Warfare are both under debate” [55, p. 3]. Furthermore, intelligence in cyberspace does not quite fall neatly into any one notch, either. Both for this reason and because little research has been targeted specifically at cyber intelligence, the selected approach of this study is to address the very concept of intelligence in cyber domain, and further analyze how cyber intelligence acquisition methods apply in different circumstances.

The primary research question of the study is:

- To what extent is the applicability of cyber intelligence acquisition methods circumstantial?

The primary research question may be broken down to sub-questions:

- What constitutes as intelligence in cyber domain?
- What is the scope of cyber intelligence?
- What is the range of intelligence methods in cyber domain?
- What factors dictate the applicability of intelligence methods in cyber domain?
- What is the range of cyber intelligence operatives?
- How can the applicability of cyber intelligence acquisition methods be assessed?

The research questions will be addressed by establishing a theoretical base from a comprehensive set of literature, amending the point of view with experts’ understanding of the field. Furthermore, a hierarchical model of intelligence in cyber domain is created and applied, aimed at untangling the circumstantial dependence of applicability of intelligence methods in cyber domain.

1.5 Perspective, Scope and Exclusions

Although the intention of this study is not to focus exclusively on military intelligence, it is convenient to derive the definition of intelligence in cyberspace from the framework of cyber warfare, among other designated frameworks in the cyber domain. Many aspects of intelligence – and hence of cyber intelligence – are primarily defined through military functions, but when expanding the point of view to other aspects of life, the corresponding non-military implications are derivable.

The perspective of the study is to examine the concept of intelligence in cyber domain in a general and universal manner, aiming at developing a functional model and sound framework for analyzing intelligence in cyber context as a whole. The concepts of both intelligence and activities in cyberspace are addressed in such a manner that artificial categorizations or technicalities do not rule out any ground. In-depth and detail analysis of various methods for extracting exploitable information by cyber means will be excluded from the study, because such detailed accounts would both draw attention from developing a more general understanding of phenomena constituting intelligence methods in cyber domain and – more importantly – not provide but a narrow and pale representation of the vast variety of intelligence collection possibilities facilitated by current cyber potential.

In this study, the concept of intelligence is treated as a discipline of collecting information required for decision making, planning, situational awareness etc. – intelligence is treated as a proactive and exploratory discipline. Hence, in the framework of this study, cyber security as well as preventive and reactive intelligence activities are excluded, for example cyber security intelligence and cyber forensics.

1.6 Key Definitions

Cyber

The word ‘cyber’ is usually used as “the prefix for a term or the modifier of a compound word.” In vernacular, however, the word occasionally appears by itself. ‘Cyber’ usually implies being related “to electronic information (data) processing, information technology, electronic communications (data transfer) or information and computer systems.” [15]

Cyber domain

By technical definition, ‘cyber domain’ refers to “an electronic information (data) processing domain comprising of one or several information technology infrastructures” [15]. In this thesis, the term is understood to encompass the logical IT environment and the IT infrastructure including interfaces to the physical world.

Hacker and hacking

In everyday language, the word hacker is often used to refer to individuals who gain illegal access to computer systems for malicious purposes, namely to steal, tamper with or corrupt information [20; 19], although it is argued that the proper term for such individuals is cracker [20]. In this study, the word ‘hacking’ will be used when referring to gaining unauthorized access to computer systems and networks, and the word ‘hacker’ when referring to persons conducting such activity.

Intelligence

In this study, the word ‘intelligence’ is understood as collection, processing and exploitation of information with respect to operative’s objectives and requirements. The word is used as a hypernym that comprises activities of different levels and scales (intelligence, surveillance, reconnaissance etc.) and is not demarcated by legal or jurisdictional considerations (encompassing legitimate intelligence activities as well as espionage, snooping, etc.), nor by organizational or geographical factors.

Malware

Malware, or malicious software, refers to software dedicated and designated to perform unwanted actions on computer systems [36].

Metadata

“Metadata is data about data” [55, p. 109], meaning content associated to the payload information. For example, a digital photograph contains at least file name and size, permissions, timestamps (date created, date modified) and possibly much more, such as date taken, place taken, camera and lens used, exposure configuration, copyright etc.

Vulnerability

A vulnerability is a weakness of an asset or control that can be exploited by a threat [44]. From an information technology perspective, vulnerabilities may be identified in following areas: organization, processes and procedures, management routines, personnel, physical environment, information system configuration, hardware, software or communications equipment, or dependence on external parties [45].

2 METHODOLOGY

2.1 Methodological Framework and Conduct of the Research

Given the fact that the conceptual framework of phenomena and activities in cyber domain is still forming and substantially dependent on chosen point of view, the initial research setting is to synthesize a neutral conceptual framework for intelligence in cyber domain that perceives the phenomenon namely from the point of view of conducting intelligence activities. Having established the conceptual framework, the topic is further developed to defining the elements composing the entity of intelligence in cyber domain – namely intelligence methods – and its characteristic attributes. Furthermore, the defined elements and attributes are developed into a hierarchical model for quantitative analysis of intelligence in cyber domain, and the obtained quantitative data is analyzed with the qualitative attributes of the phenomenon, drawing conclusions on the circumstantial applicability of intelligence methods in cyber domain. Structure of the research and thesis is illustrated in Figure 1 below:

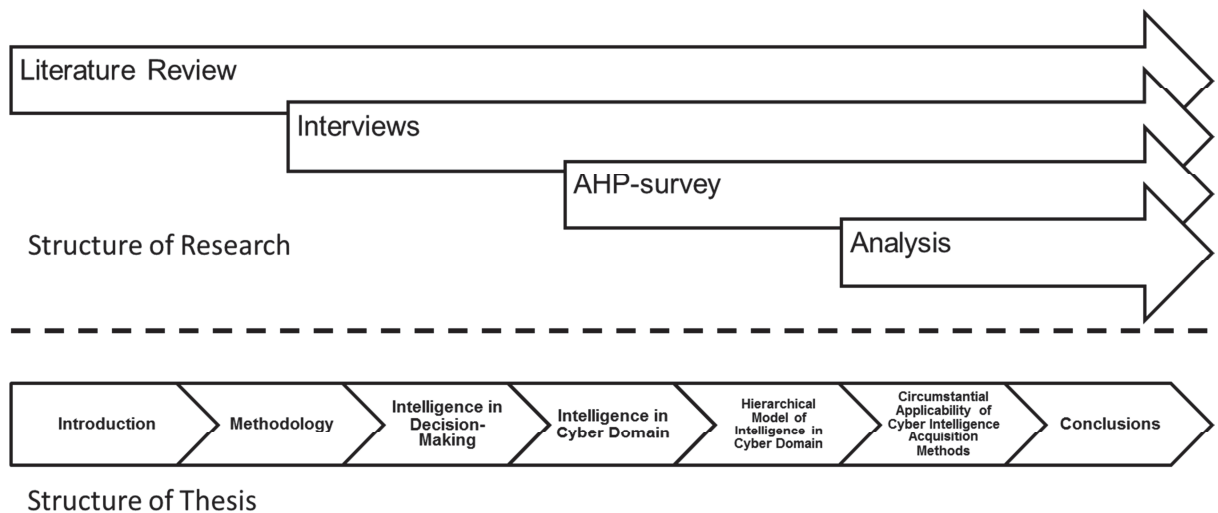


Figure 1 Structure of the Research and Thesis

To accomplish the described research construction, both qualitative and quantitative research methods are utilized. The motivation for combining different methods is that they have different strengths [109, p. 1], and through incorporating multiple approach angles to the controversial topic at hand, a both more balanced and more insightful conception on the subject. The pursued purpose for integrating qualitative and quantitative methods is ultimately convergent, meaning that both kinds of methods are used to examine the research question [109, p. 11], providing a basis for contrasting the outcomes of qualitative and quantitative

methods. However, for the purposes of establishing the preconditions for quantitative research of deductive, objective and general nature, qualitative research of the inductive and contextual qualities is incorporated in a sequential manner [109, pp. 9–10].

2.2 Research Methods

The conceptual framework of the research is initially established based on comprehensive literature review of existing research and literature. The conceptual perspective is refined with interviews with experts. Furthermore, literature and interviews are used to define the acquisition methods and characterizing attributes of intelligence in cyber domain. After this, a hierarchical model of intelligence in cyber domain is formulated into an AHP hierarchy, which is evaluated by persons interviewed earlier. The quantitative data of the AHP survey is analyzed and contrasted with the qualitative data of the earlier stages of the research.

2.2.1 Literature Review

For the purposes of founding the empirical elements of the research on sufficient basis as well as contrasting the empirical data with prior conceptions, a literature review is conducted. Furthermore, it serves the purpose of clarifying the research question and approach, resulting in a more appropriate and definite empirical approach. [137, p. 42]

“Cultivating a reference list that presents a variety of positions on the topic is essential so as not to present a distorted view of the state of the field” [118, p. 51]. For the purposes of avoiding the bias of a needlessly narrow perspective, publications of related disciplines are incorporated, because “several disciplines are working on related problems, so analyzing and critiquing those intersections can be valuable” [118, p. 51]. A number of fields conduct research that is associated with aspects of cyber intelligence, of these security and military studies being perhaps most prominent, however also many others touch upon the subject.

2.2.2 Interview

The research interview is essentially about asking purposeful questions and carefully listening to the answers to be able to explore these further [127, p. 372], and it was utilized in the study for the purpose of refining conceptions derived from literary sources. The selection of interviewees of the study encompasses a wide selection of persons whose fields perceive cyber phenomena from different perspectives, hence allowing for acquiring a variety of opinions on the field of cyber intelligence. Brief descriptions and assessments of the interviewees can be found in Annex 1.

Semi-structured – or qualitative – research interview was used because it allows for structure in terms of themes or questions to be covered during the session, but their use may vary from interview to another [127, pp. 374–375], thus allowing for discussion to proceed more freely. Hence, the interviewees were allowed to present their opinions on the questions and themes presented to them to the extent they desired, and the interviewer to present additional and more detailed questions that arose during the sessions. The thematic questions for the interviews can be found in Annex 2. The interviews were conducted in person, and the sessions were recorded.

2.2.3 AHP

AHP is a decision support tool which can be utilized to solve complex decision problems, using a multi-level hierarchical structure of objectives, criteria, subcriteria, and alternatives [135]. In the framework of the study, the AHP was applied to analyze the relative applicability of different cyber intelligence methods in given circumstances. The objective and framework were set by scenarios, with respect to which assessments were made. Three distinct scenarios were established in order to contrast the intelligence methods in different settings. The principle of application of AHP in the study is illustrated in Figure 2 below:

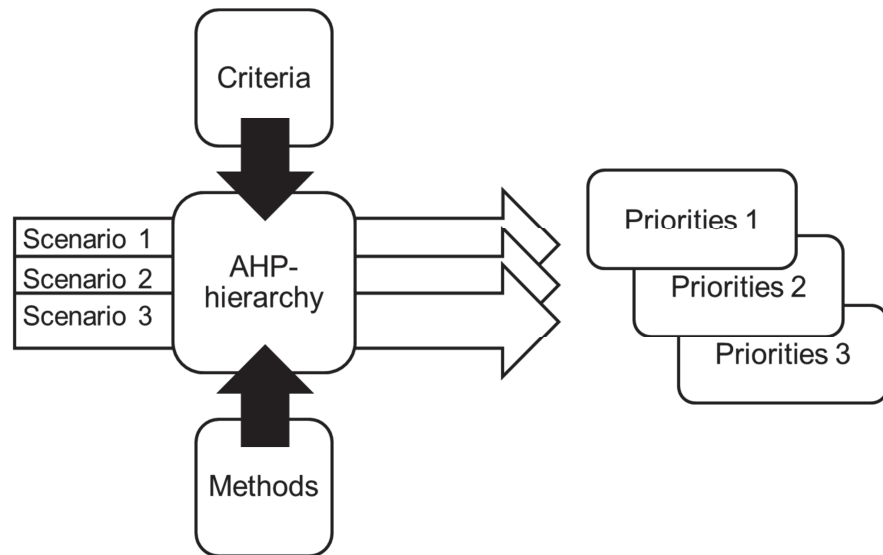


Figure 2 Principle of Application of AHP in the Research

A multi-level, hierarchical model was established based on the identified cyber intelligence methods and criteria dictating their applicability. The intelligence methods were treated as the alternatives of the hierarchy, and the criteria were grouped as sub-criteria of three main criteria. The identified intelligence methods and assessment criteria as well as the detailed composition of the hierarchy used are addressed in depth in Chapter 5. An example of a simple AHP hierarchy is depicted in Figure 3 below:

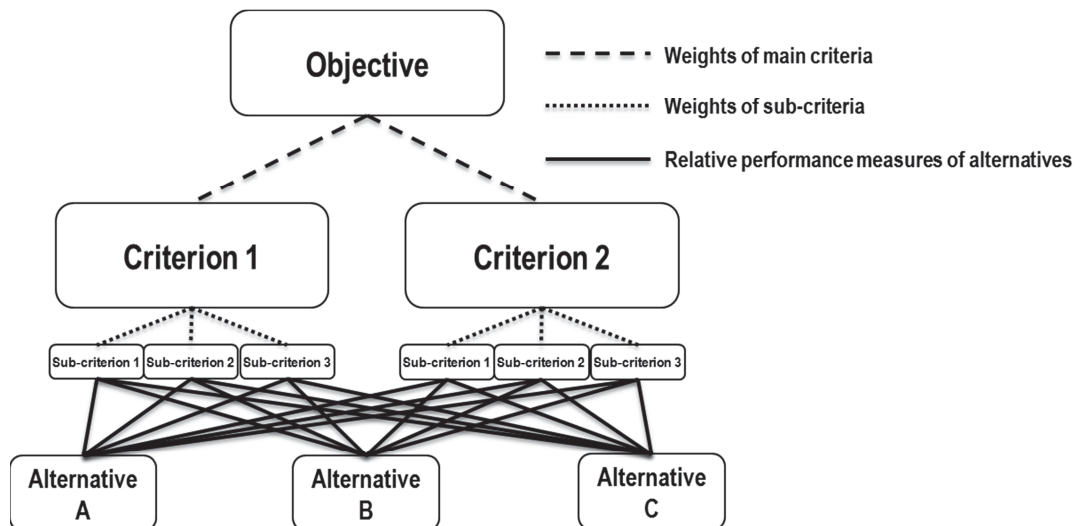


Figure 3 Example of AHP Hierarchy

The principle of the AHP calculation is in essence “to construct a matrix expressing the relative values of a set of attributes,” i.e. which attribute is most important and which least important in relation to the others. These judgments are assigned numeric values on a selected scale. [69] In the typical use of AHP, the “pertinent data are derived by using a set of pairwise comparisons. These comparisons are used to obtain the weights of importance of the decision criteria, and the relative performance measures of the alternatives in terms of each individual decision criterion” [135], illustrated in Figure 3. In this study, however, pairwise comparison was not used in order to avoid an overwhelmingly lengthy survey. Criteria were weighed in terms of direct priority assignment, and alternatives were assessed on a rating scale [8]. Details about how the survey for collecting the AHP data was constructed is further discussed in Chapter 5, and analysis of the data is conducted in Chapter 6.

2.3 Source Criticism

2.3.1 Literature

For the study, a wide range of primary, secondary and tertiary literary sources are utilized. The literary base of the thesis is wide, however the sources are exclusively non-classified, which can be considered a limitation because intelligence-related information is most often classified. Non-public research and publications undoubtedly exist, but for the purposes of keeping the thesis’ security classification intact, such sources have not been pursued.

In the context of this study, the wide variety of literary sources is on one hand a limitation because the validity and reliability can be difficult to judge in certain cases, but on another hand contrasting information from different sources allows to find congruencies as well as dissonance between them, allowing then to analyze possible causes for discrepancies. Contrasting various literary sources against experts’ views is another potent way of evaluating validity and reliability of sources.

2.3.2 Interviewees

The interviewees represent a wide selection of experts in their respective fields, providing a multitude of perspectives to the concept of cyber intelligence. The approach to the research is general and conceptual, and the topic inclined to strong opinions, which suggests that the expressed expert views might be divergent and contradicting in some respects.

2.3.3 AHP

AHP is deemed to be applicable to “any complex situation that requires structuring, measurement, and and/or synthesis is a good candidate for AHP. However, AHP is rarely used in isolation. Rather, it is used along with, or in support of other methodologies” [74]. In this study, AHP is used along with literary review and interviews.

3 INTELLIGENCE IN DECISION-MAKING

By and large, most words bear multiple meanings [54], and conceptions associated with ‘intelligence’ in the context of this study is no exception. Conceptual ambiguity and contradiction exists for example regarding the relation between words ‘intelligence’ and ‘espionage,’ and the latter in general bears a strong implication of government-related collection of information [115; 136]. Even though the terminological ambiguity is dismissed in this study by picking the word ‘intelligence’ to be used as a hypernym, an examination of the conceptual relation between intelligence and decision-making is called for before approaching the concept of cyber intelligence.

3.1 Intelligence as a Discipline

From a state point of view, “the core responsibility of intelligence as a discipline is to provide state leadership with insight into what the emerging threats are before they manifest into an attack on a state” [65]. In military context it even can be perceived that it “drives the conduct of operations” [18, p. 1-4]. For the purposes of a more general inquiry one needs, however, to expand the definition of the concept of intelligence – the utilization of intelligence is not by any means confined to military or state applications. Intelligence “is itself a dynamic concept that does not have just one definition or application. [...] [T]he ultimate purpose of the intelligence product is simple: provide an edge to the decision-maker. Intelligence is many things, but foundationally, its core mission is to provide knowledge of the world in which we live” [84, p. 2].

From an information security perspective, the nature of intelligence can be argued to be associated to violating one element of the CIA² triad: confidentiality [115]. In many respects, a breach in confidentiality – acquisition of information that can be considered sensitive or private [66] – might not extend to legal or even moral discrepancies. For example, if the target is misguidedly forthcoming with respect to sensitive information, the intelligence is in essence open-source but nevertheless provides intimate insight into the subject in question. An illustration of the CIA triad is displayed in Figure 4 below.

² Confidentiality-Integrity-Availability

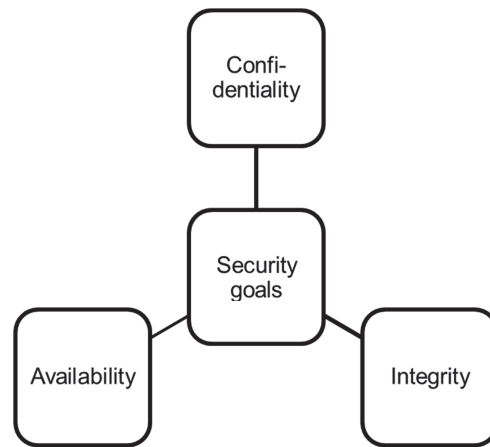


Figure 4 CIA Triad [62]

When it comes to formulating a more specific definition, “each expert tends to view the term through the spectacles of his specialty” [58]. Much effort has been made in order to formulate satisfactory definitions of intelligence for respective circumstances, not least for legislative and jurisdictive purposes [113] as well as for purposes of describing its purpose, role and impact in organizations [2; 17]. Many definitions, however, tend to be either too general in nature for practical uses or excessively restrictive and narrow in order to cover the concept in general. In order to facilitate a starting point for assessing cyber intelligence, one needs to deduce a satisfactorily general and simultaneously specific enough definition for intelligence.

Albeit objectives, methods and motives vary, the key elements of intelligence stand universal: planning and direction of intelligence functions, collection, processing, analyzing and production of information into a final product, and dissemination of the end product appropriately [86]. As discussed further on, these elements – or intelligence in general – should be understood as a cognitive process applicable to any activity instead of being strictly limited to for example military activity.

3.2 Intelligence as an Element in Decision-making

As stated afore, the core nature of intelligence is to serve the purpose of providing those who make decisions and draw plans with appropriate insight. In order to understand the role of intelligence in human activity, one needs to turn attention to how the process of carrying out intelligence coalesces into the overall process of making decisions. Albeit much of the vocabulary used when referring to intelligence of most kinds is expressed in words commonly associated to military activities, the discourse shall not be mistaken as being confined to a military framework. On a conceptual level, most of the principles translate, scale and are applicable to other frameworks.

3.2.1 The OODA Cycle

In contemporary discourse on C2, Boyd's OODA (Observe-Orient-Decide-Act) cycle is clearly the dominant model referred to in every self-respecting briefing on C2 issues [61]. In essence, it is a concept that represents a cognitive decision-making process from observation to action. Originally, it was promulgated as an attempt to explain American fighter pilots' superior success rate over their adversaries in the Korean war – the analysis was that the superiority was due to the capability of performing decision-making cycles faster than their opponents [61]. Typically, the model is represented as a closed loop, portrayed on the left in Figure 5 below, whereas the entity of Boyd's model is better represented in the workflow-like process diagram on the right.

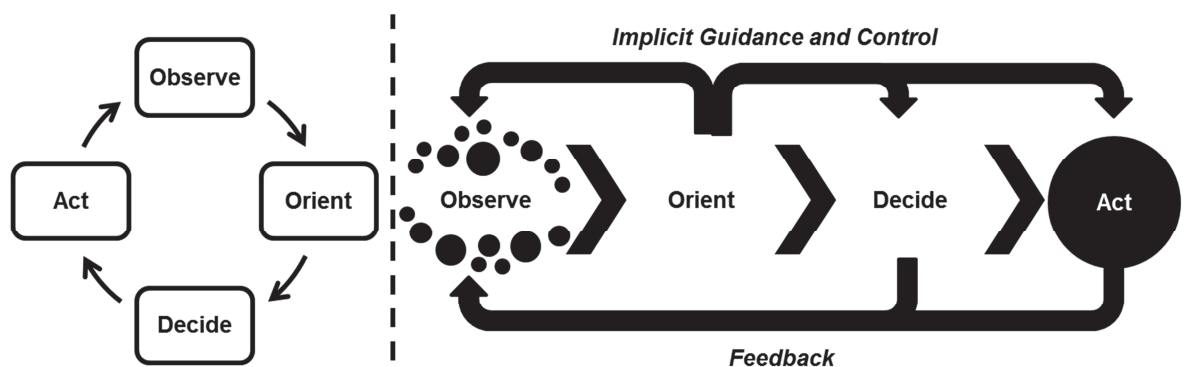


Figure 5 The OODA Cycle [61]

The simple, orbicular Byodian OODA-loop has been challenged for many reasons, not least for its simplicity. In land warfare, for example, it is argued that decision-making is a much more complex process – observations, situational aspects and angles, decisions and actions are argued to be convoluted, contrary to hands-on situations like dogfighting. [120]

Notwithstanding critique and despite its simplicity, Boyd’s OODA-loop is a sound model for decision-making – from individual to organizational level, provided that it is considered as a base model and mindset to build up from rather than a constraining checklist.

When applying the model to real-life C2 situations one comes to realize that the process involves much more than plainly decision-making itself – it is not simply an abstract phenomenon, but involves qualities (limitations and constraints as well as potential and assets) of the persons and apparatus involved. Boyd himself refined the original model over years, and other scholars have also made attempts to formulate more tangible decision making models: Lawson’s model, Wohl’s SHOR model, Brehmer’s Dynamic Decision Model of C2 and DOODA-model, to mention a few. [61] While chosen terminology and angle of approach vary, all models incorporate the fundamental concept of incorporation of new information and adaptation to it.

3.2.2 The Intelligence Cycle

In deliberate, objective-driven activities, intelligence is the process aimed at producing the required information and analysis of the situation and elements. Typically – or maybe rather traditionally – intelligence has been described through a circular model not much unlike the OODA-loop: “the intelligence cycle is the process of developing unrefined data into polished intelligence for the use of policymakers” [29]. As illustrated in Figure 6 below, it is a process that begins with direction – setting requirements for the intelligence acquirement – and resulting in dissemination of the acquired and appropriately affined information.

Traditionally, the cycle has been portrayed as an unidirectional DCPD (Direction-Collection-Processing-Dissemination) sequence on the left in Figure 6 [72]. The model has been heavily criticized to the extent of questioning its relevance even as a metaphor or analogy [140], and hence attempts have been made to better model the real-life cognitive process. One version, used in the FBI, is depicted on the right in Figure 6.

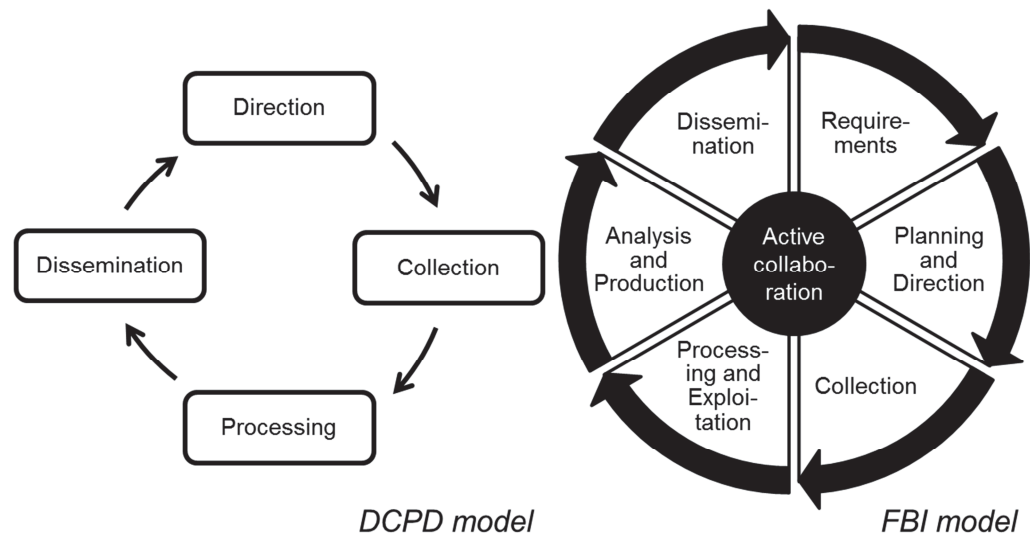


Figure 6 The Intelligence Cycle [29; 72]

In essence, intelligence can be seen as a process for establishing and maintaining situational awareness [86], and hence it is only logical that an element of cross-check – called active collaboration in the FBI model [29] – is introduced. Another way of looking at the process was introduced by Stuart Jack, depicting the intelligence analyst at the center of the cycle, being involved in all the phases of the process [72]. The fundamental insight is the iterativeness of the process, as opposed to sequentiality. When perceived as a cognitive process, this idea can be developed to the notion of the intelligence process being a both internally iterative and externally interactive, complex web of activities [77]. However, if abstaining to simplicity, the iterative nature of the intelligence process itself can be represented as an interconnected network topology of the four core functions of the original model.

3.2.3 The Intelligence Cycle as a Situation Awareness Process

In the OODA model of decision-making, the first segments can be associated with situation awareness (SA), and the latter two respectively with making decisions [63]. Bearing in mind the situation awareness function of intelligence, and understanding the concept of intelligence broadly as a process associated with acquisition of information of any appropriate kind, the intelligence process can be perceived as analogous to the SA process of the OODA cycle as depicted in Figure 7 below. The intelligence process schematic portrays it as an interconnected topology, as suggested by the Brunel team [72], which appropriately models the process as iterative, not solely confined to a fixed sequence, which is quite analogous the principles of the OODA cycle.

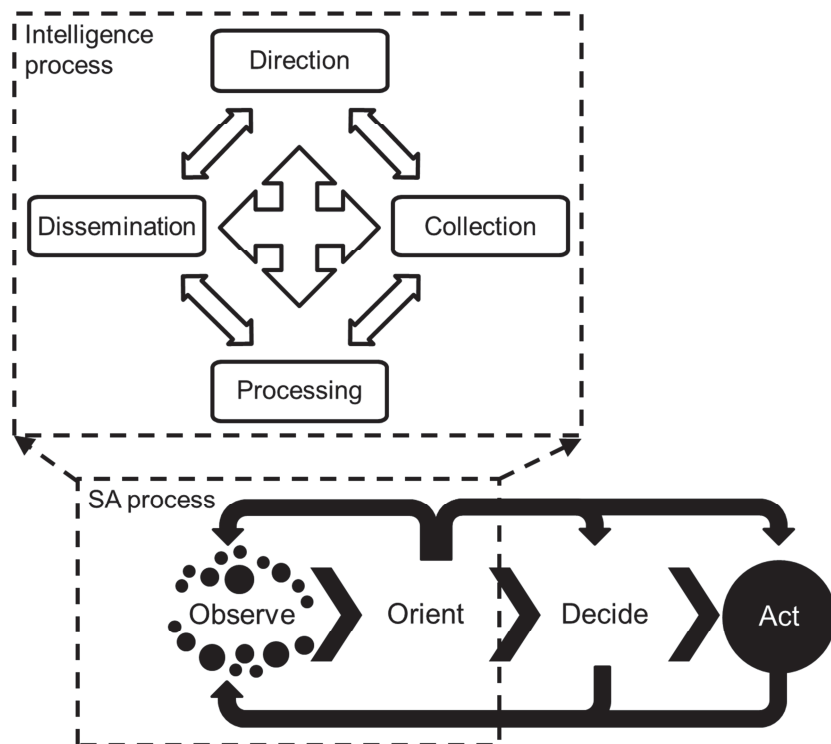


Figure 7 The Intelligence Process as the SA Process of the OODA Cycle
[61; 72]

From real-life activities' perspective, perceiving the analogue of the intelligence process to the SA process inseparably associated to decision-making is quite appropriate. When making decisions – individually or as part of a greater entity – one intuitively adapts one's thinking to the circumstantial factors involved. This, in essence, is an operation not unlike the formal representation of the intelligence process, because perception and processing of it is a concept that builds upon prior knowledge and presumptions, and processed perceptions in turn contribute to the entity of one's personal pool of knowledge. Both intuitive building of SA and the intelligence process build upon an empirical datum which, while being the basis and necessity for reflecting upon new information, is a fundamental source of bias, because the outcome is always a projection of the datum. Hence, the intelligence process should not be mistaken as an undoubtedly objective and flawless concept, but a process of perpetually refining an understanding of the perceived matter or phenomenon.

4 INTELLIGENCE IN CYBER DOMAIN

Intelligence in cyber domain – or perhaps more appropriately cyber intelligence (CYBERINT) – is a concept that is yet to receive consensus – in terms of concept as well as terminology. In order to establish a balanced conception of intelligence in cyber domain for the purposes of the thesis, a composite needs to be deduced from a number of partially contradicting points of view. In the following, this is executed through synthesizing and contrasting opinions expressed in literature and by interviewed experts.

4.1 Defining Cyber Intelligence

In many respects, the word ‘intelligence’ – and hence also ‘cyber intelligence’ – is conceived in different ways. For many, the word is mainly reserved for state-sponsored operatives and refers to legitimate activities conducted by official operatives [115; 136]. From another point of view, the term cyber intelligence is used on many occasions in a security context, the word referring primarily to intelligence on security threats and vulnerabilities – another word used is cyber threat intelligence [9; 14].

Offensive activities in cyber domain have been addressed in numerous publications. In military context, activities in cyber domain – often referred to as Computer Networks Operations (CNO) [91] – are categorized as a sub-set of information operations (IO) [79]. From this perspective, cyber warfare can be perceived as a cyberspace analogy of electronic warfare [126]. The concept of CNO is further divided into a triad of Computer Network Attack, Exploitation and Defence (Figure 8 below), in which the final aim of CNE is defined as “to gather intelligence from the target network and systems” [103].

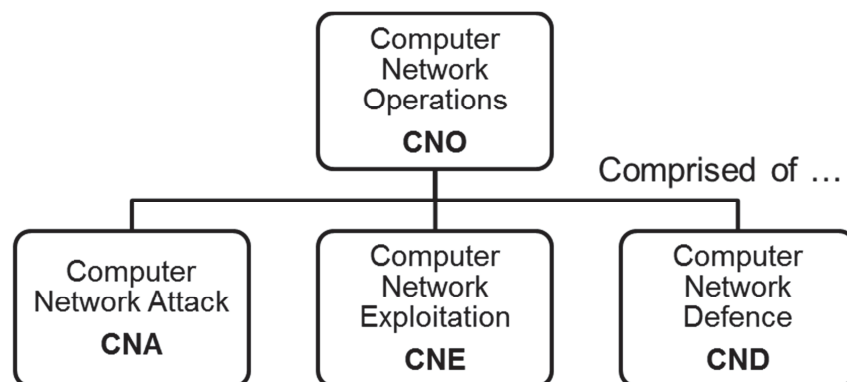


Figure 8 Relation Between CNO and CNE [103]

In his thesis, Harry Kantola, for example, has stated that conducting Computer Network Attack (CNA) -activities is dependent on advanced intelligence collection, more specifically computer network exploitation (CNE) [91]. On another account, Tero Palokangas has outlined a "computer network operations' kill-chain" [117] based on Jeffrey Carr's *Inside Cyber Warfare* [65] that strongly incorporates an intelligence – especially offensive – component. Furthermore, the role of CNE is outlined as as finding vulnerabilities, maintaining target libraries and exploiting information found on networks [117]. In conclusion, Hence, in this framework, CNE is perceived symmetrically as intelligence for CNO purposes.

On the other hand, by INSA's definition "while there is not a currently accepted definition for cyber intelligence, it should not be limited to an understanding of network operations and activities. Cyber intelligence includes the collection and analysis of information that produces timely reporting, with context and relevance to a supported decision maker. The information sources used for cyber intelligence are no more limited than they are for any other field that is observed and analyzed by intelligence professionals." [41, p. 1] Albeit indeed to the point, this view does not take a stance on the environment operated in or methodology utilized when conducting cyber intelligence. It is because the definition stands upon the premise that cyber intelligence is not a collection discipline, but "an analytic discipline relying on information collected from traditional intelligence sources intended to inform decision makers on issues pertaining to operations at all levels in the cyber domain" [105, p. 1]. Fundamentally, cyber intelligence is hence perceived as a set of analytical tools, as opposed to being a pervading intelligence discipline.

By another definition, CYBERINT is defined as "obtaining prior knowledge of threats and vulnerabilities to information communications systems through a variety of technical means." It comprises of "a series of technological and analytical approaches to cyber-specific espionage," while being "considered independent of traditional SIGINT." [60] This definition is in many respects fundamentally different from the former one introduced by INSA: it defines cyber intelligence as a collection discipline instead of a merely analytic one, however limiting it to an infrastructure perspective, aimed at mapping out points in physical and logical infrastructure exploitable for attacks. In essence, this definition does resemble that of CNE. Furthermore, utilization of cyber means for acquiring information within the data content in cyber domain or about the physical world and its inhabitants are perceived as subordinate to other intelligence disciplines: "for the purpose of conventional intelligence

collection [it] can include the penetration of foreign networks to secure information on weapons systems, policy positions, and much more. It is invasive, yet does not disrupt, deny, or destroy data, it collects” [60].

From the Finnish Defence Forces’ perspective, cyber intelligence – or information and computer networks intelligence³ – is a subset of SIGINT, alongside with ELINT and COMINT, and is further divided into intelligence on telecommunications⁴ and (foreign) intelligence on information systems⁵ [64; 92; 97]. An illustration of the Finnish military intelligence discipline hierarchy is portrayed in Figure 9 below.

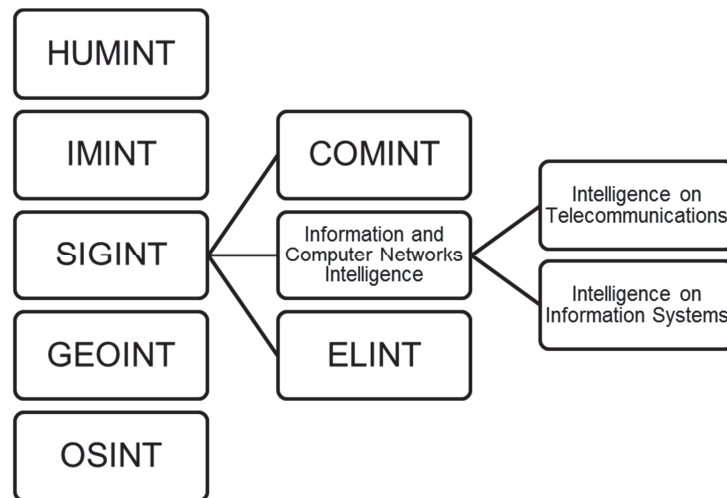


Figure 9 Finnish Classification of Military Intelligence Disciplines [97]

The fact that processing and analyzing data collected using named methods does not differ from other SIGINT analysis [92] strongly advocates the set definitions. From a military intelligence point of view, cyber domain provides a new ‘frequency band’ to exploit, and cyber intelligence can be seen as extending SIGINT to a new spectrum [92]. Intelligence on telecommunications is defined as intelligence on network traffic in cross-border computer telecommunications cables, possibly implementing elements of both COMINT and ELINT, and foreign intelligence on information systems as technical intelligence activities aimed at data on information systems outside the nation’s borders. [113] Being formulated for legislative purposes, the definition is quite confining and dictated by need for clear jurisdictional boundaries, but indeed does define essential elements of the entity of cyber intelligence.

³ Tietoverkkotiedustelu [113]

⁴ Tietoliikennetiedustelu [113]

⁵ Ulkomaan tietojärjestelmätiedustelu [113]

It can be argued that the definition excludes intelligence incorporating a real-world component and, furthermore, that there are additional matters and targets that are both possible and desirable to reconnoiter through cyber means [90]. Furthermore, it has been observed that in general intelligence activities have extended to the new cyber domain, while intensity of traditional, physical domain intelligence disciplines has not noticeably decayed [81; 89], indicating that cyber intelligence has grown to complement other forms of intelligence, which is only logical, because intelligence serves the purpose of acquiring information, which today majorly inhabits the digital realm [102].

One key aspect that consensus is established upon is that the concept of cyber intelligence strongly involves cyber domain – or cyberspace – determinatively as the medium and majorly also as the field for activities [64; 80; 81; 89; 90; 92; 95; 99; 102; 112; 115; 116; 121; 131; 136]. Depending from standpoint and background, there is fluctuation in the details and nuances of how the concept of intelligence in cyber domain is perceived. Mikko S. Niemelä [112], for example, emphasizes human-machine interaction at the periphery of computer networks, pointing out that the information of true value is namely the content produced by humans. Rain Ottis, on the other hand, emphasizes the nature of intelligence as violating confidentiality of information, and hence specifies the main driver of cyber intelligence activities as obtaining access to confidential data. Furthermore, from his point of view, activities constitute as cyber intelligence given that they incorporate exploiting vulnerabilities that allow access to logical structures of information. [115] Consequently, attacking, penetrating and even modifying a system constitutes as cyber intelligence given that the motivation is intelligence acquisition, not sabotage or other disruptive purpose.

Although definitions and conceptions mostly address intelligence – and other activity – associated with cyber domain symmetrically as associated with only that environment. However, it can be argued that there is a physical domain component to the phenomenon [90]: intelligence on whereabouts and activities of targets in the physical realm through the cyber domain [91; 99], which is in tune with the conception that cyber intelligence collects information about human-machine interaction [112]. For example, utilizing sensors on computers, mobile phones, etc. provides a wide range of exploitable information, ranging from audio-visual to spatial, movement and orientation information [80; 99]. Furthermore, it can be argued that breaching the confidentiality of information in cyber domain through physical domain actions can be categorized as cyber intelligence, for example introducing physical keyloggers to a system or hacking a system on-site [87, pp. 62–63].

One controversial aspect of categorizing and defining intelligence acquisition in cyber domain is information that is publicly available. Many make a distinction between open-source intelligence (OSINT) and cyber intelligence [81; 115], however the border is difficult to draw [131]. Analogously to afore mentioned view that cyber intelligence can serve as a collection method for conventional intelligence [60], it can be pointed out that OSINT is an intelligence collection method that can be conducted in many environments [92]. Currently, almost all aspects of life – intelligence included – utilize computers in various ways, often very comprehensively, but in most cases the activity does not amount to utilizing cyber methods per se, more aptly are they characterized as computer-assisted. Analogously, it is apt to conclude that extending open-source information searches to digital domain does not automatically amount to being cyber intelligence [115]. One suggested characterizing distinction is intentionality of publicity of the information [89; 115]. For example, newspaper articles, blog postings, tweets etc. are intended to be public and available to virtually anyone. However, acquiring information from non-protected corners of the ‘dark web’ [80; 90] or utilizing metadata of files submitted online [10; 28; 78] do not quite stay within limits of exploiting intentionally available information.

It can be argued that OSINT in cyber domain can involve a component that has HUMINT characteristics [92], and the same can be argued about social engineering [64]. One good example is conducting intelligence collection in social media, which by nature inseparably is associated with human interaction, and more importantly social networks are “amazing sources of information” [108, p. 37]. Furthermore, publicly available information is noted as an inherent and inseparable element in preparation and reconnaissance of operations in cyber domain, hacking activities for example [106], which would suggest an open-source element to cyber intelligence [99; 116]. One sound argument is that searching information online using ‘obvious’ methods – such as ‘googling’ – does not amount to being cyber intelligence [115], but rather ordinary OSINT. However, when conducting intelligence in public cyber domain in a more sophisticated and targeted manner, the setting is prominently different, because then the cyber aspect can provide possibilities beyond real-world analogies. For example, ‘Google hacking’ [131], ‘big data’ analysis of public information [90], targeted searches in social media services [81] and many other target- or purpose-specific methods are well beyond ‘obvious’ and can quite acutely outperform traditional intelligence disciplines in many respects. A sensible borderline is difficult to define [131], and undeniably cyber methods apply to OSINT [99]. In the framework of examining intelligence acquisition specifically in cyber domain, however, artificial exclusions can be concluded counter-productive rather than

promoting, because such exclusions render the perspective incomplete and thus limit also the conclusions drawn.

The definition of intelligence in cyber domain is not entirely agreed upon. It can quite confidently be concluded that one definitive attribute is the utilization of cyber domain. Furthermore, penetrative techniques of acquiring information are agreed to comprise cyber intelligence, as are monitoring ones and those having a physical-domain component. Disagreement exists however, about whether open source intelligence collection should be excluded. When considering expressly intelligence in the framework of cyber domain, it can, however, be concluded that all methods collecting information from cyber domain or through it about the physical one.

4.2 Characteristics of Cyber Intelligence

Intelligence in cyber domain is perceived to have both advocating as well as contesting characteristics. First of all, a distinct strength is seen in the stealthiness – or taste- and odorlessness – of cyber activity [80]. Albeit evading attribution is of utmost importance to cyber operatives [80], the digital realm allows easy deniability of any accusation [81]. Furthermore, phenomena occur in cyber domain at the speed of light which, given the right circumstances, translates into high speed of intelligence collection [131] and consequently lesser probability of immediate detection. Especially in the realm of military intelligence, cyber intelligence acquisition requires relatively low investments initially and for operation [92], making it an inexpensive way of gaining access to vast amounts of information [94]. Instead of financial assets, cyber intelligence requires wit and expertise [92], denoting that the key element of an operation is the level of expertise of the personnel [102; 131].

Furthermore, the networked and global nature of the cyber domain has resulted in diminishing significance of physical distance and proximity, facilitating that many operations can be conducted remotely [99]. However, this does not exclusively denote unlimited global reach, because the target has to be identified before engaging [90], which in turn may require initial support from another intelligence source [131]. One opportunity deriving from negligibility of physical location is that operatives – especially illicit – can freely choose an appropriate jurisdiction for conducting their business [115], thus excluding the risk of apprehension and prosecution in case of getting attributed to the activities conducted.

The reach of cyber intelligence methods can be limited by physically isolating confidential interaction and information from the cyber domain – for example conversing in person in a space with no digital devices or making notes on paper – or by applying cryptographic methods [81; 102]. However, records of such interaction can be made second-hand and hence indirectly intercepted [112]. Encrypted communications, on the other hand, can be detected and possibly intercepted at end-user interface where encryption is not present [81]. Albeit critical – and hence attractive – information often is isolated [102] and access to it is controlled, it is still bound to be accessed, and the interface access allows for a vast number methods of breaching the isolation [99]. Virtually anything with bytes is a potential threat [131], meaning that cyber methods possess high versatility and agility. However, the reach – or very existence of cyber capabilities – is dependent on the existence and span of the man-made infrastructure the cyber environment is built upon [97; 112].

One significant limitation of intelligence collected by cyber means is contextual ambiguity [94; 112] as well as difficulty of verification of collected information [131]. Information collected exclusively in cyber domain often lacks detail that identifies the context of activity observed [112], and hence false conclusions can be drawn. Furthermore, digital information can be forged [94; 115], which allows for deliberately misinforming the intelligence collector. Because physical locations of target systems can be unclear [90], this attribute poses a potential threat of conducting cyber intelligence acquisition in an adverse environment, risking attribution. In general, one weakness of conducting cyber intelligence – especially offensive and intrusive – is that cyber activities often leave traces [92], and upon detection the target may exploit the established connection in a number of ways ranging from hack-back to deliberate misinformation [81; 131]. Furthermore, when conducting intelligence – or any other activity – in cyber domain, one faces the risk of malware and other threats. Another potential and potent threat to cyber intelligence acquisition is information overload caused by vast amounts of available digital information [115], and together with the possibility of misinformation and contextual disambiguation reliably refining intelligence from a vast data mass might prove too difficult a task. Figure 10 below depicts the afore examined attributes of cyber intelligence acquisition in a SWOT matrix.

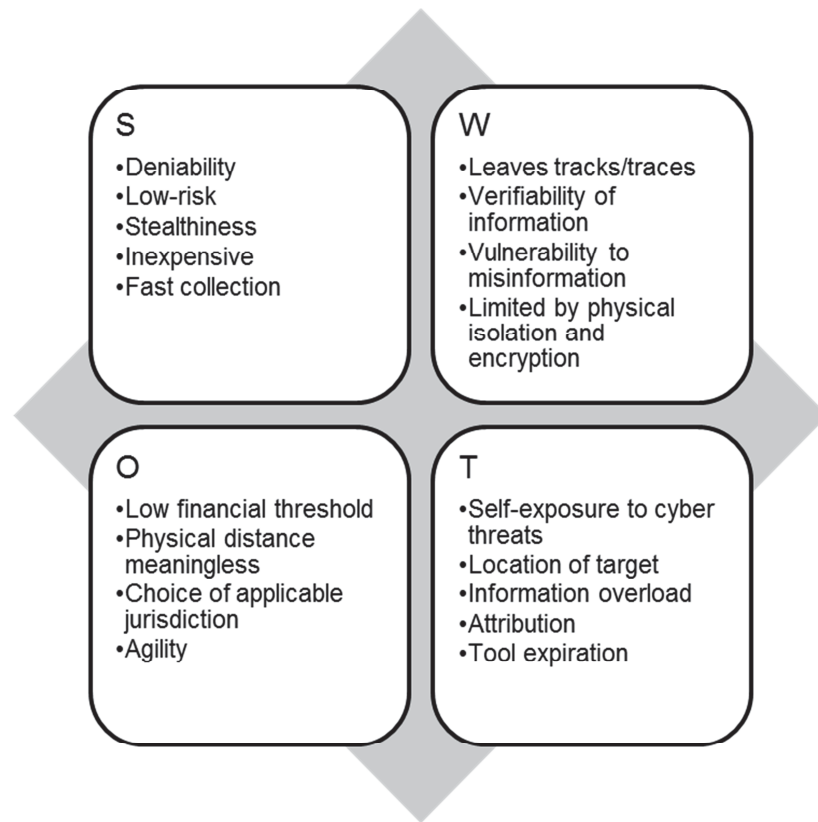


Figure 10 SWOT-analysis of Cyber Intelligence

4.3 Cyber Intelligence as an Extension of Conventional Intelligence

Cyber domain allows for implementing more effective alternatives to other intelligence disciplines, for example tracking a person through his mobile phone's position update [81] instead of following him in person. Characteristic to cyber intelligence acquisition is that it is the only way of acquiring direct access to information that exists only within the digital realm [81]. From a larger perspective, however, adequate intelligence acquisition solely from the cyber domain is neither possible nor practical [81], except for the purposes of targeting for offensive cyber operations [92].

The cyber domain can be considered a new realm of conducting activities [99] into which today's information has heavily concentrated [81; 99]. Consequently, intelligence has extended to cyber domain alongside with physical domain intelligence remaining active [81; 89]. Arguably, intelligence should be considered a unified entity in which all branches endorse each other [95; 131]. As part of all-intelligence collection, cyber intelligence benefits and endorses other forms of intelligence, and in turn cyber intelligence is endorsed by information from other sources that is unreachable by cyber means. Moreover, it can be concluded that cyber intelligence can be considered an endorsing, cross-cutting extension of

conventional intelligence that extends the reach of all conventional intelligence disciplines, as illustrated in Figure 11 below:

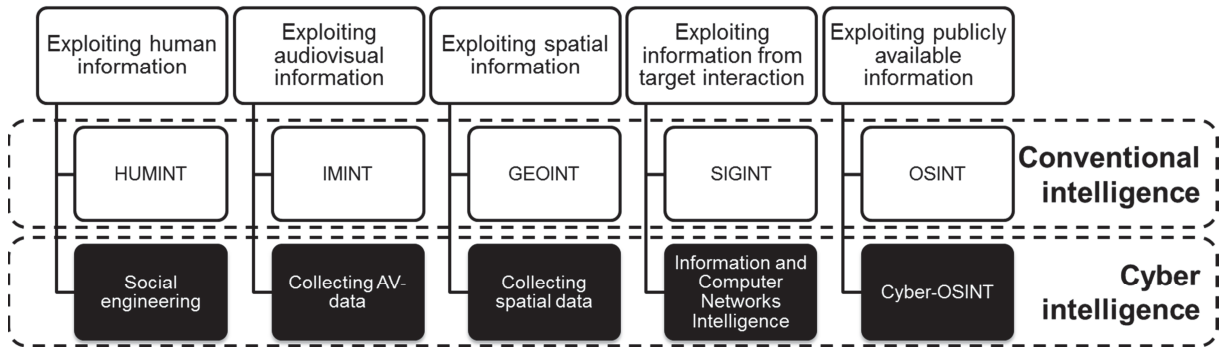


Figure 11 Cyber Intelligence as an Endorsing Parallel of Physical Domain Intelligence

4.4 Operatives of Cyber Intelligence

Cyber intelligence methods are to a high extent available to virtually anyone. However, based on motivations, the users can be divided to a relatively small number of categories. On one account, most cyber intelligence activities can be assimilated to business efforts, leaving out only ideological actors [112]. Mikko Hyppönen [82], however, has categorized threats to privacy in cyberspace in three groups:

- online criminals
- ideologically motivated operatives, such as hacktivists
- nation states, governments.

Considering parties conducting intelligence collection, the above outlined categorization encompasses majority of those of significance. The most sophisticated operative type is the nation state. Typically, such are associated with APT threats [49] and pose targeted threats especially to government agencies and companies of interest. The motivation and objective of a nation state's cyber intelligence efforts are typically intelligence collection and possibly sabotage [81], and the efforts extend enduringly over a long period of time, targeted specifically, carefully concealed [4].

Criminals, on the other hand, are driven and motivated by money [81]. As such, their efforts are commonly directed at maximizing coverage – number of malware infections or successful phishing e-mails – instead of conducting focused, stealthy efforts [49]. As opposed to

sanctioned nation state actors, criminals usually lack the jurisdictional privileges of the former. However, in some cases criminals have been involved in government-sanctioned intelligence efforts [92], effectively transforming the legal constraints of common criminals. In addition to criminals, many businesses conduct intelligence acquisition for their own purposes – legally or illegally – having fundamentally the same financial driving factor in their operation, but carrying out the activity more in the form of legitimate market information collection or corporate espionage. Furthermore, businesses may as well be involved in government-sanctioned intelligence collection or benefit from intelligence gathered by their governments [112].

In addition to government sanctioned intelligence collection and financially driven such, another prominent operative is an ideological one: hacktivists. Instead of money or other gain, a hacktivist is driven and motivated by protest [81], thus changing the focus of interest to that of an ideology. Although ideological ambitions may take many forms, a hacktivists actions generally are logical [81], aimed at correcting a wrong, proclaiming a message or preventing actions that conflict with their ideology. Other, marginal types of actors involved in forms of intelligence collection exist, comprising curiosity-driven actors such as script-kiddies and ‘old-school’ code writers as well as radical groups [81].

5 A HIERARCHICAL MODEL OF INTELLIGENCE IN CYBER DOMAIN

For the purpose of analyzing and examining intelligence in cyber domain in a systematic and balanced manner, a unified model of the affiliated functions is required. Such a model is, however, not readily available in existing literature. The bulk of literature addresses intelligence from a security point of view, assuming the point of view and role of the target for intelligence collection. With the vast increase of publicly known breaches in private, commercial as well as government-related breaches of confidential information, this focus answers to the acute need to address discrepancies in security measures of existing technology. Year 2014, for example, has been concluded to have been “a year of mega breaches,” with publicized incidents affecting hundreds of millions customers [1].

The understandable and admittedly essential focus on security measures, however, is limited in respect to understanding the phenomenon resulting in the discrepancies. Another typical focus is to address and examine different fields of cyber activities providing the technical and methodological solutions aimed at breaching the confidentiality of undisclosed information. For example, numerous studies and have been made on the hacking process and hacking as a phenomenon – one prominent and well-known publication is *Hacking Exposed 7* [106], and there exists a virtually endless variety of case-type inquiries and studies [46; 68] as well as news articles about uncovered hacking incidents. Another area that has received in-depth attention is social engineering, being closely entangled to hacking. From another point of view, technical surveillance methods have been uncovered especially through leaks of classified information.

However meaningful in understanding the vast potential risks to confidentiality and security of confidential information, descriptions of technical and methodological solutions enabling exploitation of information do not aim at establishing profound understanding about the phenomenon of intelligence in cyber domain. In order to develop such understanding, the entity of intelligence in cyber domain needs to be arranged and categorized in terms of logical sub-sets. For this purpose, existing more narrow and focused models can be used to deduce an universal representation.

5.1 Identifying Cyber Intelligence Methods

Perhaps the most prominent phenomenon providing – at least most stereotypically associated with – utilizable intelligence is hacking. One well-expressed and useful model is the hacking process [132] presented in Figure 12 below. The process is expressed as a logical workflow starting with footprinting, followed by scanning and enumeration of the target system, which after access is gained through identified exploitable vulnerabilities. Having established access, the attacker is enabled to escalate access to the system, pilfer information and possibly alter the system in order to cover tracks and create back doors. If the motive of the intruder is offensive, gained access can be exploited to deny the service of the system. [106]

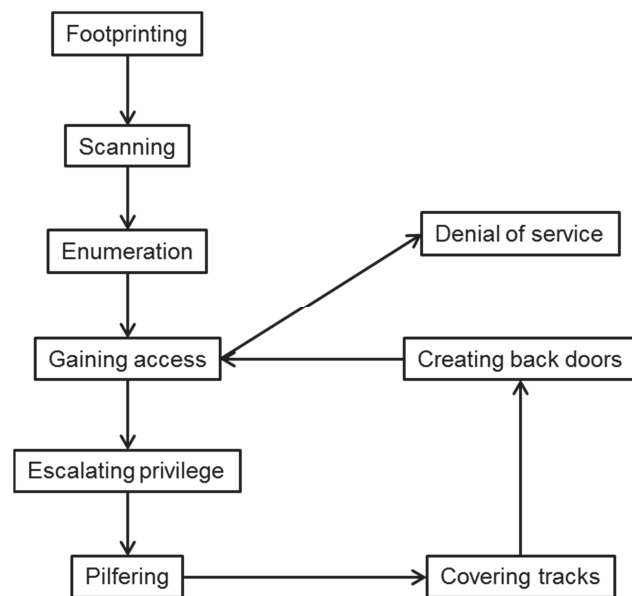


Figure 12 The Hacking Process [106; 132]

In the described model of the hacking process, footprinting is understood as reconnaissance of the target system, carried out through collecting publicly available information about the target and its systems, ranging from technical data such as domains and their metadata, IP addresses, used technical infrastructure as well as contextual data such as publicly available information about the target and its affiliations, i.e. for example information on a target organization, its personnel, known practices and security measures, upcoming events etc. [132] From an intelligence perspective, the activities carried out in the footprinting phase of the workflow can be understood as open-source intelligence (OSINT), which is “drawn from publicly available material, including” the Internet, traditional mass media and various specialized publications, audio-visual material and geospatial information [31].

This is not to say, however, that all information is unlimitedly accessible – gaining access to the sources may require effort in a number of ways, technical, spatial as well as contextual [142]. Technical effort might mean for example utilizing non-indexed sources, i.e. dark web information inaccessible through search engines, or sources available in commercial databases, accessible after paying for access rights. Spatial effort might, for example, mean accessing possibly even unique information that exists only in non-digital form in designated locations such as archives or libraries. Although working language in many disciplines is often English and likewise information directly related to technical descriptions or topologies of computer systems, which enables low threshold of comprehension of information, in many cases information exists in such a form that requires special contextual expertise in order to exploit it – the required contextual effort might range from plain linguistics to comprehension of complex concepts [136].

For the purposes of a model of cyber intelligence methods, footprinting translates to OSINT. Bearing in mind established definition and preconditions of cyber intelligence, the whole spectrum of OSINT should not, however, be included, but limit the discipline to information accessible through cyber means – i.e. information available on or accessible through computer systems or networks. As a distinction between this sub-set and other open-source information, terms Cyber-OSINT and Non-Cyber-OSINT shall be used, and the former included in the set of methods to be analyzed.

Having established available open-source information through footprinting, the following stage of the hacking process workflow is scanning. Scanning is an active networks reconnaissance process that provides information on services (ports, protocols) and infrastructure (topology, superficial identification and classification attached devices) of the perceived target system [132]. Scanning provides the operator with a detailed technical overview of the target system visible from the established point of view, facilitating identification of possible access points to it.

After adequate scanning of the target system, the hacking process proceeds to enumeration of individual entities the target system. Based on initial perception of the target system, entities of interest are identified and fingerprinted more closely, providing more detailed information of the system – account names, detailed identification of services and their versions etc. Hence, specific exploitable vulnerabilities and points of prospective access are defined. [106; 132] As an intelligence method scanning defines the perceived infrastructure landscape,

analogously to visual scoping of landscape and surroundings in the physical world, whereas enumeration can be perceived as analogous to zooming in on identified points of interest in a scoped landscape. Both being active and probing in nature, although differing in scope and resolution, scanning and enumeration can be treated together as an intelligence method. However, the risks and considerations involved differ between operating in public and restricted domain, and thus the activity shall be treated separately in these two situations.

In the hacking process, stages of footprinting, scanning and enumeration of a target system can be understood as an iterative, narrowing-down process aimed at establishing a feature or features about the target system available for exploitation – the deduced information can then be used for gaining access or directing an DOS or DDOS attack on the system [106; 132]. When considering the purposes of intelligence, attacking the system can be omitted. Gaining access to the system, however, is a meaningful stage of the hacking process in terms of gaining intelligence. The set of possible technical solutions for establishing access to a system is vast, and the choice of method is made based on identified exploitable vulnerabilities. For example, access can be gained through exploiting known standard passwords, faking authentication through eavesdropping on traffic packages, accessing backdoors in the software present on the system, extracting and cracking password HASH files etc [106; 132]. Gaining access to the target system can be considered as an individual method of cyber intelligence, being by its intrusive nature analogous to breaking through physical boundaries and restraints such as doors and locks. As an individual intelligence method, gaining access can be translated to intrusion, meaning illicitly crossing over to within a system of interest.

In the hacking process workflow, gaining access is followed by escalating privilege [106; 132]. In terms of technical solutions, the process is iterative from the new standpoint inside the system, establishing a new set of perceived objects of interest and identifying specific exploitable properties. In terms of intelligence methodology, escalating privilege does not translate to yet uncovered methods. However, by definition footprinting cannot be considered a sub-set of OSINT while acting inside a restricted system. Instead, the term exploiting privileged information shall be used. Scanning and enumeration, on their behalf, can be treated as such inside the target system as well, but by nature the activity possesses different qualities in terms of detectability, and thus the activities shall be treated separately outside and within a system.

Furthermore, the hacking process proceeds to pilfering of information, meaning extraction of data from within a privileged system [106; 132]. When operating inside restricted environments, perceiving the system and extracting data from it are fundamentally two distinctively different types of activity. As a real world analogue, pilfering translates to physically carrying items out from guarded premises, and terminologically in an intelligence framework, the term exfiltration shall be used. As a method of cyber intelligence, exfiltration can take a great number of forms, ranging from utilization of physically transportable containers (physical drives etc.), incorporating encryption or steganography, using common data transfer protocols or other fathomable methods, for example screen shots of accessed data, copying by hand, memorizing etc. – such methods can be classified as out of band [55, pp. 125–126].

The last steps of the hacking process workflow are covering tracks and creating back doors [106; 132], meaning altering access privilege and tracking information within the system in order to stealthily maintain or create new means of accessing it, for example creating back doors. As methods of cyber intelligence, these translate into concepts of obfuscation and sustaining access. Physical analogues for them are, for example, repairing inflicted damages caused in the process of entering or disabling surveillance and opening locked doors and windows respectively.

The above described hacking process does not, however, represent the entire scope of methods utilizable in cyber intelligence. In essence, the described hacking process is a targeted, technology-oriented methodology of infiltrating a restricted target system of interest. Albeit effective in accomplishing the specific task, its set of methods possesses little qualities that would facilitate exploitation of human vulnerabilities. On the other hand, it by nature builds upon existing qualities of systems and infrastructure, and does not proactively create opportunity for intelligence collection. Nor is it a set of methods that would incorporate deriving information through surveilling mass or individual activity. However, hacking can be a valuable contributing factor in gaining access and information supporting and enabling such capabilities.

Whereas scanning and enumeration are methods for working toward gaining access inside a target system, more is required for developing higher level of situational awareness within it. For purposes of establishing an encompassing picture of the target infrastructure both in terms of interconnectivity, levels of accessibility and hardware and software configuration,

methodology of scanning and enumeration can be utilized for the purposes of determining the detailed topology of the infrastructure – possibly simultaneously with respect to internal and external connectivity. One descriptive term for this is ‘lateral movement’ [115]. By nature, this activity can enable both deducing intelligence about the organization using the network and thus working towards desired intelligence aims and, not less importantly, facilitate the use of other methods. Being both more profound and elaborate in nature as well as facilitating a fundamentally higher level of understanding of the target infrastructure, this activity shall be treated as an individual intelligence method, referred to as network mapping.

The discipline exploiting the direct human aspect in vulnerabilities is called social engineering. It is not a single technical solution, but a range of both technical and sociological means of deception aimed at exploiting the thoughtlessness, gullibility and/or lack of suspicious thinking that allows a perpetrator to gain more access to information or to systems containing information [123]. Reflecting on more traditional intelligence disciplines, the core quality of social engineering – exploitation of persons and their knowledge – is closely related of those of human intelligence (HUMINT), which “is defined as any information that can be gathered from human sources. [...] Understanding people, with all of their complexities, is crucial to the business of running assets to collect HUMINT” [30]. Often social engineering is performed in a way that misleads a person through persuasion or deception to perform a desired task, for example to install a malicious software or enter a website that has malicious intent. This nature of exploiting users and their flaws is not only characteristic, but also unique in the spectrum of methodology in the cyber domain, and hence social engineering should be treated as a separate intelligence method.

Many of the methods for intelligence collection in cyber domain are limited to accessing digital information within computer systems and networks. The objectives and motives of cyber activity, however, originate from the real world and from desires of individuals or organizations [105], and hence the objectives of intelligence collection in and through cyberspace are fundamentally related to the real world. Bearing this in mind, collecting intelligence about real-world targets (persons, objects etc.) through cyberspace can be resourceful in many respects. Most currently used computers have built-in webcams and microphones, and the amount of smartphone users is predicted to reach $1,75 \cdot 10^9$ in year 2014 [47], which makes the personal devices a vast potential source of information. Several cases of eavesdropping on audio and video sources have been reported [111; 129], and the increase of sensors on end-user devices facilitates increasingly detailed information to be collected

through them [80]. Crossing over from the digital domain to the real world is by nature a distinct kind of intelligence collection, and hence physical surveillance through cyber means shall be treated as an individual intelligence collection method.

Whereas many cyber intelligence methods target individual entities (systems, organizations, individuals etc.), much can be learned from analyzing the traffic within a network. Many companies, VeriSign for example, offer tools for network analysis “designed to provide telecommunications carriers with cost-effective solutions for revenue assurance and network optimization” [52]. While motives can on many occasions be legitimate, analyzing network traffic and behavior can be used for deriving situational awareness on multiple levels. Changes in macro-level traffic patterns can indicate a changes or disturbance in both cyber and real-world domains, for example in real-world be a sign of a terrorist attack or an outbreak of a disease, in cyber domain on the other hand a sign of a DDOS attack or the emergence of a new malware [83]. On micro-level, changes in an individual’s activity on social media (Twitter, Facebook etc.) can indicate changes in his/hers real-life tendencies [134]. In many countries, for example Sweden, legislation permits collection of intelligence from network infrastructure. This does not, however, imply a *carte blanche*: intelligence collection is strictly regulated and monitored. [85] Terminologically, intelligence collection based on online activity shall be referred to in the study as network surveillance.

One phenomenon having practically as long a history as cyberspace itself is malware. Whereas in early times malware proved to be more of a nuisance to users through crippling systems or causing massive spamming, recent developments have proven that malicious programs increasingly endanger confidentiality of information, along with its integrity and availability. The scope of malware capable of data theft ranges from mass-targeted ones that steal private confidential information (usernames, passwords, credit card information etc.) of anyone they might come across [40] to target-system or target-organization specific surveillance [143]. Compared to other cyber intelligence methods, the use of malware is characterized by independence from operator oversight, and thus shall be treated as an individual method of intelligence collection or enabler of the use of other methods through creating points of entry.

While most cyber intelligence methods are characterized by the ability of being carried out remotely, but much can be achieved through physical proximity and access as well. Such attacks are referred to as physical attacks, which can range from personally accessing a target

system on-site (for example accessing an equipment room, performing a cold boot attack) to introducing malicious hardware to the target system (for example a keylogger or network-connected hacking device) [87, pp. 62–64]. While a physical attack may in many cases risk detection and perpetrator identification, if successful it can at best circumvent a system's whole security infrastructure.

For most parts, cyber intelligence collection methods are characterized by exploiting existing vulnerabilities in existing software and hardware infrastructure – in a sense, actions are hence dictated by the cyber terrain. This postulate, however, only applies to the extent where software and hardware supply chain stays intact and is not affected by actors with means to alter products in order to serve their own cause. Vulnerabilities of components in cyber infrastructure typically arise from flaws – intentional or non-intentional – spanning over the whole life cycle of an infrastructure. With vulnerabilities originating spontaneously in the supply chain, it is hardly implausible the “supply chain for electronic components, including microchips, could be infiltrated at some stage by hostile agents” [59]. The software supply chain, on its behalf, “connects software suppliers, service suppliers, contractors, distributors, retailers and end-users. The structure is so complex that potential risks exist in every step.” [73] There have been alleged cases of manufacturers' shipped hardware being diverted to an intelligence agency's workshop for alterations before being delivered [88], as well as aspirations to dictate building-in vulnerabilities by legislative means [75]. While requiring prominent capacity in order to avail, “once malicious firmware has been inserted into electronic components, it can be almost impossible to detect” [59], which stands also in cases of pre-installed compromised software. Thus, alterations made in the supply chain are considered an individual method in the cyber intelligence collection methods' framework.

5.2 Identifying Evaluating Criteria

Having established a set of categorized intelligence methods in the cyber domain, a set of criteria is required in order to assess and evaluate the value of different intelligence methods. Existing, publicly available models for evaluating intelligence focus mainly on the cognitive factors and security processes, the perspective being majorly military [29]. When assessing the entity of methods for cyber intelligence from a more general perspective, a somewhat different perspective is justifiable: the choice and extent of use of intelligence methods is not solely dictated by performance, but need to be balanced with respect to risk and capability.

In a study made on military intelligence, it was concluded that the effectiveness “is directly related to how useful its output is to users” [130]. Since intelligence is often time-critical, especially in the cyber framework where advancements can take place nearly at the speed of light, the speed of a method is to be considered a meaningful factor. Intelligence collection resources are seldom infinite and the volume of raw data available virtually abysmal, which demands efficiency of the method used. In order to be capable of deducing meaningful information from the environment, the resolution of the method used needs to be sufficient. Especially in cyber domain where the context of activity can in many cases be ambiguous [112], it is imperative that the information collected can be verified to a sufficient level of certainty. The products of intelligence – be it in a military, business or other context – are fundamentally a basis for decision-making and situational awareness, which calls for precision, which can be evaluated in terms of validity and reliability.

Perhaps the most self-evident criterion for evaluating intelligence is the capability of the method. Considering the dependency on technological aspects, being up-to-date in terms of technology is imperative, especially being sufficiently informed about the prospects in the target environments and possessing sufficient technology to advance one’s objectives. The former is highly proximate with the requirement of technical expertise: the more sophisticated the target organization and systems are, the higher level of expertise an operator requires. In addition to that, when it comes to information of non-technical nature, sufficient contextual expertise is required as well – for example linguistic skills or understanding of other specialty fields. Even though many point out that carrying out tasks in cyber domain can be relatively cheap [92], one must not overlook the impact of resources – funds and number of personnel – on effectivity. Intelligence is goal-oriented by nature, aimed at providing sound information for decision-making. In order to efficiently allocate tools and personnel to tasks that serve the desired purpose, leadership is required. No intelligence discipline is intended for operating individually, but their efforts are used to both verify each other’s observations and assessments and steer and focus efforts toward requirements yet to be met and matters requiring closer observation. Hence from intelligence collection point of view, the support of other intelligence sources is to be considered.

Thirdly, for both legal and secrecy reasons, the use of cyber intelligence methods bear risk factors to be considered. Firstly, jurisdictional limitations are a significant risk factor for any operative in cyber domain: even though little international consensus exists regarding cyber intelligence activities, national legislation differs intensely from a country to another, which is

a factor most operatives need to bear in mind when conducting cyber activities. Secondly, secrecy is in many respects a quality to be fostered in cyber domain: avoiding attribution to dubious let alone illegal activity is in most cases to be pursued, detection of used methodology and tools might render them useless, and a target noticing getting attention can complicate an operation significantly. As risk factors, these translate into exposure of method, operative and target.

5.3 Identifying the Operative Types

In order to analyze the qualities of the identified cyber intelligence methods with respect to the identified evaluating criteria, the circumstantial perspective needs to be defined in terms of operative, target and setting. In order to grasp an encompassing understanding about the subject, it is convenient to choose perspectives from different verges of the field. In order to facilitate a analysis, framework scenarios are needed in order to sensibly evaluate the methods against the criteria. Scenarios are derived from the core categorization outlined by Hyppönen, discussed earlier in Section 4.4:

1. Finnish criminal organization, operating from Finland.

- Objective: acquire any information and means exploitable for direct financial revenue.

2. Hacktivist group from an Arabic-speaking country, operating from the Middle East.

- Objective: defacing official Finnish government websites and social media accounts with propaganda of the group's ideological agenda.

3. Non-European foreign nation state, conducting intelligence operations on Finnish target organizations and systems.

- Objective: acquire confidential information about Finnish R&D on online communication security technology.

5.4 A Hierarchical Model of Cyber Intelligence

The identified set of cyber intelligence methods and assessment criteria are formulated into an AHP hierarchy. Table 1 below summarizes the identified intelligence methods, evaluating criteria and circumstantial perspectives. From the methods and criteria, an AHP-hierarchy can be composed, treating the intelligence methods as alternatives of the hierarchy, and the evaluating criteria as criteria and sub-criteria of the hierarchy.

Table 1 Elements of the Hierarchical Model of Intelligence in Cyber Domain

Intelligence Methods	Evaluating Criteria	Circumstances
Cyber-OSINT	Performance	1. Finnish criminal organization, operating from Finland. Objective: acquire any information and means exploitable for direct financial revenue. 2. Hactivist group from an Arabic-speaking country, operating from the Middle East. Objective: defacing official Finnish government websites and social media accounts with propaganda of the group's ideological agenda. 3. Non-European foreign nation state, conducting intelligence operations on Finnish target organizations and systems. Objective: acquire confidential information about Finnish R&D on online communication security technology.
Scanning and enumeration in public domain	Speed	
Scanning and enumeration in restricted domain	Efficiency	
Intrusion	Resolution	
Exploiting privileged information	Verifiability	
Exfiltration of data	Validity	
Obfuscation	Reliability	
Sustaining access	Capability	
Network mapping	Technology	
Social engineering	Expertise	
Physical surveillance	Technical	
Network surveillance	Contextual	
Malware	Resources	
Physical attack	Leadership	
Alterations in the supply chain	Support from other INTEL	
	Risk	
	Jurisdiction	
	Exposure of operative	
	Exposure of method	
	Exposure of target	

For the purposes of collecting expert assessments, the online interface of Expert Choice Comparison Suite is utilized, allowing the contributors to submit evaluations as an online survey. The matrix of composed AHP-hierarchy is displayed in Figure 13 below.

	Evaluating Criteria															
	Performance						Capability						Risk			
	Speed	Efficiency	Resolution	Verifiability	Validity	Reliability	Technology	Expertise		Resources	Leadership	Support from other INTEL	Jurisdiction	Exposure of operative	Exposure of method	Exposure of target
								Technical	Contextual							
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Cyber-OSINT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Scanning and enumeration in public domain	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Scanning and enumeration in restricted domain	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Intrusion	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Exploiting privileged information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Exfiltration of data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Obfuscation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Sustaining access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Network mapping	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Social engineering	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Physical surveillance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Network surveillance	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Malware	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Physical attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Alterations in the supply chain	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 13 AHP-hierarchy in Expert Choice Comparison Suite

Using AHP, having combined identified assessment criteria and cyber intelligence acquisition methods into a hierarchy and applying different circumstantial attributes to the assessments, sets of circumstantially dependently prioritized methods are acquired. When comparing the sets of priorities, circumstantially converging and diverging shapes can be identified. This is illustrated in Figure 14 below:

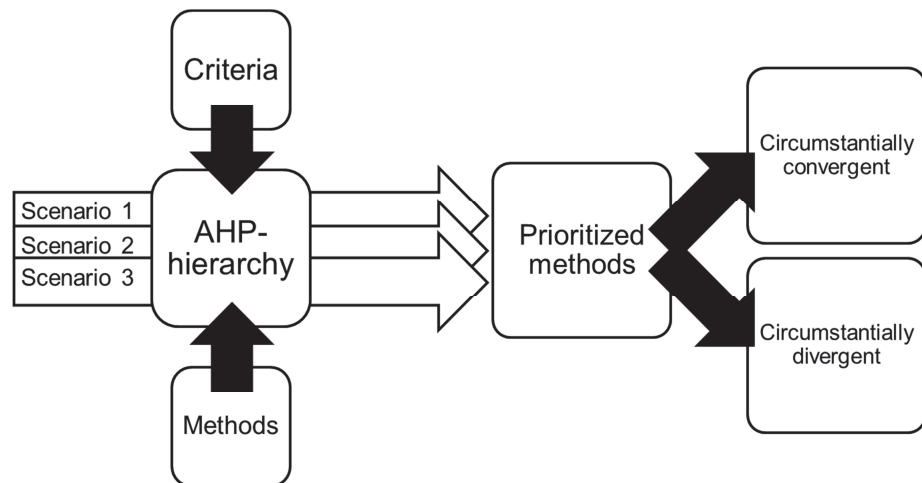


Figure 14 The Principle of Assessing Intelligence Methods Using an AHP Hierarchy

5.5 Composing the Survey Based on the AHP-model

The survey is composed with the following measurement method and evaluation options:

- For each scenario, a separate survey is carried out.
- Criteria and sub-criteria are prioritized by submitting direct priority input (0-100%).
- For each criterion, all sub-criteria are evaluated prioritized on the same screen.
- Alternatives are evaluated on an evenly distributed 20-step scale (0-100%), with the option of deeming an evaluation not applicable for evaluation against a certain criterion.
- For each criterion, all alternatives are evaluated on the same screen.

Cover letter for the survey is depicted in Annex 3, and a detailed implementation of the survey is depicted in Annex 4.

6 CIRCUMSTANTIAL APPLICABILITY OF CYBER INTELLIGENCE ACQUISITION METHODS

From the survey conducted based on the established model of intelligence acquisition methods in cyber domain, a number of conclusions can be deduced both about general applicability of different methods, as well as differences in their applicability for different purposes.

6.1 Overview of the Results

The survey produced three sets of data – one for each scenario. Raw data of completed surveys are presented in numeric form in Annex 5, and resulting priorities for each scenario are presented in Annex 6. The computed data is presented in unnormalized form to account for differences of scores between scenarios. Furthermore, Ideal Mode with Aggregating Individual Judgment (AIJ) -option is used.

For further analysis, resulting assessments of method priorities have been refined into radar charts. Figures 15 and 16 represent composite priorities of assessed methods with respect to all criteria. In Figures 17-19, priorities have been presented with respect to individual main assessment criteria. The radar chart is chosen because the data includes a great number of individual data classes (15 methods) with common axis dimensions (0–90%).

The resulting priorities of individual cyber intelligence acquisition methods represent their preferability – or applicability – in a set frame of reference: the higher the score is, the more favorable the method is. In the radar chart, convergence of a priority data set to a spherical plot would designate equal resulting priorities of each method. Principally, the overall and criteria-specific priorities of cyber intelligence acquisition methods are assessed to be along the same lines. For scenarios 1 and 2, assessed priorities differ only little, however scenario 3 tends to be assessed higher on many accounts. Figure 15 below shows the calculated arithmetically averaged priorities of the cyber intelligence acquisition methods.

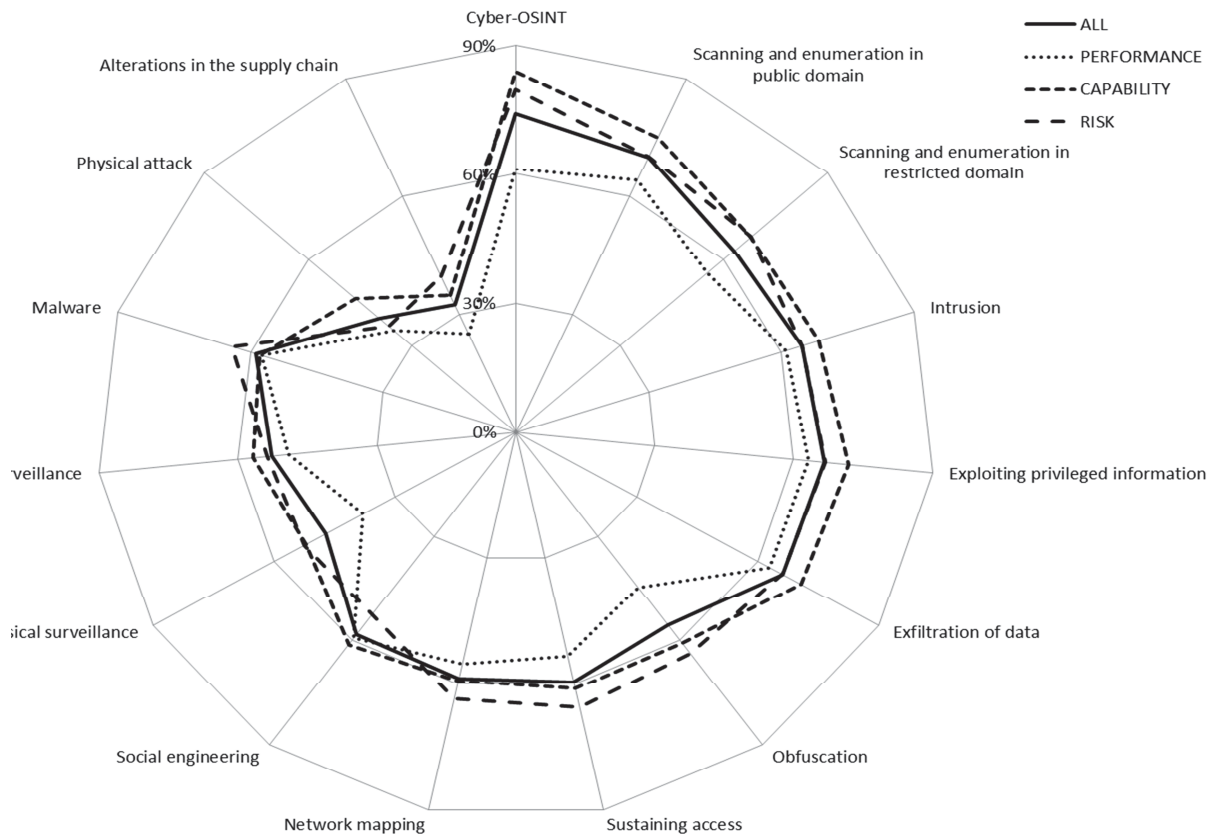


Figure 15 Arithmetic Averaged Priorities of Cyber Intelligence Acquisition Methods

6.2 Assessment on the Survey Results

The number of responses received to the survey was relatively low: out of 14 requests, 4 complete surveys were submitted. Additionally, 5 partial responses were submitted. These assessments were omitted in order to sustain balance in the data sets: dissonant partial assessments could distort the results of an individual survey, with greatest impact on the head part of the submitted assessments, and also create an imbalance between the data sets of the scenarios. For data sets of each scenario, standard deviations have been computed in order to assess the level of consensus between the participants. Computed mean, median, minimum and maximum standard deviations are presented in Tables 2–3 below.

Table 2 Standard Deviations of Participants' Assessments

		Scenario		
		1	2	3
Standard deviation of assessments on cyber intelligence acquisition methods	σ_{mean}	0.23	0.18	0.18
	σ_{med}	0.23	0.18	0.16
	σ_{min}	0.00	0.02	0.02
	σ_{max}	0.41	0.40	0.39

Table 3 Standard Deviations of Participants' Normalized Assessments to criteria weights

		Scenario		
		1	2	3
Standard deviations of normalized weights of criteria	σ_{mean}	0.06	0.08	0.08
	σ_{med}	0.05	0.06	0.06
	σ_{min}	0.02	0.02	0.02
	σ_{max}	0.16	0.20	0.20

Overall, the mean standard deviations for the bulk of the data – assessments of intelligence methods against individual criteria – is quite high, approximately 0.20, which is 20% of the assessment scale. Hence, the level of agreement between participants is limited, which is rather understandable considering that the individuals taking part in the survey represented a wide range of backgrounds and hence points of view. Considering that the number of participants is quite low, a single differing opinion may have a disproportionately prominent impact on the computed standard deviation. For scenarios 1 and 2, the mean and median standard deviations are substantially higher than for scenario 3, consequently suggesting a lower level of consensus. This could be caused by the greater level of perceived ambiguity of the first two scenarios, consequently resulting in individuals interpreting them and evaluating them differently.

One source of error is that the participants are likely to have experienced ambivalence and uncertainty regarding the survey format, especially when making their first assessments. Assuming that the assessments have been submitted in order, starting with scenario 1 and ending with scenario 3, the participants are likely to have become increasingly familiar with the survey format and have established a consistent attitude toward the assessments as the survey advanced. Consequently, scenario 1 is more likely to have inconsistency within data sets than the other two. AHP inconsistency ratio cannot be computed for data sets because pairwise comparison was not used.

When comparing resulting priorities of methods in different scenarios, one aspect to be considered is the normalization feature of the AHP: assessed weights of criteria and sub-criteria weights are normalized in order to conform the weights to a uniform scale where the sum of individual global weights is exactly 1 [8]. The weighting coefficients of the main criteria for the scenarios are presented in Table 5. A full account on the computed weights of criteria and sub-criteria can be found in Annex 6.

As a consequence of normalization, any intended implied difference between inputs submitted to different scenarios is reduced to a uniform scale. Consequently, the standard deviations of the participants' normalized criteria weight assessments (Table 3) are substantially lower than those of assessed values for methods. Specifically for the purposes of contrasting assessments on different scenarios as well as those submitted by different individuals, this trait is appropriate rather than adverse, because the purpose of assigning criteria priorities is to establish their significances compared to each other. Furthermore, such mapping conforms possibly divergent perceptions of the input scale used.

Furthermore, a sensitivity analysis (Table 4) was conducted on the data. Dynamic Sensitivity –functionality of Expert Choice Comparion was utilized, experimenting on the weight of each criterion individually. The upper and lower limits recorded indicate the priority values at which the rank order of the cyber intelligence acquisition methods altered. The sensitivity range was in the order of magnitude of ± 0.02 - 0.03 for Scenarios 1 and 3, and ± 0.06 for Scenario 2 denoting that even quite small changes in the criteria weight distribution affect the rank order of methods.

Table 4 Sensitivity Analysis of Criteria Weights

	Scenario 1			Scenario 2			Scenario 3		
Criterion	Lower limit	Weight	Upper limit	Lower limit	Weight	Upper limit	Lower limit	Weight	Upper limit
Performance	0.27	0.29	0.30	0.46	0.52	0.55	0.30	0.32	0.34
Capability	0.33	0.34	0.35	0.36	0.40	0.47	0.27	0.34	0.36
Risk	0.36	0.37	0.38	0.03	0.08	0.18	0.32	0.35	0.37

6.3 Analysis of Results Acquired from the Survey

6.3.1 Weights of Criteria

Table 5 below presents the criteria priorities composed from individual assessments. The values are presented in local form, meaning that the sum of priorities of each set of sub-criteria is 1.0. Depending on the scenario at hand, participants evaluated priorities of the criteria with some level of variation. The order of magnitude of priorities of the main evaluating criteria in scenarios 1 and 3 were assessed consistently as risk being most significant and performance the least, however the priorities were almost equally divided for both scenarios. For scenario 2, risk was assessed close to negligible, and performance considerably most significant with a share of over 50%.

Table 5 Local Weights of Evaluating Criteria

Criteria	SC1	SC2	SC3	AVERAGE
Performance	0.29	0.52	0.32	0.38
Speed	0.22	0.17	0.12	0.17
Efficiency	0.22	0.23	0.20	0.22
Resolution	0.16	0.15	0.15	0.15
Verifiability	0.13	0.14	0.14	0.14
Validity	0.10	0.16	0.21	0.16
Reliability	0.18	0.17	0.18	0.18
Capability	0.34	0.40	0.34	0.36
Technology	0.24	0.28	0.23	0.25
Expertise	0.24	0.28	0.22	0.25
Technical	0.60	0.57	0.49	0.55
Contextual	0.40	0.43	0.51	0.45
Resources	0.18	0.16	0.21	0.18
Leadership	0.20	0.18	0.21	0.20
Support from other INTEL	0.13	0.10	0.14	0.12
Risk	0.37	0.08	0.35	0.27
Jurisdiction	0.19	0.16	0.25	0.20
Exposure of operative	0.30	0.30	0.26	0.29
Exposure of method	0.26	0.26	0.26	0.26
Exposure of target	0.25	0.28	0.23	0.25

Out of the sub-criteria for performance, efficiency was assessed to be of highest priority for scenarios 1 and 2 and second highest for scenario 3, whereas speed was assessed equally significant to efficiency in scenario 1 and validity most significant in scenario 3 by a small margin. For all scenarios, verifiability was assessed least significant. Valuing efficiency of the method high suggests that it is one of the benefits sought from utilizing cyber intelligence.

For capability, technology and expertise were assessed most significant, while support from other INTEL was deemed least significant. Technical expertise was assessed more important in scenarios 1 and 2, whereas in scenario 3 their shares were virtually equal. Evaluating technology and technological expertise high suggests that technological sophistication and skill is a key element in conducting cyber intelligence activities.

For risk, exposure of operative was deemed most and jurisdiction least significant for scenarios 1 and 2, whereas for scenario 3, allocation was almost shared alike, with exposure of operative and method having slightly higher priority. The evaluated priorities suggest that avoiding attribution is deemed of high value when conducting intelligence in cyber domain, whereas legal considerations are considered of lesser importance.

6.3.2 Overall Priorities

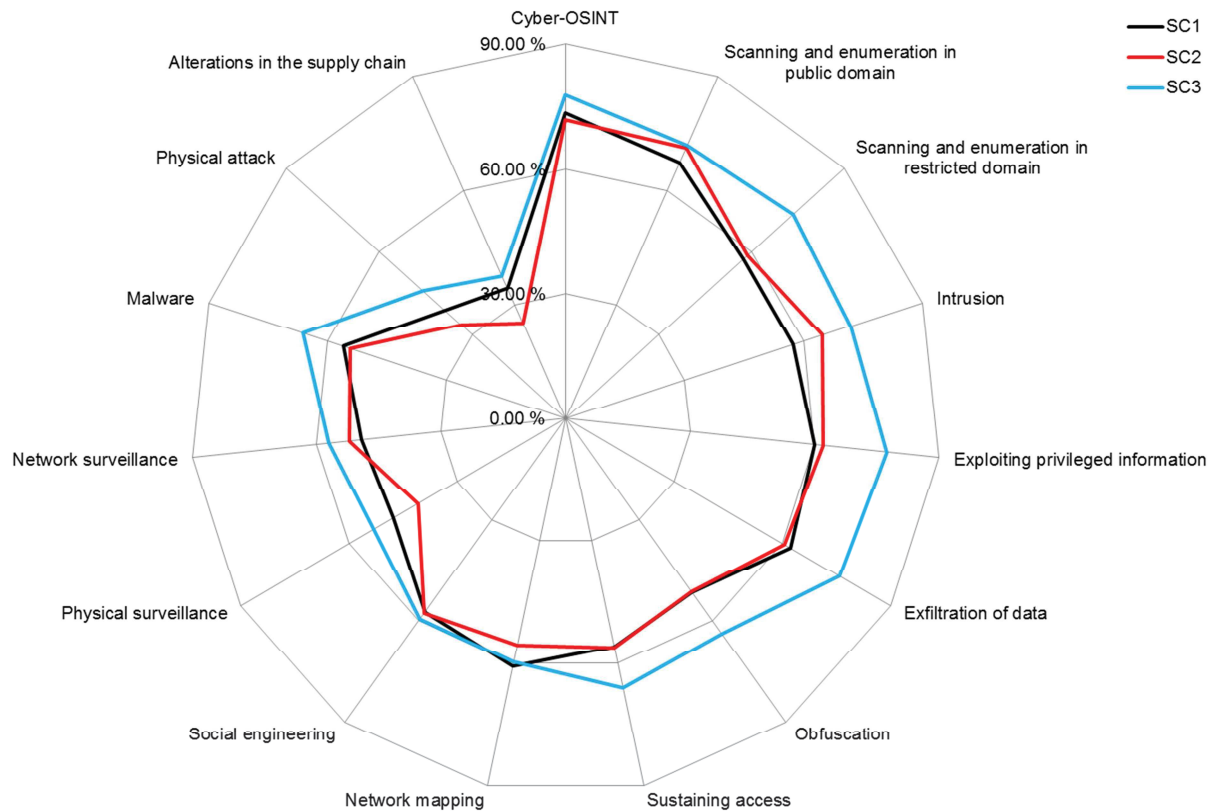


Figure 16 Priorities of the Intelligence Methods With Respect to All Assessment Criteria

As depicted in Figure 16 above, in general the priorities of the intelligence methods are assessed substantially higher with respect to scenario 3 than the others. Out of 15 methods assessed, the values for scenario 3 amount to over 70% for six methods, 60-70% for three and 50-60% for four, whereas for scenario 1 the amounts are one, three and four and for scenario 2 two, three and seven respectively. For all scenarios, cyber-OSINT is assessed the most and physical attack and alterations in the supply chain are assessed the least preferable. The preferability assessments on cyber-OSINT, social engineering and network mapping are deemed close to same for all scenarios.

The overall priority assessment suggests that for sophisticated cyber intelligence operative most intelligence methods are applicable to a higher extent than for operatives with lesser means. Activities requiring physical access such as altering products en route or accessing systems on-site are deemed less preferable, which would indicate a general tendency of preferring operating remotely.

6.3.3 Performance

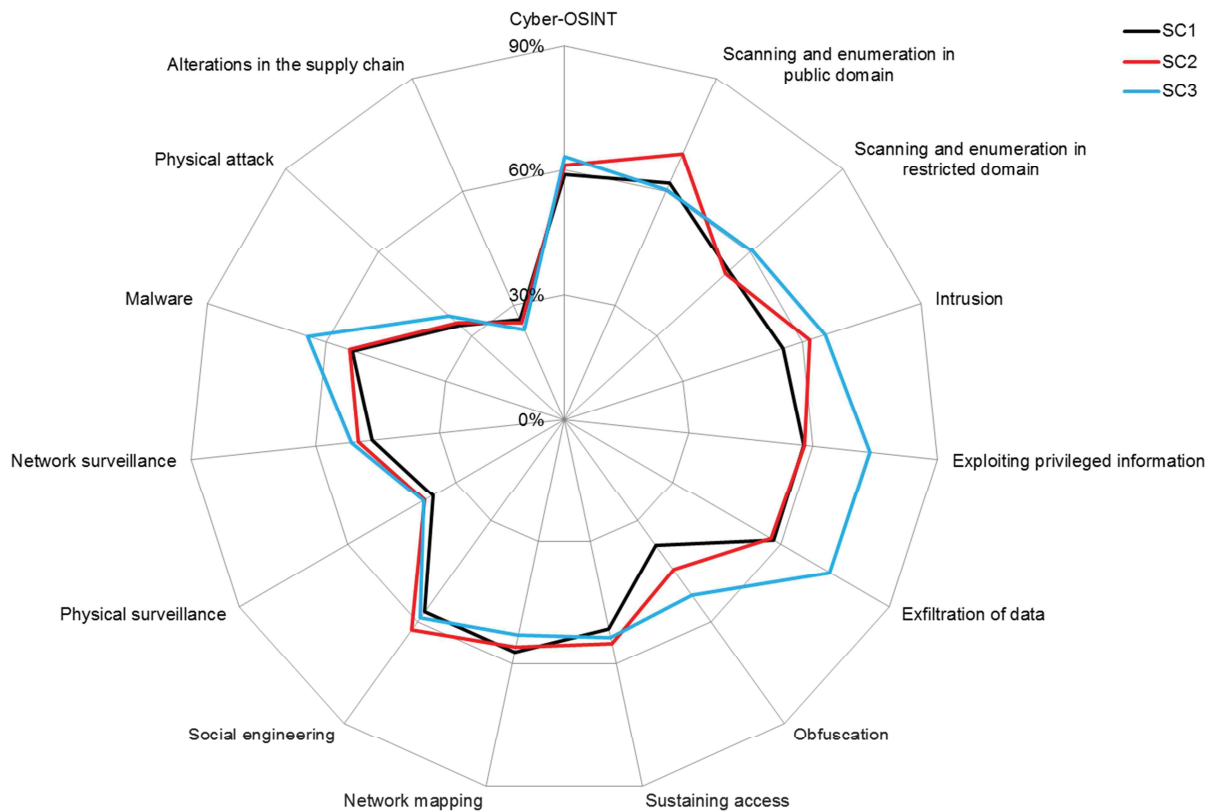


Figure 17 Priorities of the Intelligence Methods With Respect to Performance

Priorities of methods with respect to performance, as depicted in Figure 17 above, indicate a close resemblance between scenarios 1 and 2, whereas on the account of scenario 3 a number of methods stand out. For scenario 3, intrusion, exploiting privileged information, exfiltration of data, obfuscation and malware are assessed of substantially higher priority than for the other scenarios. Overall, physical attack, alterations in the supply chain and physical surveillance are assessed least preferable in terms of performance. For scenario 2, scanning and enumeration in public domain is assessed relatively more preferable, and the preferability is assessed equal for all scenarios for over 50% of the methods.

The fact that most methods have been assessed equally preferable in terms of performance suggests that the relative effectivity of many intelligence acquirement methods is to a high extend independent of circumstances. On the account of methods with variation in assessed preferability it can be suggested that the performance of the method could be more circumstantially dependent, hence being varyingly applicable to different situations.

6.3.4 Capability

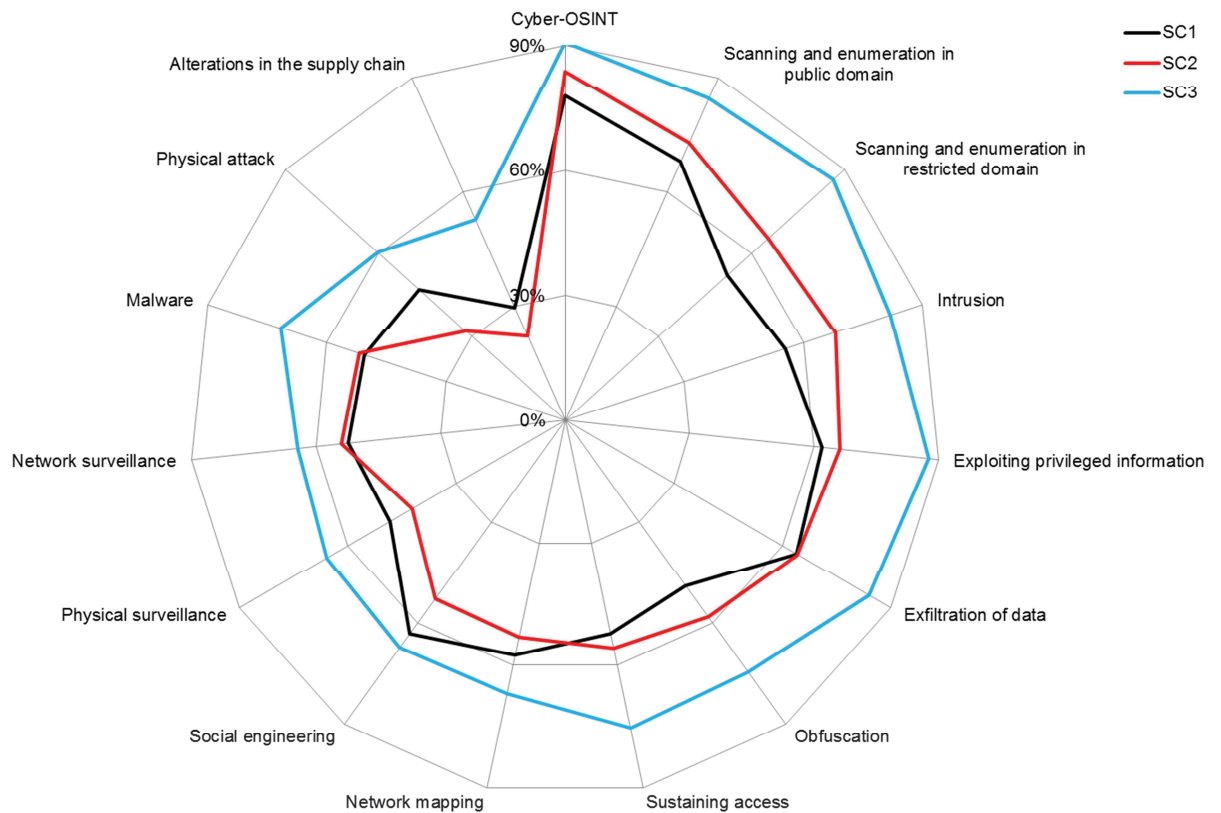


Figure 18 Priorities of the Intelligence Methods With Respect to Capability

As depicted in Figure 18 above, the most prominent differences between the intelligence acquisition methods arise when compared with respect to capability of operative. Overall, in context of scenario 3 the methods are prominently more preferable, none having been assessed below 50%. When considering the two other scenarios, preferability of malware, network surveillance and exfiltration of data are assessed equal, whereas physical attack, alterations in the supply chain and social engineering are assessed most prominently more preferable in the context of scenario 1, and scanning and enumeration in both domains as well as intrusion in the context of scenario 2.

Unsurprisingly, the applicability of the intelligence acquisition methods are evaluated highest from nations-state operative's perspective, which reflects the fact that superior means translate into higher capability to apply various methods. Considering the other two scenarios, the methods most prominently in favor of scenario 1 indicate correlation between the capability and physical proximity, whereas those in favor of scenario 2 would suggest more prominent assessed praxis in core hacking activities.

6.3.5 Risk

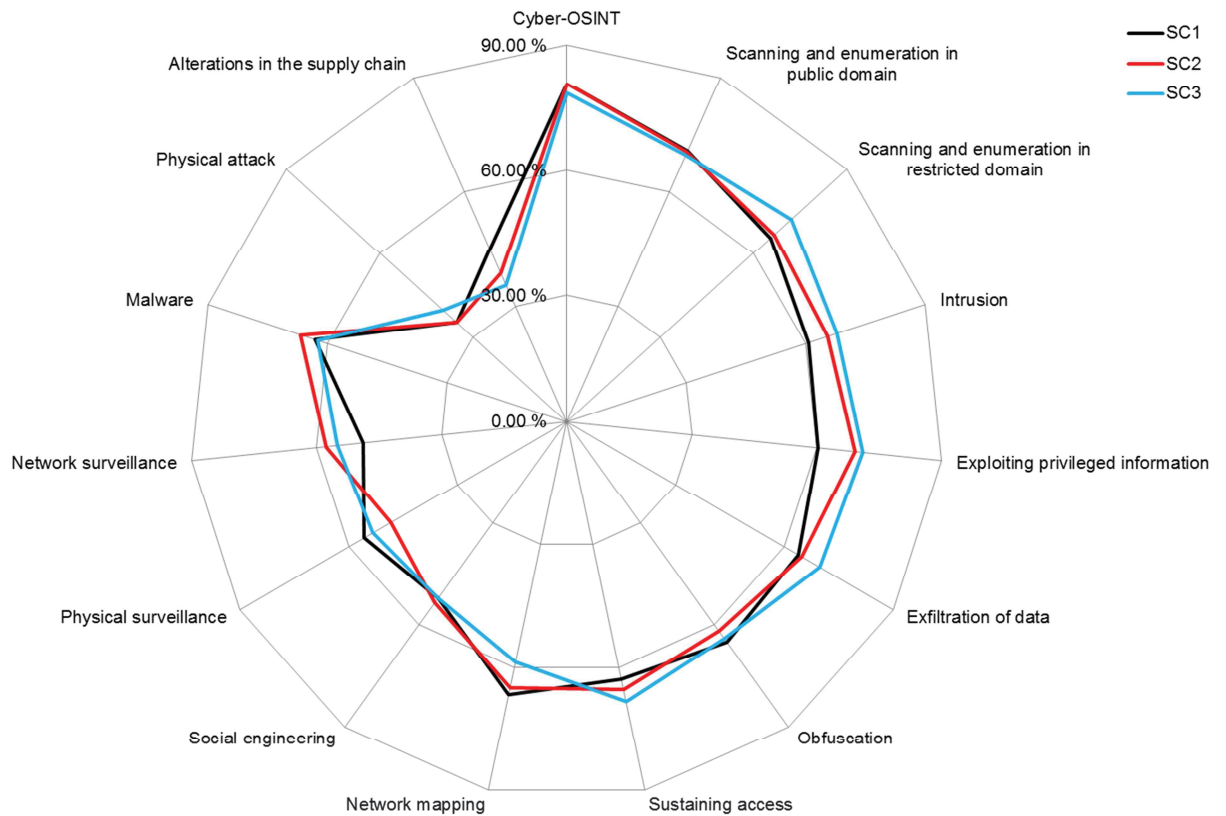


Figure 19 Priorities of the Intelligence Methods With Respect to Risk

As depicted in Figure 19, assessed priorities of most cyber intelligence acquisition methods are very close to equal for all the scenarios when perceived from risk perspective, unlike the other evaluating criteria. The most preferable – and hence least risky – methods are assessed to be cyber-OSINT and scanning and enumeration in both domains, whereas the least preferable are assessed to be physical attack and alterations in the supply chain.

The data quite prominently suggests that perceived risks involved in conducting cyber intelligence activities are rather associated with the attributes and qualities of the methods utilized rather than the circumstances of by and upon whom the activity is conducted. The assessed level of risk quite distinctly increases in proportion to the level of insolence and invasiveness of the method, subtle and non-invasive methods like cyber-OSINT and scanning and enumeration being least risky, whereas methods requiring physical access to the target system being considered most risky.

7 CONCLUSIONS, DISCUSSION AND SUGGESTIONS

Overall, making effective use of the cyber domain creates substantial potential in the current world where all aspects of life are increasingly networked and digitized [64; 116]. This stands also for intelligence in cyber domain. Due to the migration of information into digital form and networked environments [102], it even can be argued that forgoing its possibilities could prove substantially limiting [64]. Furthermore, segregating related activities in the physical and cyber domains should be refrained from, because in many respects the cyber domain can provide new perspectives to phenomena in the physical, whereas the physical domain provides concrete context to phenomena in the cyber domain.

It can be concluded that Intelligence in cyber domain is an endorsing, cross-cutting intelligence discipline that adds value to all aspects of conventional intelligence and furthermore that it bears a substantial amount of characteristic traits – both advantageous and disadvantageous – and furthermore that the applicability of cyber intelligence methods is only partly circumstantially limited.

7.1 Overview of the Research Process

The main objective of the study was to assess, to what extent the applicability of cyber intelligence acquisition methods is circumstantial. In order to reach a conclusion, the very concept of intelligence in cyber domain, its defining attributes, methods, factors dictating its applicability, and range of operatives were to be addressed. For analysis, means to assess the applicability of cyber intelligence acquisition methods were required.

The study was conducted in sequential a manner, starting with defining the concept of intelligence in cyber domain and identifying its key attributes, followed by identifying the range of intelligence methods in cyber domain, criteria influencing their applicability, and types of operatives utilizing cyber intelligence. The methods and criteria were refined into a hierarchical model, to which was also incorporated the element of circumstantial context in order to facilitate analysis on how different circumstances affect the applicability of cyber intelligence acquisition methods.

In order to obtain a comprehensive understanding of the topic and facilitate analysis from multiple angles, a spectrum of sources was used. The existing conceptions of cyber intelligence were mapped through an extensive literature study on a wide variety of sources. The established understanding was further developed through 15 semi-structured interviews with experts of different backgrounds, whose wide range of points of view proved to substantially enhance the perspective on the subject. Furthermore, four of the interviewed experts participated in a relatively extensive survey based on the constructed hierarchical model on cyber intelligence that was formulated in to an AHP hierarchy and executed in the Expert Choice Comparison online application. Through the survey, the qualitative empirical findings were enhanced by quantifying expert perceptions and thus pointing out further distinctive traits of cyber intelligence.

7.2 Summary of Results

Intelligence, in essence, can be characterized as collection of information in a manner that violates confidentiality. This trait, however, does not imply legal or moral infringement, albeit such can take place if intelligence is collected in a belligerent manner. Instead, information is collected and processed in order to deduce in-depth understanding of the subject at hand. For many, the term ‘intelligence’ is exclusively reserved for with collection of information for the purposes of national interest, conducted by the military or designated agencies. However, if one dismisses this premise and perceives intelligence in a more general context, it can be concluded that it is a cognitive process of focused and purpose-oriented gathering of information that comprises the iterative elements of direction, collection, processing and dissemination. Furthermore, in the context of human decision-making process, intelligence can be concluded to be quite analogous to the situation awareness process in general.

Intelligence in cyber domain, on its behalf, bears a multitude of implications, depending on standpoint and context. In addition to the obvious military implication, another common association is that of security: cyber threat intelligence focuses on analyzing the vulnerability to threats present in the cyber domain. However, in a general frame of reference, cyber intelligence connotes quite a variety of methods facilitating acquisition of exploitable information. As can be derived from military context, cyber intelligence incorporates a substantial intrusive element that in essence does not differ from offensive in cyber domain otherwise than how it relates to the contents of target systems: cyber offensive strikes the integrity and availability of information and systems, cyber intelligence only alters systems in

order to gain more access or avert detection. Moreover, although cyber intelligence acquisition methods in many cases incorporate methods that provide unauthorized access to information, there is also a substantial public-domain element to it.

From the perspective of applicability of intelligence acquisition methods in cyber domain, the setting can be modeled in a hierarchical manner:

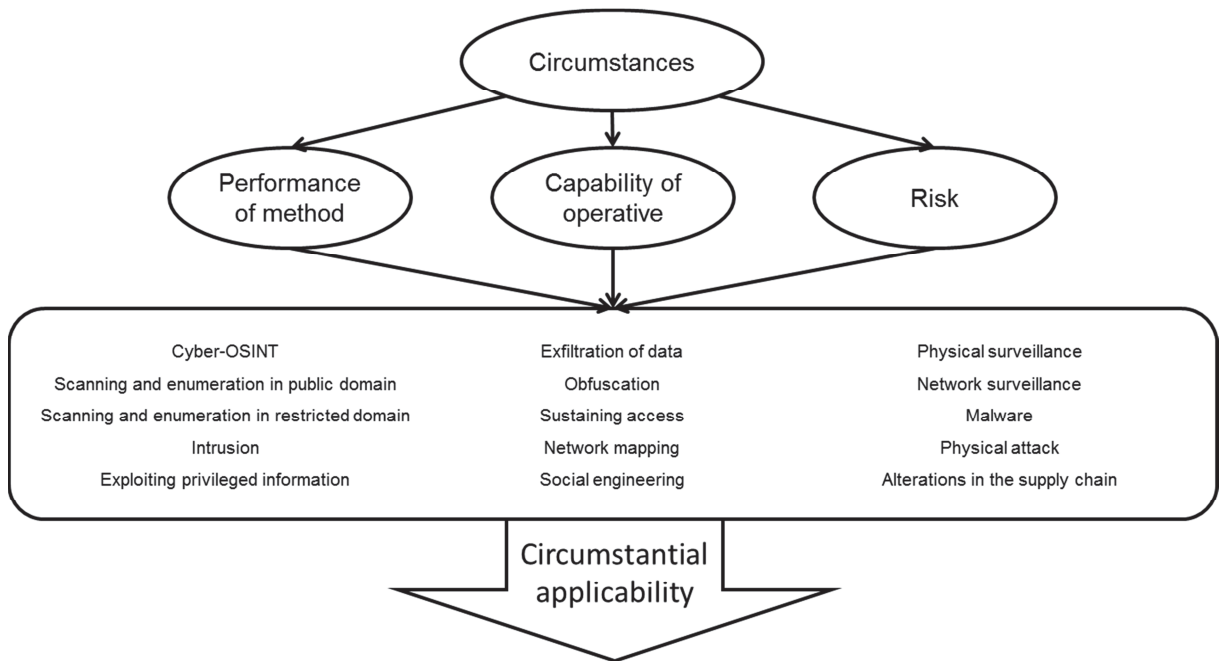


Figure 20 Hierarchical Model for Evaluating Circumstantial Applicability of Cyber Intelligence Methods

As outlined in Figure 20 above, the assessment of applicability of cyber intelligence acquisition methods can be broken down to three criteria: performance of the method, capability of the operative and risk. The criteria comprise sub-criteria. The setting is approached with respect to set circumstances of assessment – operative, target and environment – which are reflected in weights of the criteria and assessments of the methods with respect to criteria. The outcome of the assessment is a scored ranking of the intelligence methods that represents the circumstantial applicability of the different methods of cyber intelligence acquisition.

The hierarchical model was applied to scenarios derived from widely accepted categorization of most prominent cyber intelligence operatives: nation state actors, criminals and idealistic. Overall, analysis based on the hierarchical model indicated that the circumstantially most applicable methods entail low level of invasiveness and allow for any desirable distance to target, whereas the least applicable methods required physical access to target. The fact that evading detection and especially attribution is a substantial defining inhibition in cyber domain endorses the indicated conclusion. Furthermore, operating from safe distance and favorable jurisdiction are considered advantages of cyber intelligence and possible traces left a disadvantage, which advocates the assessment that concrete actions in the physical domain are deemed inferior in terms of applicability.

On another account, the hierarchical model appears to provide insight into comparing and assessing cyber intelligence operatives. Firstly, the overall priorities appear to reflect the differences in level of utilization of cyber intelligence methods. From performance perspective, the scores yielded primarily reflect the methods' qualities with respect to the target rather than operative. However, the assessment is subjective from the operative's perspective, and hence the assessments reflect also how performance of the methods varies with perspective. Capability, on the other hand, reflects most the capacity and sophistication of the operative, showing substantial differences especially in favor of a nation-state operative. Moreover, more subtle differences in assessed risk reflects the conception that to a high extent the level of risk different operatives face differs only a little, and is rather dependent on the method utilized.

Lastly, based on the study, it can be concluded that the applicability of intelligence acquisition methods in cyber domain is to a high extent circumstantial, depending on attributes of the operative and target in question as well as the setting in question. Overall, applicability of cyber intelligence acquisition methods can be assessed to be inversely proportional to the extent of invasiveness of the method. In other words, stealthy methods with negligible chance of attribution are deemed most applicable, whereas methods requiring physical access to target are deemed least applicable. This applies, however, predominantly to the relative applicability of methods in a given setting, whereas the applicability varies with circumstances, especially with respect to capability of the operative.

7.3 Validity and Reliability

The perspective of the study was quite ample. A broad angle of view was chosen at the expense of the level of detail because of scarcity of existing public research that would focus on the intelligence aspect of activity in cyber domain, which in turn shows from the modest consensus on the concept. Moreover, also the chosen security classification level of the work dictated that concepts needed to be addressed on a general rather than detailed level, because when examined in detail, aspects of intelligence easily turn out to be classified. Addressing the topic on a general and conceptual level results in possible limitations to validity and reliability of the study.

Reliability of research denotes the extent to which the research yields consistent findings [127, p. 680]. One illustrating indicator of the consistency of data available on the subject is the substantial dispersion of opinions indicated in the conducted AHP survey – the mean standard deviation of submitted assessments was approximately 20%. The number, together with the fact that the number of data sets was a humble four, indicates limitations in the reliability of the qualitative data in the research, possibly originating from participants' differing subjective conceptions of the scenarios and assessment scales. However, the multiple sub-criteria to each evaluating criteria in the hierarchical model accumulated to a score averaged and weighted according to the AHP principle, which contributes to diminishing fluctuations in the data. However, the standard deviation can be argued to indicate more generally the level of consensus among experts on the subject. Moreover, variation in perceptions was evident in both literary sources and interviews. On a general and conceptual level such as in this study, the topic is highly subject to personal opinion. Partly, the veil of secrecy around intelligence can be indicted for this: detailed public information is scarce. Partly, however, the likely reason is the abstract nature of cyber phenomena, which in many respects is difficult or impossible to measure and quantify. The topic was addressed broadly both quantitatively in terms of the crude hierarchical model as well as qualitatively, and hence it is sensible that opinions from different standpoints show differences.

Validity of research in turn denotes the extent to which the research accurately measures the subject studied [127, p. 684]. Albeit the chosen level of detail translates into possible limitations in the reliability of the research, the wide selection of research methods and sources contribute to increasing its validity. The conclusions drawn were based on a range of literary sources, a relatively encompassing selection of interviewees and an extensive AHP-

survey. The evidence appears to converge, and the constructed hierarchical model appears to reflect the qualitative results yielded in the research. The general nature of the research, however, causes also potential limitations to the validity of the conclusions drawn. Firstly, the literary base was limited to non-classified sources. Even though little public research on cyber intelligence exists, it is likely rather than improbable that classified studies have been conducted, because developing cyber capabilities is an acute trend on national level in many countries. Hence, basing research on literature that possibly provides a mere peek to the subject might result in misconceptions and drawing conclusions that are fundamentally off. Furthermore, the same appears to apply to interviewees: on many accounts it was evident that conducting interviews for a thesis that is going to be publicly available substantially limited the depth and detail of information disclosed. In turn, lack of detail might result in misinterpreting the statements given. Moreover, the hierarchical model was based on the aforementioned sources, which might be reflected in shaping the model unrealistically. The assessments submitted to the survey in turn might be off due to participants misinterpreting the intended point of view or scales of the survey. With respect to validity, the most probable source of limitations is the constrained knowledge base the argument is based upon, but in turn the wide variety of sources counters the limitations of individual sources.

7.4 Discussion

Although it could superficially be argued that intelligence collection in cyber domain is a discipline of immense potential, approach to the topic should be kept in sensible perspective. To begin with, acquisition of intelligence in cyber domain should not be mistaken as being associated only symmetrically to cyber purposes, i.e. facilitating other activities in the same domain. Neither the infrastructure of and nor the information in the cyber domain exist for their own sake, but serve a physical domain purpose [90], and hence also intelligence collected in the cyber domain serve purposes of physical domain actors – persons, organizations, nations... From this standpoint, it is only logical to conclude that information in the two domains is affiliated rather than distinct, and the issue addressed should be about in what way (and form) the intelligence is acquired most suitably in the given circumstances and based on what the intelligence can be verified. Moreover, when considering the discovery that cyber intelligence is a discipline that cross-cuttingly extends and enhances the reach and potential of all conventional intelligence disciplines (Figure 11), the baseline and background information from conventional intelligence acquisition methods can be concluded to provide

cyber intelligence perspective and context that are often more ambiguous when exclusively in the digital environment.

Cyber intelligence is widely demonized and condemned in public discourse [96], most prominently for the implications to personal privacy. However, the hype around the topic can be counter-productive in terms of dismissing the bigger picture [64]. Namely for the purposes of putting phenomena into perspective and understanding the gestalt of cyber intelligence, it is meaningful to examine it in a neutral context and broad perspective. Hence, given that existing research addressing specifically cyber intelligence as a whole is scarce, the chosen approach to this study is justified, notwithstanding the limitations to validity and reliability. It is only through public research that the understanding of concepts and phenomena evolves in the academic framework, and from there the established conceptions further provide perspective to public discourse. Moreover, if examined in the framework of academic research, an analogy is quite easily drawn between the approaches of intelligence and academic research: in both concepts, information is collected, analyzed and utilized in a purpose-oriented manner. Given that information increasingly inhabits namely the cyber environment, it can be argued that the distinction is merely semantic and based on the motivation of collection.

7.5 Future Work

The results of the study yield a great number of potential future work, both in terms of further developing the research conducted as well as independent areas of study. As concluded, the validity and reliability of research conducted and conclusions drawn were substantially limited by the assumed broad scope of study and chosen public base of information. Building upon the general conceptions outlined in this study, the perception of both the entity and narrower aspects of cyber intelligence can be further developed. Conducting a similar research based on more sensitive data is a quite obvious possible way of refining the findings of this study, but further developing the methodological solutions is another potent option.

The hierarchical model formulated as well as how it was applied to the research has multiple prospective aspects to be improved. To begin with, the subject of whether the elements of the model – criteria as well as intelligence methods – represent the concept and its dependencies in the best possible manner. One aspect that would especially improve the focus of the model is defining more detailed scenarios. For example, the model could be utilized in a case-based

study of online threats. Considering collecting data using the model, more specific assessment scales could be useful. Even defining more concrete and unambiguous scales individually for each criterion could prove valuable, because differences in subjective understanding of the scale was an obvious source of imprecision. Furthermore, making assessments as a group of experts instead of submitting individual assessments could help finding a consensus as well as understanding the assessment scales alike, thus reducing deviation in the assessments. Furthermore, the assessments could be conducted in an iterative manner, for example first establishing consensus about the weights of the criteria and separately assessing the alternatives using priorities defined earlier.

When addressing a concept as controversial as cyber intelligence, interviews conducted could benefit from increased concreteness, for example selecting a real-life case as the theme of interviews. A less conceptual and more technically oriented approach could also prove valuable. Another approach could be utilizing the Delphi method [127, p. 38] to iterate the expert opinions, however in such case the amount of interviewees needs perhaps to be smaller.

Moreover, from personal security perspective – or operational security in military framework – a study of how a person's adoption and active use of social media contributes to vulnerability to physical threats, for example being targeted by terrorists or other criminals. There are indications of social media having been utilized by ISIS to target Israeli government personnel [141]. Furthermore, terrorist use of cyber methods is recognized as a growing threat [81].

BIBLIOGRAPHY

- [1] *2014: A Year of Mega Breaches* [research report]. Ponemon Institute LLC. January 2015 [cited 26.2.2015]. Available: <http://tinyurl.com/ljlvfqh>.
- [2] *ADRP 2-0 Intelligence*. Washington: Department of the Army Headquarters, 2012. [cited 3.1.2014]. Available: <http://tinyurl.com/pk9ynmd>.
- [3] *Advanced Persistent Threats and Other Advanced Attacks: Threat Analysis and Defense Strategies for SMB, Mid-Size, and Enterprise Organizations* [white paper]. Websense. [cited 9.4.2015]. Available: <http://tinyurl.com/p276jz4>.
- [4] *Advanced Persistent Threats: Higher Education Security Risks* [white paper]. Dell SecureWorks. [cited 9.4.2015]. Available: <http://tinyurl.com/om2nk2h>.
- [5] *Alert (TA14-329A) Regin Malware* [web page]. US-CERT. 25.11.2014 [cited 9.4.2015]. Available: <http://tinyurl.com/q6usysf>.
- [6] *Anssi Kärkkäinen* [profile]. LinkedIn. [cited 15.4.2015]. Available: <http://tinyurl.com/mozgjud>.
- [7] *Catharina Candolin* [profile]. LinkedIn. [cited 15.4.2015]. Available: <http://tinyurl.com/pyqcbs7>.
- [8] *Comparion Help Document*. Expert Choice, 2015.
- [9] *Cyber Intelligence Centre* [web page]. [cited 30.3.2015]. Available: <http://tinyurl.com/p4xa2qe>.
- [10] *Document Metadata Can Reveal Secrets* [web page]. iOSINT. 15.4.2010 [cited 1.2.2015]. Available: <http://tinyurl.com/q2ep3ml>.
- [11] *Dr Rain Ottis* [web page]. CCD COE. [cited 2.2.2015]. Available: <http://tinyurl.com/nkyqe9k>.

[12] *Duqu infection linked to Microsoft Word exploit* [electronic article]. BBC. 2.11.2011 [cited 3.3.2015]. Available: <http://tinyurl.com/ndtyzuv>.

[13] *Equation Group: Questions and Answers* [report]. Kaspersky. February 2015 [cited 9.4.2015]. Available: <http://tinyurl.com/py2r4ac>.

[14] *Establishing a Formal Cyber Intelligence Capability* [white paper]. VeriSign. [cited 30.3.2015]. Available: <http://tinyurl.com/d6q83qe>.

[15] *Finland's Cyber Security Strategy* [online publication]. Helsinki: Secretariat of the Security Committee, 2013. 40 pages. ISBN 978-951-25-2438-9. [cited 25.3.2015]. Available: <http://tinyurl.com/qhab8ew>.

[16] *First Virus* [web page]. Affordable Computer Security Service. [cited 1.2.2015]. Available: <http://tinyurl.com/pmmd7k4>.

[17] *FM 2-0 Intelligence*. Washington, DC: Department of the Army Headquarters, 2004. [cited 25.8.2014]. Available: <http://tinyurl.com/qb3llsw>.

[18] *FM 2-0 Intelligence*. Washington, DC: Department of the Army Headquarters, 2010. [cited 14.4.2015]. Available: <http://tinyurl.com/ok9l9s2>.

[19] *Hacker* [web page]. Merriam Webster. [cited 1.2.2015]. Available: <http://tinyurl.com/5lylgn>.

[20] *Hacker* [web page]. Webopedia. [cited 1.2.2015]. Available: <http://tinyurl.com/argwz>.

[21] *Hacking History: A Timeline of Hack Tactics* [blog posting]. SSLs.com. 23.4.2014 [cited 31.1.2015]. Available: <http://tinyurl.com/px23vyj>.

[22] *Harry Kantola* [profile]. LinkedIn. [cited 15.4.2015]. Available: <http://tinyurl.com/lprxwa>.

[23] *History of Hacking* [blog posting]. Ethical Hacking. 29.11.2009 [cited 1.2.2015]. Available: <http://tinyurl.com/nnld29m>.

[24] *The History of Malware* [web page]. Radware. [cited 1.2.2015].
Available: <http://tinyurl.com/pc48anv>.

[25] *History of Spyware* [web page]. TuneupAdvisor. [cited 9.4.2015].
Available: <http://tinyurl.com/luxzcja>.

[26] *The History of Spyware* [web page]. Lavasoft. [cited 1.2.2012].
Available: <http://tinyurl.com/mugqppu>.

[27] *History of the Web* [web page]. World Wide Web Foundation.
[cited 31.1.2015]. Available: <http://tinyurl.com/npmj85s>.

[28] *How Dangerous is Image File Metadata?* [web page]. The Assurer.
[cited 1.2.2015]. Available: <http://tinyurl.com/25me4f3>.

[29] *Intelligence Cycle* [web page]. FBI. [cited 29.12.2014].
Available: <http://tinyurl.com/pwnjsyh>.

[30] *INTelligence: Human Intelligence* [web page]. CIA.
21.10.2010, updated 30.4.2013 [cited 1.3.2015]. Available: <http://tinyurl.com/ld5rpuj>.

[31] *INTelligence: Open Source Intelligence* [web page]. CIA.
23.7.2010, updated 30.4.2013 [cited 27.2.2015]. Available: <http://tinyurl.com/367oxrf>.

[32] *The Internet Relay Chat by Jarkko Oikarinen* [web page]. Eyerys.
[cited 1.2.2015]. Available: <http://tinyurl.com/pptk8hl>.

[33] *Jarno Limnéll* [profile]. LinkedIn. [cited 15.4.2015].
Available: <http://tinyurl.com/oqobcdw>.

[34] *Jos eroat kirkosta, salaiset tietosi voivat vuotaa* [electronic article]. Iltalehti. 30.11.2008
[cited 14.4.2015]. Available: <http://tinyurl.com/obajodc>.

[35] *Kauto Huopio* [profile]. LinkedIn. [cited 15.4.2015].
Available: <http://tinyurl.com/qdt4y7y>.

[36] *Malware* [web page]. The Tech Terms Computer Dictionary. [cited 28.1.2015].
Available: <http://tinyurl.com/pry2fya>.

[37] *Martti J Kari* [profile]. LinkedIn. [cited 15.4.2015].
Available: <http://tinyurl.com/kwxrdlt>.

[38] *Mikko Hypponen* [web page]. F-Secure. [cited 15.4.2015].
Available: <http://tinyurl.com/q9m6dod>.

[39] *Mikko Niemelä* [profile]. LinkedIn. [cited 15.4.2015].
Available: <http://tinyurl.com/qz9q57j>.

[40] *New Virus Spotted on Android Phones Can Steal Personal Data* [electronic article].
Tech2. 9.12.2014 [cited 1.3.2015]. Available: <http://tinyurl.com/nlozct7>.

[41] *Operational Levels of Cyber Intelligence* [white paper].
Intelligence and National Security Alliance Cyber Intelligence Task Force.
September 2013 [cited 1.3.2015]. Available: <http://tinyurl.com/lxa9qum>.

[42] *"Red October" Diplomatic Cyber Attacks Investigation* [web page]. Kaspersky Lab.
14.1.2013 [cited 18.1.2013]. Available: <http://tinyurl.com/qd67uvx>.

[43] *Riku Kalinen* [web page]. Global Information Assurance Certification.
[cited 16.4.2015]. Available: <http://tinyurl.com/on2ue4g>.

[44] SFS-ISO/IEC 27000 Information Technology - Security Techniques - Information
Security Management Systems - Overview and Vocabulary.
Helsinki: Finnish Standards Association SFS, 2010. 19 pages.

[45] SFS-ISO/IEC 27005 Information Technology. Security Techniques. Information Security
Risk Management. Helsinki: Finnish Standards Association SFS, 2013. 126 pages.

[46] *A Short History of Hacking and Case Studies of Cracked Windows Servers*
[GIAC paper]. SANS Institute. 2013 [cited 26.2.2015].
Available: <http://tinyurl.com/nm42xap>.

[47] *Smartphone Users Worldwide Will Total 1.75 Billion in 2014* [web page]. eMarketer. 16.1.2014 [cited 1.3.2015]. Available: <http://tinyurl.com/qcjkj8>.

[48] *Tero Palokangas* [profile]. LinkedIn. [cited 15.4.2015]. Available: <http://tinyurl.com/l6474hj>.

[49] *Threats on the Horizon: The Rise of the Advanced Persistent Threat* [report]. Fortinet. [cited 9.4.2015]. Available: <http://tinyurl.com/qedoo72>.

[50] *Timo Kiravuo* [profile]. LinkedIn. [cited 15.4.2015]. Available: <http://tinyurl.com/mbxlmjf>.

[51] *Topi Tuukkanen* [profile]. LinkedIn. [cited 15.4.2015]. Available: <http://tinyurl.com/mhatrar>.

[52] *VeriSign Network Analysis Service Combats Revenue Leakage, Helps Carriers Maximize Infrastructure Investments* [electronic article]. PR Newswire. 3.6.2013 [accessed 1.3.2015]. Available: <http://tinyurl.com/mfecz5x>.

[53] *Who Built The First Modern Computer?* [web page]. CS4FN. [cited 31.1.2015]. Available: <http://tinyurl.com/odgt5j7>.

[54] *Words with Multiple Meanings* [web page]. YourDictionary. [cited 14.4.2015]. Available: <http://tinyurl.com/lgplhjv>.

[55] Andress, J. & Winterfield, S. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd ed. Waltham: Elsevier Inc., 2014. 306 pages. ISBN 978-0-12-416672-1.

[56] Anonymous. *Hakkerin käsikirja*. Helsinki: IT Press, 2002. 920 pages. ISBN 951-826-224-1.

[57] Bencsáth, B., Pék, G., Buttyán, L. & Félegyházi, M. *Duqu: A Stuxnet-like Malware Found in the Wild* [report]. Budapest University of Technology and Economics, Laboratory of Cryptography and System Security. 14.10.2011 [cited 4.4.2015]. Available: <http://tinyurl.com/7jzekx4>.

[58] Bimfort, M. T. *A Definition of Intelligence* [web page]. CIA. 18.9.1995, posted 8.5.2007, updated 3.8.2011 [cited 12.1.2015]. Available: <http://tinyurl.com/pgcbx3b>.

[59] Borg, S. *Securing the Supply Chain for Electronic Equipment: A Strategy and Framework* [online publication]. [cited 2.3.2015]. Available: <http://tinyurl.com/pmdulmh>.

[60] Brantly, A. *Defining the role of Intelligence in Cyber: a Hybrid Push and Pull*. In: Phythian, M. (Ed.). *Understanding the Intelligence Cycle*. London: Routledge, 2013. Pp. 76–98. ISBN 978-0-415-81175-0.

[61] Brehmer, B. *The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control* [electronic article]. In: 10th International Command and Control Research and Technology Symposium: The Future of C2. Swedish National Defence College Department of War Studies. [cited 20.1.2015]. Available: <http://tinyurl.com/23ey8ca>.

[62] Breithaupt, J. & Merkow, M. S. *Information Security Principles of Success* [web page]. Pearson Education, Pearson IT Certification. 4.6.2014 [cited 30.3.2015]. Available: <http://tinyurl.com/p99nkgg>.

[63] Breton, R. & Rousseau, R. *The C-OODA: A Cognitive Version of the OODA loop to represent C2 Activities*. Valcartier 13.-16.2005. Lecture slides. Command and Control Process Modeling Group. 27 pages. [cited 27.3.2015]. Available: <http://tinyurl.com/nzd4v6n>.

[64] Candolin, C. Dr.Sc, Head of the Cyber Defence Sector, Defence Command of the Finnish Defence Forces. Helsinki. Interview, 12.2.2015. Interview notes are in author's possession.

[65] Carr, J. *Inside Cyber Warfare*. Sebastopol: O'Reilly Media, Inc., 2010. 212 pages. ISBN 978-0-596-80215-8.

[66] Chia, T. *Confidentiality, Integrity, Availability: The three components of the CIA Triad* [blog posting]. IT Security Community Blog. 20.8.2012 [cited 14.4.2015]. Available: <http://tinyurl.com/pan9o2h>.

- [67] Clarke, Z., Clawson, J. & Cordell, M. *A Brief History of Hacking...* [web page]. [cited 31.1.2015]. Available: <http://tinyurl.com/nd9nfr8>.
- [68] Coursey, D. *Study: Hacking Passwords Easy As 123456* [electronic article]. PCWorld. 21.1.2010 [cited 26.2.2015]. Available: <http://tinyurl.com/psrozsx>.
- [69] Coyle, G. *The Analytic Hierarchy Process (AHP)* [online publication]. [cited 2.2.2015]. Available: <http://tinyurl.com/3bfdla>.
- [70] Crawford, S. P. *First Do Not Harm: The Problem of Spyware*. Berkeley Technology Law Journal. Vol. 4, no. 3, pp. 1433–1475. [cited 9.4.2015]. Available: <http://tinyurl.com/plw4frl>.
- [71] Dalakov, G. *Colossus computer of Max Newman and Tommy Flowers* [web page]. [cited 31.1.2015]. Available: <http://tinyurl.com/6dts6za>.
- [72] Davies, P. H. J., Gustafson, K. & Ridgen, I. *The Intelligence Cycle is Dead, Long Live the Intelligence Cycle*. In: Phythian, M. (Ed.). *Understanding the Intelligence Cycle*. London: Routledge, 2013. Pp. 56–75. ISBN 978-0-415-81175-0.
- [73] Du, S., Lu, T., Zhao, L., Xu, B., Guo, X. & Yang, H. *Towards An Analysis of Software Supply Chain Risk Management*. In: The World Congress on Engineering and Computer Science WCECS 2013, San Francisco, 23-25.10.2013. 6 pages. ISBN 978-988-19252-3-7. [cited 4.4.2015] Available: <http://tinyurl.com/lhw35dr>.
- [74] Forman, E. H. & Gass, S. I. *The Analytic Hierarchy Process – An Exposition* [online publication]. [cited 2.2.2015]. Available: <http://tinyurl.com/p8vrq5n>.
- [75] Gamet, J. *China Demands Back Door into Computers, Software* [electronic article]. The Mac Observer. 29.1.2015 [cited 2.3.2015]. Available: <http://tinyurl.com/pm98zfl>.
- [76] Gidda, M. *Edward Snowden and the NSA files – timeline* [electronic article]. The Guardian. 21.8.2013 [cited 9.4.2015]. Available: <http://tinyurl.com/k4bx26t>.

- [77] Gill, P. & Phythian, M. *From Intelligence Cycle to Web of Intelligence: Complexity and the Conceptualisation of Intelligence*. In: Phythian, M. (Ed.). *Understanding the Intelligence Cycle*. London: Routledge, 2013. Pp. 21–42. ISBN 978-0-415-81175-0.
- [78] Glad, T. *Tiedustelu avoimista lähteistä metatiedon avulla*. Bachelor's Thesis. Leppävaara, 2013. Laurea University of Applied Sciences. 48 Pages.
- [79] Heikkala, T., Källi, J., Majuri, P., Puuperä, S., Rissanen, T., STerämä, S., Toivanen, J. & Vaara, I. *Operaatioturvallisuus 2030*. In: Sirén, T. (Ed.). *Strateginen kommunikaatio ja informaatio-operaatiot 2030*. Helsinki: National Defence University, 2011. Pp. 127–146. ISBN 978-951-25-2254-5.
- [80] Huopio, K. Chief Specialist, National Cyber Security Centre Finland, Finnish Communications Regulatory Authority. Helsinki. Interview, 13.2.2015. Interview notes are in author's possession.
- [81] Hyppönen, M. Chief Research Officer, F-Secure. Helsinki. Interview, 30.3.2015. Interview notes are in author's possession.
- [82] Hyppönen, M. *Three Types of Online Attack*. November 2011, TEDxBrussels. Lecture. [cited 26.2.2015]. Available: <http://tinyurl.com/myektwx>.
- [83] Jellenc, E. *Profiles of Cyber Terrorists and Hackers*. Ankara 4.11.2013, COE DAT. Lecture. Notes are in author's possession.
- [84] Jensen, C. J., McElreath, D. H. & Graves, M. *Introduction to Intelligence Studies*. Boca Raton: CRC Press, 2013. 352 pages. ISBN 978-1-4665-00037.
- [85] Jerräng, M. *Klart för FRA-spaning i kabel* [electronic article]. ComputerSweden. 14.10.2009 [cited 14.4.2015]. Available: <http://tinyurl.com/mtty8te7>.
- [86] Johnson, L. K. *National Security Intelligence*. In: Johnson, L. K (Ed.). *The Oxford Handbook of National Security Intelligence*. Oxford: Oxford University Press, Inc., 2010. Pp. 3–32. ISBN 978-0-19-537588-6.

[87] Johnson, M. *Cyber Crime, Security and Digital Intelligence*. Surrey: Gower Publishing Limited, 2013. 252 pages. ISBN 978-1-4094-5449-6.

[88] Kain, E. *Report: NSA Intercepting Laptops Ordered Online, Installing Spyware* [electronic article]. Forbes. 29.12.2013 [cited 9.4.2015].
Available: <http://tinyurl.com/mr77f8u>.

[89] Kalinen, R. Specialist, Finnish Security Intelligence Service. Helsinki. Interview, 25.3.2015. Interview notes are in author's possession.

[90] Kantola, H. Major, Staff Officer, Cyber Defence Sector at the Defence Command of the Finnish Defence Forces, researcher at NATO CCDCOE. Helsinki. Interview, 10.2.2015. Interview notes are in author's possession.

[91] Kantola, H. *Datanetvärksattacker, trend eller nödvändighet? - ur ett småstatsperspektiv*. General Staff Officer's Thesis. Helsinki, 2011. National Defence University. 87 pages.

[92] Kari, M. J. Colonel, Deputy Director, Finnish Defence Intelligence Agency. Helsinki. Interview, 3.3.2015. Interview notes are in author's possession.

[93] Kelley, M. B. & Nudelman, M. *The Snowden Saga: Here's Everything We Know About The NSA's Nightmare Leak* [electronic article]. Business Insider UK. 14.11.2013 [cited 9.4.2015]. Available: <http://tinyurl.com/nbg9gpa>.

[94] Kenttälä, M. Personal communication, 14.4.2015. Material is in author's possession.

[95] Kiravuo, T. M. Sc., Researcher, Aalto University. Espoo. Interview, 6.3.2015. Interview notes are in author's possession.

[96] Klimas, L. *'Dangers of Surveillance': Privacy Expert Reviews Why Increased Spying Is Bad* [electronic article]. The Blaze. 2.4.2013 [cited 16.4.2015].
Available: <http://tinyurl.com/ogtk733>.

[97] Korkiamäki, I. *Suomen kyberturvallisuus sotilaallisesta näkökulmasta*. Espoo 3.3.2015, Aalto University. Lecture. Notes are in author's possession.

[98] Kremen, S. H. *Apprehending The Computer Hacker: The Collection and Use of Evidence* [web page]. Computer Forensics Online. [cited 1.2.2015].
Available: <http://tinyurl.com/qx4tjs7>.

[99] Kärkkäinen, A. Major (Engineering), Chief of Cyber Division, Finnish Defence Forces C5 Agency. Helsinki. Interview, 27.2.2015. Interview notes are in author's possession.

[100] Kärkkäinen, A. *A Cyber Security Architecture for Military Networks Using a Cognitive Network Approach*. General Staff Officer's Thesis. Helsinki, 2013. National Defence University. 116 pages.

[101] Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G. & Wolff, S. *Brief History of the Internet* [web page]. Internet Society. [cited 31.1.2015]. Available: <http://tinyurl.com/ogtkzgm>.

[102] Limnéll, J. Dr. Sc. (Mil.), Professor, Aalto University. Espoo. Interview, 16.2.2015. Interview notes are in author's possession.

[103] Lucénus, J. *Computer Network Exploitation*. In: Vankka, J. (Ed.). *Cyber Warfare*. Helsinki: National Defence University, 2013. Pp. 27–46. ISBN 978-951-25-2456-3.

[104] MacAskill, E., Borger, J., Hopkins, N., Davies, N. & Ball, J. *GCHQ taps fibre-optic cables for secret access to world's communications* [electronic article]. The Guardian. 21.6.2013 [cited 1.3.2015]. Available: <http://tinyurl.com/k8gr7o2>.

[105] Mattern, T., Felker, J., Borum, R. & Bamford, G. *Operational Levels of Cyber Intelligence*. *International Journal of Intelligence and Counter Intelligence*, 2014. Vol. 27, no. 4, pp. 702–719. ISSN 0885-0607.

[106] McClure, S., Scambray, J. & Kurtz, G. *Hacking Exposed 7: Network Security Secrets & Solutions*. 7th Ed. New York, USA: McGraw-Hill, 2012. 741 pages.
ISBN 978-0-07-178028-9.

- [107] Milleta, I. & Saaty, T. L. *On the Relativity of Relative Measures - Accommodating both Rank Preservation and Rank Reversals in the AHP*. European Journal of Operational Research, 2000. Vol. 121, No. 1, pp. 205–212. ISSN 0377-2217.
- [108] Mitnick, K. *Social engineering*. Indianapolis: Wiley Publishing, Inc., 2011. 382 pages. ISBN 978-0-470-63953-5.
- [109] Morgan, D. L. *Integrating qualitative and quantitative methods: a pragmatic approach*. Thousand Oaks: SAGE Publications, Inc., 2014. 269 pages. ISBN 978-0-7619-1523-2.
- [110] Moskowitz, J. *Regin spying tool linked to NSA among first malware meant for espionage* [electronic article]. The Christian Science Monitor. 24.12.2014 [cited 9.4.2015]. Available: <http://tinyurl.com/ny6vxhw>.
- [111] Nicks, D. *Report: U.K. Spy Agency Stored Millions of Webcam Images* [electronic article]. Time. 27.2.2014 [cited 1.3.2015]. Available: <http://tinyurl.com/o95bcrp>.
- [112] Niemelä, M. S. MD, Silverskin Information Security Oy. Helsinki. Interview, 17.2.2015. Interview notes are in author's possession.
- [113] Nordström, H., Laitinen, K., Lundelin, M., Herrala, J., Sjöblom, J., Honkanen, K. & Nurminen, M. *Guidelines for developing Finnish legislation on conducting intelligence. A report of the Working Group*. Ministry of Defence, 2015. 141 pages. ISBN 978-951-25-2624-6. [cited 19.1.2015]. Available: <http://tinyurl.com/mjl8c9b>.
- [114] O'Hara, G. *Cyber-Espionage: A Growing Threat to the American Economy*. CommLaw Conspectus: Journal of Communications Law and Technology Policy, 2010. Vol. 19, No. 1, pp. 241–275. [cited 9.4.2015]. Available: <http://tinyurl.com/n4uwys0>.
- [115] Ottis, R. Ph. D., Postdoctoral Researcher, Jyväskylä University. Jyväskylä. Interview, 4.2.2015. Interview notes are in author's possession.
- [116] Palokangas, T. Major, Senior Staff Officer, J3 of the Defence Command. Helsinki. Interview, 26.2.2015. Interview notes are in author's possession.

[117] Palokangas, T. *Cyberwar: Another Revolution in Military Affairs?* In: Rantapelkonen, J. & Salminen, M. (Eds.). *The Fog of Cyber Defence*. Helsinki: National Defence University, 2013. Pp. 146–153. ISBN 978–951–25–2430–3.

[118] Paulus, T. M., Lester, J. N. & Dempster, P. G. *Digital Tools for Qualitative Research*. London: SAGE Publications Ltd, 2014. 206 pages. ISBN 978-1-4462-5607-7.

[119] Pilkington, E. *Edward Snowden: I brought no leaked NSA documents to Russia* [electronic article]. The Guardian. 18.10.2013 [cited 9.4.2015]. Available: <http://tinyurl.com/mcyrqnl>.

[120] Polk, R. B. *A Critique of The Boyd Theory - Is It Relevant to the Army?* Fort Leavenworth: United States Army Command and General Staff College, 1999. 73 pages. [cited 20.1.2015] Available: <http://tinyurl.com/oc3awfh>.

[121] Rantapelkonen, J. Dr. Sc. (Mil.), Lieutenant Colonel, Professor, Department of Operational Art and Tactics at National Defence University, Finland. Helsinki. Interview, 25.3.2015. Interview notes are in author's possession.

[122] Rantapelkonen, J. & Salminen, M. (Eds.). *The Fog of Cyber Defence*. Helsinki: National Defence University, 2013. 234 pages. ISBN 978–951–25–2430–3.

[123] Rouse, M. *Social Engineering* [web page]. TechTarget. [cited 1.3.2015]. Available: <http://tinyurl.com/3z6jkfy>.

[124] Rouse, M., Layton, A., Scott, J. & Zydyk, M. *Bulletin Board System (BBS)* [web page]. WhatIs.com. [cited 1.2.2015]. Available: <http://tinyurl.com/qjjguh2>.

[125] Saarinen, J. *Ammottava tietoturva-aukko sai valtioiden tukemat hakkeriryhmät urkkimaan tietoja* [electronic article]. Helsingin sanomat. 10.4.2014 [cited 14.4.2015]. Available: <http://tinyurl.com/nebvthk>.

[126] Said, R. *Kyberhyökkäyksen vaikutuksesta*. Bachelor's Thesis. Helsinki, 2014. National Defence University. 21 pages.

- [127] Saunders, M., Lewis, P. & Thornhill, A. *Research Methods for Business Students*. 6. Ed. Harlow: Pearson, 2012. 696 pages. ISBN 978-0-273-75075-8.
- [128] Schmitt, M. N. (Ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, United Kingdom: Cambridge University Press, 2013. 282 pages. ISBN 978-1-107-61377-5.
- [129] Storm, D. *Remotely Listen in Via Hacked VoIP Phones: Cisco Working on Eavesdropping Patch* [electronic article]. Computerworld. 8.1.2013 [cited 1.3.2015]. Available: <http://tinyurl.com/of2zzpx>.
- [130] Thompson, J., Landee-Thompson, B., Fichtl, T. & Adelman, L. *Measurement and Evaluation of Military Intelligence Performance* [report]. United States Army Research Institute for the Behavioral and Social Sciences. April 1989 [cited 4.4.2015]. Available: <http://tinyurl.com/k4q3uq9>.
- [131] Timonen, J. M. Sc., First Lieutenant (Engineering), Finnish Defence Forces C4 Agency. Helsinki. Interview, 27.2.2015. Interview notes are in author's possession.
- [132] Timonen, J. *Kyberdemo*. Helsinki, 9.2.2015. National Defence University. Lecture. Notes are in author's possession.
- [133] Toivonen, J. *Verkkohyökkäysten voima kasvaa myös Suomessa* [electronic article]. Helsingin sanomat. 3.1.2015 [cited 14.4.2015]. Available: <http://tinyurl.com/nlv2m4a>.
- [134] Townsend, M. *How a Team of Social Media Experts is Able to Keep Track of the UK Jihadis* [electronic article]. The Guardian. 17.1.2015 [cited 1.3.2015]. Available: <http://tinyurl.com/opg7xm8>.
- [135] Triantaphyllou, E. & Mann, S. H. *Using the Analytic Hierarchy Process for Decision Making in Engineering Applications: Some Challenges*. International Journal of Industrial Engineering: Theory Applications and Practice, 1995. Vol. 2, no. 1, pp. 35–44. ISSN 1072-4761. [cited 2.2.2015]. Available: <http://tinyurl.com/n9j8j4v>.

- [136] Tuukkanen, T. Commander, Research Manager, Cyber Defence Section of Finnish Defence Research Agency. Riihimäki. Interview, 20.2.2015. Interview notes are in author's possession.
- [137] Valkola, E. *Kirjallisuustutkimus tutkimusmenetelmänä*. In: Jormakka, J. & Lappalainen, E. (Eds.). *Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa*. Helsinki: National Defence University, 2004. Pp. 42–29. ISBN 951-25-1540-7.
- [138] Vankka, J. (Ed.). *Critical Infrastructure Protection Against Cyber Threats*. Helsinki: National Defence University, 2014. 126 pages. ISBN 978-951-25-2600-0.
- [139] Vanninen, A. & Halminen, L. *Espoolaisnuorukaisen epäillään vieneen tuhansien luottokorttien tiedot* [electronic article]. Helsingin sanomat. 19.10.2013 [cited 14.4.2015]. Available: <http://tinyurl.com/nn9o5zb>.
- [140] Warner, M. *The Past and Future of the Intelligence Cycle*. In: Phythian, M. (Ed.). *Understanding the Intelligence Cycle*. London: Routledge, 2013. Pp. 9–20. ISBN 978-0-415-81175-0.
- [141] Wihersaari, J. Personal communication, 15.4.2015. Notes are in author's possession.
- [142] Wihersaari, J. *Julkisiin lähteisiin perustuva tiedustelu (Open Source Intelligence, OSINT)*. In: Saarelainen, J., Tynkkynen, V., Aherto, J., Hyytiäinen, M. & Metteri, J. *Johtamissodankäynti*. Helsinki: National Defence University, 2000. Pp. 238–254. ISBN 951-25-1187-8.
- [143] Villapaz, L. *Symantec Discovers Regin: 'Stealth' Malware Used For Spying Purposes* [electronic article]. International Business Times. 23.11.2014 [cited 1.3.2015]. Available: <http://tinyurl.com/ou26flk>.
- [144] Özteke, C. *Cyber - A New War Domain*. Defence Turkey. Vol. 8, no. 48, p. 8. ISSN 1306-5998.

ANNEXES

ANNEX 1	DESCRIPTIONS OF AND ASSESSMENTS ON THE INTERVIEWEES	6 pages
ANNEX 2	THEME QUESTIONS FOR INTERVIEWS	1 page
ANNEX 3	COVER LETTER FOR AHP SURVEY	4 pages
ANNEX 4	AHP SURVEY	8 pages
ANNEX 5	RESPONSES TO AHP-SURVEY	7 pages
ANNEX 6	RESULTS OF AHP SURVEY	4 pages

DESCRIPTIONS OF AND ASSESSMENTS ON THE INTERVIEWEES

Candolin, Catharina

Dr. Catharina Candolin works currently as the head of the Cyber Defence Sector at the Defence Command of the Finnish Defence Forces. Her educational background is in Computer Science and Engineering, on which she wrote her dissertation, *Securing military decision making in a network-centric environment*, at Helsinki University of Technology in year 2005. She has worked at the Finnish Defence Forces since year 2003, and prior to her current position she worked for 5 years as Chief of information management at the Defence Command of the Finnish Defence Forces. [7]

Having studied engineering and worked in the C4 field for nearly a decade, Dr. Candolin can be considered an expert in C4 systems that has perspective to the cyber field from information and computer systems perspective. She does not, however, have experience in intelligence, which can be considered a limitation to her expertise with respect to cyber intelligence.

Huopio, Kauto

Kauto Huopio has worked as Chief Specialist at Finnish Communications Regulatory Authority (FICORA) / National Cyber Security Centre Finland (NCSC-FI) since year 2001, having an over 13-year experience at his current position. Prior to joining the FICORA he had worked for 5 years as senior network engineer. [35]

With an experience of well over a decade in cyber security and being substantially involved in maintaining CERT-FI's cyber situation awareness, Huopio possesses valuable insight on current development of online threats as well as relatively long-term perspective to them. The fact that he has been cited in numerous newspaper articles associated with cyber security [34; 125; 133; 139] suggests that he is considered an authority. He does not, however, have personal working experience on intelligence.

Hyppönen, Mikko

Mikko Hyppönen is the Chief Research Officer for F-Secure, having worked for the company since 1991. "Mikko Hypponen has assisted law enforcement authorities in the United States, Europe and Asia on cybercrime cases. He has also written for international publications like the Scientific American, Foreign Policy, New York Times and virus Bulletin, as well as addressing the most important security-related conferences worldwide." [38]

Having worked in the field of information security with one of the now leading cyber security companies in the world since the public emergence of the Internet, Mikko Hyppönen can be assessed to have exceptionally profound insight into cyber security, and it is not surprising that he is considered a leading authority in the field. From the perspective of the thesis, Hyppönen might possibly have due to his background a critical perception of cyber intelligence.

Kalinen, Riku

Riku Kalinen works as a specialist at the Finnish Security Intelligence Service. He has worked in the field of cyber counterintelligence for 20 years [89] and holds a GIAC Reverse Engineering Malware (GREM) certification [43]. Based on his lengthy experience and occupation, he can be considered an expert on cyber security threats and furthermore to have profound perspective to the field. Due to his place of employment, his point of view is from countering cyber intelligence rather than conducting such.

Kantola, Harry

Major Harry Kantola works currently as researcher at the NATO Cooperative Cyber Defence Centre of Excellence as well as at the Cyber Defence Sector at the Defence Command of the Finnish Defence Forces. His general staff officer's thesis *Datanetvärksattacker, trend eller nödvändighet? - ur ett småstatsperspektiv* addressed offensive computer networks operations from a small state perspective, and he is a co-author of *The Fog of Cyber Defence, Countering Threats-a Comprehensive Model for Utilization of Social Media for Security and law Enforcement Authorities and Modelling Cyber Warfare as a Hierarchic Error Effect of Information*. [22]

Judging by his publications and the fact that he is appointed as representative to the CCDCOE major Kantola can be considered an expert on cyber warfare. Given that cyber intelligence has a substantial offensive element, Kantola's research can be considered to be valuable to this study.

Kari, Martti

Colonel Kari works presently as Deputy Director of the Finnish Defence Intelligence Agency (FDIA). He has worked at the Finnish Intelligence Research Establishment (FIRE) for half of his 3-decade career in the Finnish Defence Forces. [37] He was summoned to the workgroup of preparing *Guidelines for developing Finnish legislation on conducting intelligence* as permanent expert member [113].

Due to his extensive experience in military intelligence, Colonel Kari can be considered to have a substantially profound perspective to the field. Furthermore, having been involved with writing the recently published *Guidelines for developing Finnish legislation on conducting intelligence*, he can be considered to have insight to the different aspects of cyber intelligence. This can to an extent be considered also a limitation, because it might bring bias of perceiving the subject from military intelligence perspective.

Kiravuo, Timo

Timo Kiravuo works as researcher at Aalto University, Dept. of Communications and Networking (Comnet). He currently works on a doctoral thesis on security aspects of large Ethernets. He has a 2-decade experience in the IT field, half of which at Nixu, a prominent information security consulting company. [50] Having extensive experience in IT and doing research on network security, he can be considered an expert on countering cyber threats. However, his insight into the field of intelligence can perhaps be limited.

Kärkkäinen, Anssi

Major (Engineering) Anssi Kärkkäinen is the Chief of Cyber Division at Finnish Defence Forces C5 Agency [6]. He has written a thesis by the title *A Cyber Security Architecture for Military Networks Using a Cognitive Network Approach* [100]. Kärkkäinen's field of expertise can be considered cyber security, however his experience in the intelligence framework is limited.

Limnell, Jarno

Doctor of Military Sciences (National Defense University), Master of Social Science (Helsinki University), Captain (ret.) Jarno Limnell works as Professor of Cyber Security at Aalto University, and he is the VP of Cyber Security and Business Development at Insta Group Oy. He has previously worked as Director of Cyber Security at McAfee and Stonesoft. His last position in the Finnish Defence Forces was as lecturer at the National Defence University. He is the author of *Kyberturvallisuus* and a co-author of *The Fog of Cyber Defence*. [33] Professor Limnell can be considered an expert in cyber security. The security perspective might, however, limit his perspective to the field of intelligence.

Niemelä, Mikko S.

Mikko Niemelä is the founder, Managing Director and Senior Security Advisor at Silverskin Information Security Oy. The subject of his GIAC (GSNA) Gold Certification thesis was *Choosing corporate level instant messaging system and implementing audit controls*. [39] Niemelä can be considered an expert with hands-on experience in the field of conducting offensive intelligence on private corporations. His close affiliation to Silverskin Oy might perhaps be considered to be a source of bias.

Ottis, Rain

“Dr Rain Ottis is an Associate Professor in Tallinn University of Technology, Estonia. From 2008 to 2012 he served as a scientist at the NATO Cooperative Cyber Defence Centre of Excellence, where he worked on strategic analysis and concept development in the context of national and international cyber security. Prior to that assignment he served as a communications officer in the Estonian Defence Forces, focusing primarily on cyber defence training and awareness. In addition to his current assignment, he is teaching cyber security in University of Jyväskylä, Finland. He is a graduate of the United States Military Academy (BS, Computer Science) and Tallinn University of Technology (PhD, Computer Science; MSc, Informatics). His research interests include cyber conflict, national cyber security, politically motivated cyber attacks and the role of volunteers in cyber security.” [11]

Dr. Ottis has substantial expertise in the field of cyber security, and has also military experience. A possible limitation with respect to the thesis might be his security-oriented perspective.

Palokangas, Tero

Major Tero Palokangas works as a senior staff officer at J3 of the Defence Command of the Finnish Defence Forces [48]. He can be considered to bring an operational perspective to the examination of cyber intelligence, whereas his experience on intelligence might be a limitation.

Timonen, Jussi

First Lieutenant (Engineering) “Jussi Timonen is a Ph.D. Student at the Finnish National Defence University and working at the Finnish Defence forces C4 agency. His main research areas are information fusion, common operational picture and situational awareness in critical infrastructure.” [138, p. 126] Timonen can be considered to have substantial insight to hacking activities and cyber security. His experience on the field of intelligence is perhaps a limitation.

Tuukkanen, Topi

Commander Tuukkanen works as Research Manager (Cyber) at Finnish Defence Research Agency, and he has published the works *Adapting the Current National Defence Doctrine to Cyber Domain* and *Cyber Sovereignty* [51]. Hence, he can be recognized to have insight into cyber warfare. However, his level of practical expertise might be a limitation.

Rantapelkonen, Jari

Doctor of Military Sciences, Lieutenant Colonel Jari Rantapelkonen works as Professor at the Department of Operational Art and Tactics of the National Defence University. He is the co-editor of *The Fog of Cyber Defence*. [122] Professor Rantapelkonen can be recognized as an authority in the field of cyber warfare from an Operational Art perspective. However, his technical expertise is a limitation from the perspective of the thesis.

THEME QUESTIONS FOR INTERVIEWS

1. The definition of intelligence in cyber domain and how it relates to other intelligence disciplines.

- How would you define intelligence in cyber domain?
- How and by what attributes is cyber intelligence differentiated from other intelligence disciplines?

2. Reach, limits, advantages and disadvantages of intelligence in cyber domain.

- To what extent can intelligence requirements be met solely through intelligence methods in cyber domain?
- What are the greatest advantages and disadvantages compared to other disciplines?
- What kind of intelligence can only be acquired through intelligence in cyber domain?
- What kind of intelligence cannot be acquired?

3. Intelligence operatives in cyber domain.

- How would you categorize intelligence operatives in cyber domain?
- What are their typical objects/motives?

4. Intelligence methods in cyber domain.

- How would you categorize different intelligence methods in cyber domain?

5. Criteria for evaluating intelligence methods in cyber domain.

- What factors would you point out as most enabling / facilitating the use of intelligence methods in cyberspace?
- What factors would you point out as most limiting / restraining the use of intelligence methods in cyberspace?
- What factors would you point out as best determining the quality of intelligence methods in cyberspace?

COVER LETTER FOR AHP SURVEY

Dear Sir or Madam,

Thank you for taking the time to share your views on the topic of intelligence in cyber domain, and furthermore thank you for agreeing to submit your assessments to the AHP-model of cyber intelligence acquisition created for the analysis purposes of the study.

The following stage of the study is a survey conducted in an online interface of Expert Choice Companion Solution. You will receive links to the surveys along with this message.

One aim of the study is to establish a model of intelligence acquisition in cyber domain, categorizing types of acquisition methods and criteria for evaluating the qualities of these methods from a given perspective. The model has been established based on existing literature and refined based on interviews with experts of the field. The model incorporates methods directly contributing to or enabling intelligence acquisition in cyber domain. The focus is on acquisition of information, and the aspects of analyzing, synthesizing, disseminating and exploiting the acquired intelligence have been excluded.

The Analytic Hierarchy Process (AHP) is a multi-criteria decision-making approach and was introduced by Thomas L. Saaty. It is a decision support tool which can be used to solve complex decision problems. It uses a multi-level hierarchical structure of objectives, criteria, sub criteria, and alternatives. [135] A schematic illustration of the AHP model is displayed in Figure A3.1 below.

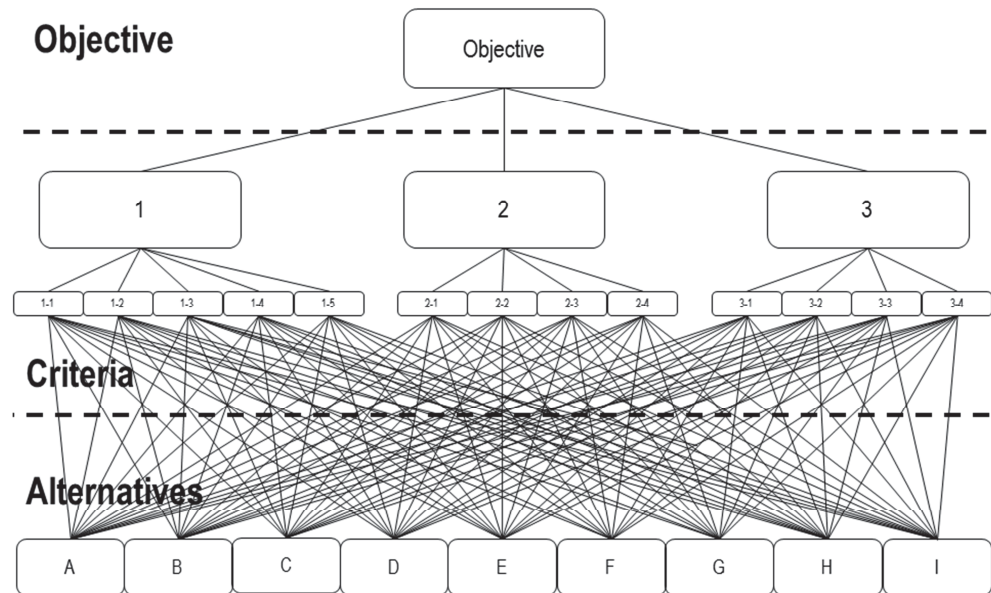


Figure A3.1 Example of an AHP Hierarchy

In the AHP model, alternatives are weighed with respect to the set criteria and the criteria are weighed appropriately in with respect to each other by giving the assessed items numeric values. Further information about the AHP as a method can be found online, for example from http://en.wikipedia.org/wiki/Analytic_hierarchy_process and <https://aaltodoc.aalto.fi/bitstream/handle/123456789/15146/isbn9783319125022.pdf>.

In this study, the AHP will be used as a tool to analyze how favorable different intelligence acquisition methods are from different operatives' points of view. The assessment will be done with respect to the preconditions of three distinct scenarios:

- 1. Finnish criminal organization, operating from Finland.**
 - Objective: acquire any information and means exploitable for direct financial revenue.
- 2. Hactivist group from an Arabic-speaking country, operating from the Middle East.**
 - Objective: defacing official Finnish government websites and social media accounts with propaganda of the group's ideological agenda.
- 3. Non-European foreign nation state, conducting intelligence operations on Finnish target organizations and systems.**
 - Objective: acquire confidential information about Finnish R&D on online communication security technology.

The scenarios are coarse rather than detailed. Please try to empathize with the scenario and affiliated objectives as well as you can. In the generated AHP model, individual intelligence acquisition methods are treated as alternatives of the hierarchy, and they are evaluated based on three main criteria (with sub-criteria). The elements of the AHP model are displayed in Table A3.1 below.

Table A3.1 Elements of the AHP Model on Intelligence Acquisition Methods in Cyber Domain

Intelligence Acquisition Methods in Cyber Domain	Evaluating Criteria
<ul style="list-style-type: none"> • Cyber-OSINT • Scanning and enumeration in public domain • Scanning and enumeration in restricted domain • Intrusion • Exploiting privileged information • Exfiltration of data • Obfuscation • Sustaining access • Network mapping • Social engineering • Physical surveillance • Network surveillance • Malware • Physical attack • Alterations in the supply chain 	<p>Performance</p> <ul style="list-style-type: none"> • Speed • Efficiency • Resolution • Verifiability • Validity • Reliability <p>Capability</p> <ul style="list-style-type: none"> • Technology • Expertise <ul style="list-style-type: none"> ○ Technical ○ Contextual • Resources • Leadership • Support from other INTEL <p>Risk</p> <ul style="list-style-type: none"> • Jurisdiction • Exposure of operative • Exposure of method • Exposure of target

The assessment will proceed in the following sequence:

- Step 1: Description of scenario
- Step 2: Assessment of significance of main evaluating criteria with respect to scenario
- Steps 3-6 : Assessment of significance of sub-criteria with respect to scenario
- Steps 7-22: Assessment of alternatives with respect to criteria
- Step 23: Comments on the survey
- Step 24: End of survey

Please pay attention to the fact that three identical surveys have been generated for the set scenarios, and therefore the assessment process needs to be carried out three times, once for each scenario. When assessing the alternatives, choose a value between 0% and 100% where 0% stands for poor and 100% stands for outstanding. If you deem the criteria not applicable to an alternative, choose the option 'Not Applicable.' In case you need to make additional presumptions in order to make your assessments, or you have other remarks to make, please enter them in the comment field at the end of the survey. If you experience any problems or if you have any questions regarding the survey, please do not hesitate to contact me.

Thank you very much for your time and effort!

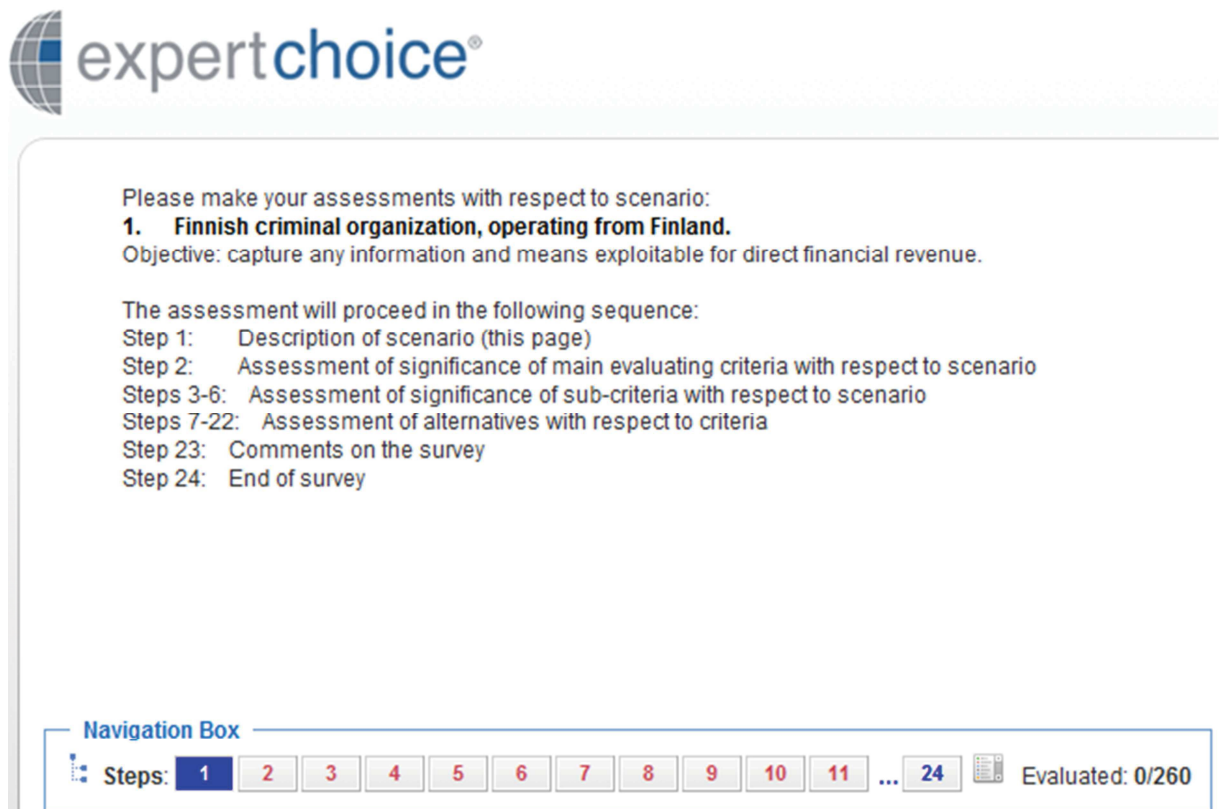
With best regards,

Lieutenant (Navy) Karri Wihersaari
karri.wihersaari@mil.fi

AHP SURVEY

1 STEP 1 – DESCRIPTION OF SCENARIO

On the start page of the survey, the scenario to be assessed and an overview of the survey are depicted. Figure A4.1 depicts the start page of the survey for scenario 1. Start pages of other two surveys are identical apart from the scenario description.



The screenshot shows the 'expertchoice' logo at the top left. Below it, the text reads: 'Please make your assessments with respect to scenario: **1. Finnish criminal organization, operating from Finland.** Objective: capture any information and means exploitable for direct financial revenue.'

Below this, it states: 'The assessment will proceed in the following sequence:' followed by a list of steps:

- Step 1: Description of scenario (this page)
- Step 2: Assessment of significance of main evaluating criteria with respect to scenario
- Steps 3-6: Assessment of significance of sub-criteria with respect to scenario
- Steps 7-22: Assessment of alternatives with respect to criteria
- Step 23: Comments on the survey
- Step 24: End of survey

At the bottom, there is a 'Navigation Box' containing a series of numbered buttons from 1 to 24. Button 1 is highlighted in blue. To the right of the buttons is a small icon of a document and the text 'Evaluated: 0/260'.

Figure A4.1 Description of the Scenario and Overview of the Survey

2 STEPS 2-6 – PRIORITIZING THE MAIN AND SUB-CRITERIA

In steps 2-6 of the survey, the main and sub-criteria are prioritized in terms of significance with respect to the scenario. The legends for the criteria in the survey are as follows:

- **Evaluating criteria:** How significant are the main evaluating criteria? Please make your assessment with respect to the set scenario:

1. Finnish criminal organization, operating from Finland.

Objective: capture any information and means exploitable for direct financial revenue.

Evaluating scale 0-1, where 0 stands for not significant, 1 stands for very significant.

- **Performance:** Criteria contributing to the the performance of an intelligence acquisition method.
 - **Speed:** By using the method, is intelligence acquired quickly enough?
 - **Efficiency:** When using the method, to what extent is the time, effort, and/or cost well-used?
 - **Resolution:** Is the resolution of the method appropriate? Does the method produce or contribute to producing intelligence in appropriate detail?
 - **Verifiability:** Is the information gathered verifiable using other sources?
 - **Validity:** Is the validity of intelligence collected sufficient?
 - **Reliability:** Is the reliability of intelligence collected sufficient?
- **Capability:** Criteria contributing to the capability of an operative to utilize an intelligence method.
 - **Technology:** Is the operative sufficiently up-to-date and equipped in terms of technology with respect to the method?
 - **Expertise:** Does the operative possess sufficient expertise with respect to the method?
 - **Technical:** Does the operative possess sufficient technical expertise with respect to the method?
 - **Contextual:** Does the operative possess sufficient contextual expertise (i.e. expertise required to comprehend the content) with respect to the method?

- **Resources:** Does the operative have sufficient resources (funds, personnel) in order to utilize the method?
- **Leadership:** Is the operative capable of effectively directing the use of the method?
- **Support from other INTEL:** Is the operative capable of supporting the method by other information sources?
- **Risk:** Criteria contributing to the risks involved in utilizing an intelligence method.
 - **Jurisdiction:** To what extent is the method utilizable by the operative with respect to jurisdiction? How well is the method utilizable within legal constraints?
 - **Exposure of operative:** How preferable is the method with respect to risking the operative being identified?
 - **Exposure of method:** How preferable is the method with respect to risking the method used being identified?
 - **Exposure of target:** How preferable is the method with respect to risking the target noticing the intelligence efforts?

Figures A4.2–6 depict the survey pages for prioritizing the criteria.

Enter values from 0 to 1 for each objective with respect to "Evaluating criteria"		
Performance <p>Criteria contributing to the the performance of an intelligence acquisition method.</p>	Evaluating criteria <p>How significant are the main evaluating criteria? Please make your assessment with respect to the set scenario: 1. Finnish criminal organization, operating from Finland. Objective: capture any information and means exploitable for direct financial revenue.</p> <p>Evaluating scale 0-1, where 0 stands for not significant, 1 stands for very significant.</p>	Performance WRT Evaluating cri...
Performance	<input type="text"/>	
Capability	<input type="text"/>	
Risk	<input type="text"/>	

Figure A4.2 Weighing the Main Criteria

Enter values from 0 to 1 for each objective with respect to "Evaluating criteria > Performance"

Speed	Performance	Speed WRT Performance
By using the method, is intelligence acquired quickly enough?	Criteria contributing to the the performance of an intelligence acquisition method.	

Speed	<input type="text"/>	<input type="text"/>
Efficiency	<input type="text"/>	<input type="text"/>
Resolution	<input type="text"/>	<input type="text"/>
Verifiability	<input type="text"/>	<input type="text"/>
Validity	<input type="text"/>	<input type="text"/>
Reliability	<input type="text"/>	<input type="text"/>

Figure A4.3 Weighing the Sub-criteria of Performance

Enter values from 0 to 1 for each objective with respect to "Evaluating criteria > Capability"

Technology	Capability	Technology WRT Capability
Is the operative sufficiently up-to-date and equipped in terms of technology with respect to the method?	Criteria contributing to the capability of an operative to utilize an intelligence method.	

Technology	<input type="text"/>	<input type="text"/>
Expertise	<input type="text"/>	<input type="text"/>
Resources	<input type="text"/>	<input type="text"/>
Leadership	<input type="text"/>	<input type="text"/>
Support from other INTEL	<input type="text"/>	<input type="text"/>

Figure A4.4 Weighing the Sub-criteria of Capability

Enter values from 0 to 1 for each objective with respect to "Evaluating criteria > Capability > Expertise"

Technical	Expertise	Technical WRT Expertise
Does the operative possess sufficient technical expertise with respect to the method?	Does the operative possess sufficient expertise with respect to the method?	

Technical

Contextual

Figure A4.5 Weighing the Sub-criteria of Expertise

Enter values from 0 to 1 for each objective with respect to "Evaluating criteria > Risk"

Jurisdiction	Risk	Jurisdiction WRT Risk
To what extent is the method utilizable by the operative with respect to jurisdiction? How well is the method utilizable within legal constraints?	Criteria contributing to the risks involved in utilizing an intelligence method.	

Jurisdiction

Exposure of operative

Exposure of method

Exposure of target

Figure A4.6 Prioritizing Sub-criteria of Risk

3 STEPS 7-22 – ASSESSMENT OF ALTERNATIVES WITH RESPECT TO CRITERIA

In steps 7-22 of the survey, the alternatives are assessed against each sub-criteria with respect to the scenario. The legends for the alternatives in the survey are as follows:

- **Cyber-OSINT:** The collection and utilization of open source and publicly available information available through cyber domain.
- **Scanning and enumeration in public domain:** Scanning and enumeration of target system(s) in public environments.
- **Scanning and enumeration in restricted domain:** Scanning and enumeration of target system(s) in environments of restricted access (for example after breaking in to a closed network).
- **Intrusion:** Breaking into a restricted system.
- **Exploiting privileged information:** Utilization of information available in a restricted system or network.
- **Exfiltration of data:** To extract data found in a restricted system or network.
- **Obfuscation:** Erasing traces of unsanctioned activities in a system.
- **Sustaining access:** Establishing bridgehead and creating new points of entry into a target system.
- **Network mapping:** Investigating the topology and infrastructure composition of a system.
- **Social engineering:** Exploiting human-originated vulnerabilities through technical and/or social interaction.
- **Physical surveillance:** Exploiting sensors available on computers, mobile phones etc. in order to gain intelligence on activities or whereabouts of an object.
- **Network surveillance:** Surveillance and interception of network traffic.
- **Malware:** Targeted or non-targeted utilization of malware in order to gain access to or collect information from a closed system.
- **Physical attack:** Accessing a target system on-site or introducing malicious hardware to the target system.
- **Alterations in the supply chain:** Altering hardware and/or software before delivery to the end-user in order to gain access to and/or collect confidential information.

Figure A4.7 depicts the first survey page for assessing the alternatives.

Rate the impact of Alternatives with respect to Evaluating criteria > Performance > Speed

Cyber-OSINT

The collection and utilization of open source and publicly available information available through cyber domain.

Speed

By using the method, is intelligence acquired quickly enough?

Description for Cyber-OSINT WRT Speed

Cyber-OSINT	Not rated
Scanning and enumeration in public domain	Not rated
Scanning and enumeration in restricted domain	Not rated
Intrusion	Not rated
Exploiting privileged information	Not rated
Exfiltration of data	Not rated
Obfuscation	Not rated
Sustaining access	Not rated
Network mapping	Not rated
Social engineering	Not rated
Physical surveillance	Not rated
Network surveillance	Not rated
Malware	Not rated
Physical attack	Not rated
Alterations in the supply chain	Not rated

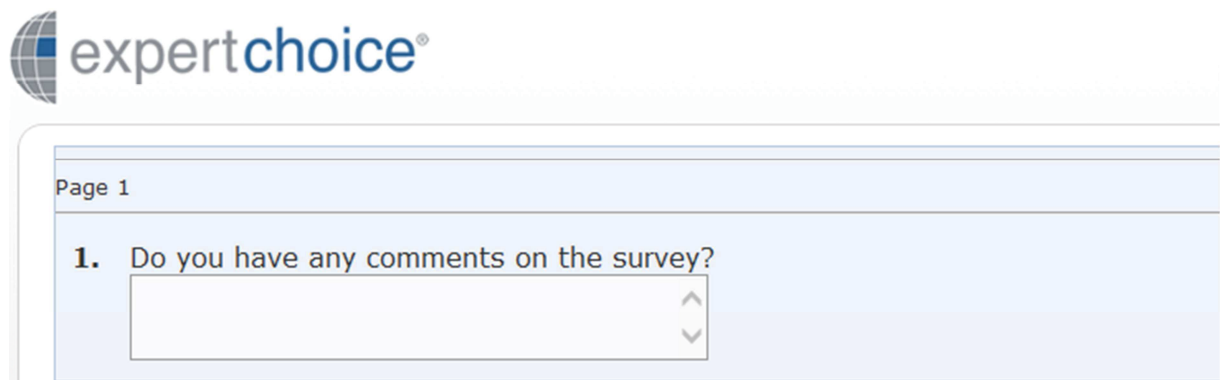
Cyber-OSINT

Intensity Name	Priority
Not rated	
100% - Outstanding	100%
95%	95%
90%	90%
85%	85%
80%	80%
75% - Very Good	75%
70%	70%
65%	65%
60%	60%
55%	55%
50% - Good	50%
45%	45%
40%	40%
35%	35%
30%	30%
25% - Moderate	25%
20%	20%
15%	15%
10%	10%
5%	5%
0% - Poor	0%
Not applicable	0%
Direct Value	

Figure A4.7 Evaluating Alternatives Against Speed

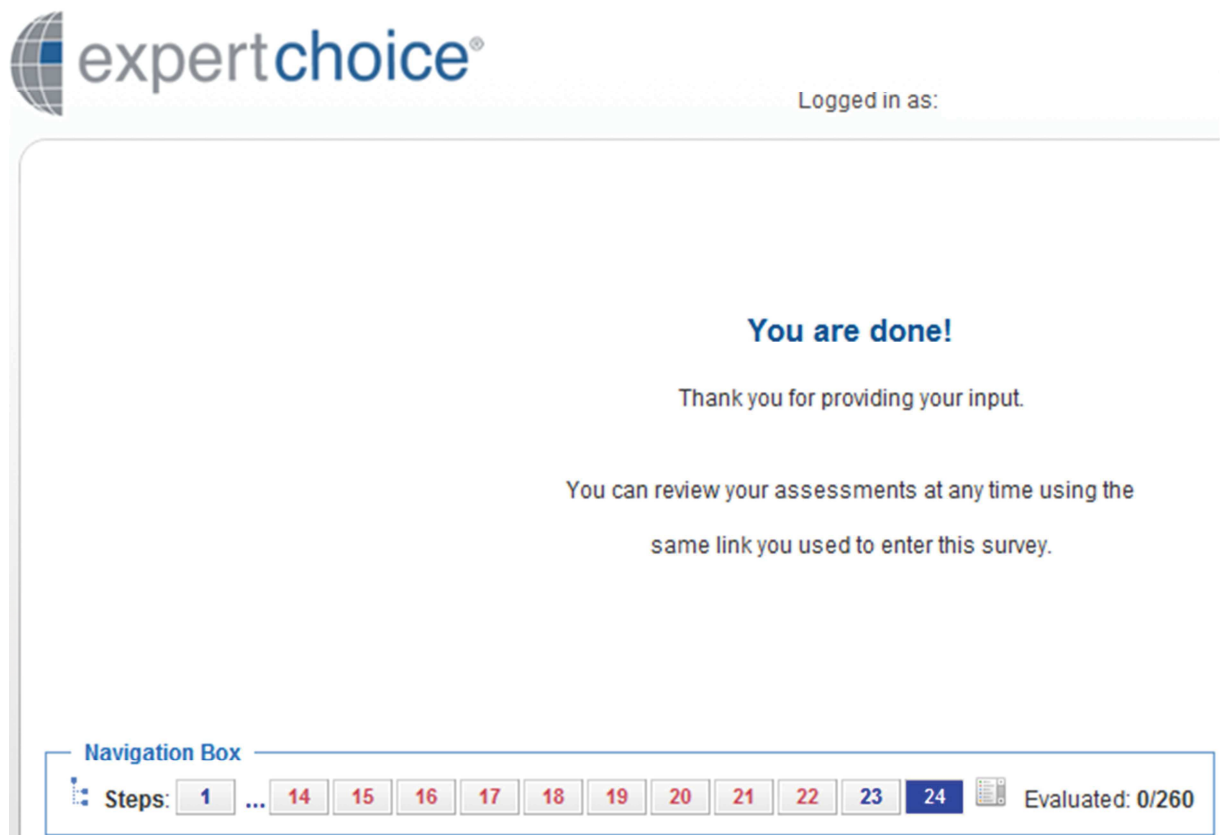
4 STEPS 23–24 – COMMENTS ON THE SURVEY AND END OF THE SURVEY

After the survey, the contributor is allowed to submit remarks on the survey. The comment input page is depicted in Figure A4.8. The end page of the survey is depicted in Figure A4.9.



The screenshot shows the expertchoice logo at the top left. Below it, a light blue header bar contains the text "Page 1". The main content area is a light blue box with the question "1. Do you have any comments on the survey?" followed by a text input field with up and down arrow icons on the right side.

Figure A4.8 Comment Page



The screenshot shows the expertchoice logo at the top left. To the right of the logo, the text "Logged in as:" is visible. The main content area is white and contains the following text: "You are done!" in bold blue, "Thank you for providing your input." in black, and "You can review your assessments at any time using the same link you used to enter this survey." in black. At the bottom, there is a "Navigation Box" with a list of steps: "Steps: 1 ... 14 15 16 17 18 19 20 21 22 23 24". The number 24 is highlighted in a dark blue box. To the right of the steps, there is a small icon and the text "Evaluated: 0/260".

Figure A4.9 End Page of the Survey

RESPONSES TO AHP-SURVEY

The survey was conducted in three parts identical in all respects except the framework scenarios. Out of 14 persons requested, 4 responded in full. 5 persons submitted partial assessments, which have been omitted from the presented results. Two participants assessed some of the items not applicable (NA) for performance measures of alternatives with respect to the assessment criteria in question. The assessments have been anonymized, with each participant number consistently referring to participants. Survey results are presented in Tables A5.1 and A5.2:

Table A5.1 Unnormalized Criteria Weights Submitted to Scenarios 1–3

Parent criteria assessed against	Prioritized sub-criteria	Scenario 1				Scenario 2				Scenario 3			
		Participant				Participant				Participant			
		1	2	3	4	1	2	3	4	1	2	3	4
Main criteria	Performance	0.76	0.50	0.44	0.70	0.49	0.79	0.90	1.00	0.77	0.86	0.86	0.72
	Capability	1.00	0.50	0.67	0.60	0.44	0.79	0.52	0.70	0.90	0.84	0.86	0.85
	Risk	0.50	0.81	0.84	0.90	0.00	0.10	0.19	0.20	0.88	0.91	0.89	0.84
Performance	Speed	1.00	0.30	0.84	0.60	0.15	0.20	0.75	0.81	0.96	0.03	0.45	0.45
	Efficiency	0.85	0.50	0.64	0.80	0.87	0.09	0.87	0.77	1.00	0.72	0.49	0.79
	Resolution	0.71	0.20	0.69	0.40	0.10	0.09	0.86	0.63	0.80	0.55	0.55	0.31
	Verifiability	0.46	0.22	0.33	0.60	0.10	0.16	0.79	0.55	0.16	0.86	0.80	0.27
	Validity	0.44	0.21	0.26	0.30	0.16	0.08	0.82	0.73	0.89	0.74	0.86	0.72
	Reliability	1.00	0.16	0.58	0.50	0.30	0.14	0.87	0.59	0.55	0.78	0.83	0.53
Capability	Technology	0.85	0.30	0.85	0.80	0.85	0.96	0.94	0.79	0.93	0.80	0.94	0.85
	Expertise	1.00	0.47	0.53	0.80	0.90	0.88	0.95	0.77	0.77	0.94	0.87	0.77
	Resources	0.62	0.20	0.69	0.60	0.10	0.60	0.89	0.46	0.80	0.82	0.85	0.77
	Leadership	1.00	0.10	0.45	0.80	0.44	0.46	0.80	0.61	0.89	0.92	0.84	0.68
	Support from other INTEL	0.82	0.03	0.33	0.30	0.10	0.03	0.80	0.30	0.72	0.54	0.55	0.33
Expertise	Technical	1.00	0.89	0.70	0.80	0.90	0.92	0.99	0.76	1.00	0.86	0.85	0.67
	Contextual	1.00	0.20	0.34	0.70	0.91	0.25	0.91	0.65	1.00	0.86	0.84	0.78
Risk	Jurisdiction	0.77	0.01	0.71	0.12	0.07	0.03	0.91	0.12	0.80	0.81	0.95	0.48
	Exposure of operative	0.36	0.74	0.63	0.86	0.10	0.50	0.91	0.53	0.92	0.73	0.83	0.78
	Exposure of method	0.42	0.65	0.51	0.60	0.52	0.25	0.80	0.25	0.75	0.75	0.87	0.80
	Exposure of target	0.48	0.67	0.52	0.46	0.10	0.50	0.87	0.43	0.91	0.66	0.85	0.47

Table A5.2 Method Assessments Submitted to Scenarios 1–3

			Participant				Participant				Participant				
Criterion	Method		1	2	3	4	1	2	3	4	1	2	3	4	
Performance	Speed	Cyber-OSINT	0.50	0.50	0.60	1.00	0.15	0.25	0.85	1.00	0.25	0.25	0.75	0.85	
		Scanning and enumeration	in public domain	0.25	0.90	0.60	0.85	0.50	0.25	0.85	0.90	0.90	0.25	0.75	0.90
			in restricted domain	NA	0.05	0.90	0.70	0.25	0.25	0.40	0.75	0.90	0.15	0.40	0.90
		Intrusion	0.25	0.25	0.70	0.50	0.50	0.15	0.65	0.75	0.50	0.20	0.45	0.80	
		Exploiting privileged information	0.55	0.05	0.45	0.90	0.25	0.10	0.60	0.85	0.75	0.20	0.60	0.95	
		Exfiltration of data	0.75	0.05	0.75	0.90	0.25	0.35	0.40	0.80	0.75	0.30	0.50	0.95	
		Obfuscation	0.50	0.05	0.40	0.45	0.45	0.35	0.30	0.50	0.75	0.30	0.45	0.45	
		Sustaining access	0.75	0.05	0.35	0.70	0.25	0.35	0.40	0.70	0.25	0.40	0.35	0.70	
		Network mapping	0.90	0.15	0.70	0.85	0.50	0.25	0.65	0.60	0.95	0.25	0.60	0.70	
		Social engineering	0.20	0.35	0.60	0.50	0.40	0.25	0.50	0.60	0.25	0.20	0.50	0.65	
		Physical surveillance	0.15	0.00	0.20	0.40	0.15	0.45	0.15	0.60	0.25	0.35	0.40	0.45	
		Network surveillance	0.50	0.00	0.55	0.65	0.75	0.15	0.35	0.55	0.90	0.25	0.55	0.60	
		Malware	0.55	0.10	0.65	0.60	0.35	0.50	0.40	0.50	0.25	0.50	0.60	0.85	
		Physical attack	0.15	0.25	0.30	0.65	0.10	0.80	0.05	0.45	0.25	0.65	0.35	0.45	
		Alterations in the supply chain	0.00	0.00	0.15	0.45	0.20	NA	0.10	0.20	0.25	0.00	0.15	0.20	
	Efficiency	Cyber-OSINT	0.40	0.75	0.60	1.00	0.30	0.65	0.55	1.00	0.25	0.75	0.75	0.55	
		Scanning and enumeration	in public domain	0.30	0.50	0.65	0.90	0.95	0.45	0.70	0.85	0.25	0.65	0.55	0.55
			in restricted domain	0.90	0.00	0.75	0.95	0.90	0.15	0.55	0.90	0.40	0.25	0.65	0.65
		Intrusion	1.00	0.05	0.70	0.80	0.95	0.25	0.60	0.75	0.75	0.45	0.65	0.80	
		Exploiting privileged information	0.95	0.05	0.65	1.00	0.50	0.25	0.55	0.85	0.75	0.45	0.70	0.95	
		Exfiltration of data	1.00	0.05	0.70	0.90	0.50	0.25	0.45	0.85	0.95	0.45	0.75	0.80	
		Obfuscation	0.60	0.05	0.45	0.75	0.50	0.25	0.40	0.55	0.50	0.45	0.60	0.40	
		Sustaining access	1.00	0.05	0.55	0.80	1.00	0.30	0.55	0.70	0.95	0.55	0.60	0.70	
		Network mapping	0.65	0.25	0.70	0.45	0.75	0.50	0.55	0.60	0.50	0.25	0.65	0.45	
		Social engineering	0.60	0.65	0.75	0.40	0.90	0.65	0.50	0.45	0.75	0.50	0.40	0.60	
		Physical surveillance	0.25	0.15	0.45	0.25	0.10	0.20	0.35	0.30	0.10	0.50	0.45	0.35	
		Network surveillance	0.85	0.00	0.65	0.55	0.95	0.20	0.30	0.40	0.50	0.50	0.65	0.65	
		Malware	0.70	0.15	0.55	0.80	1.00	0.35	0.40	0.40	1.00	0.50	0.65	0.70	
		Physical attack	0.00	0.25	0.40	0.35	0.00	0.55	0.05	0.20	0.05	0.70	0.45	0.20	
		Alterations in the supply chain	0.00	0.00	0.20	0.65	0.50	NA	0.05	0.10	0.25	0.00	0.35	0.25	
Resolution	Cyber-OSINT	0.25	0.55	0.55	0.35	0.25	0.60	0.85	0.45	0.25	0.75	0.65	0.65		
	Scanning and enumeration	in public domain	0.85	0.50	0.50	0.40	0.75	0.50	0.75	0.50	0.50	0.40	0.45	0.70	
		in restricted domain	0.85	0.05	0.75	0.55	0.75	0.10	0.50	0.60	0.70	0.55	0.60	0.80	
	Intrusion	1.00	0.10	0.60	0.75	1.00	0.60	0.60	0.70	0.90	0.75	0.70	0.90		
	Exploiting privileged information	0.75	0.05	0.65	0.90	1.00	0.60	0.55	0.75	0.90	0.75	0.70	0.90		
	Exfiltration of data	0.75	0.05	0.50	0.85	1.00	0.50	0.55	0.85	0.90	0.75	0.75	0.90		
	Obfuscation	0.75	0.05	0.45	0.45	0.80	0.25	0.40	0.45	0.75	0.55	0.60	0.40		
	Sustaining access	1.00	0.05	0.45	0.75	0.95	0.25	0.45	0.65	0.00	0.55	0.70	0.80		
	Network mapping	0.80	0.25	0.45	0.60	0.50	0.40	0.55	0.70	0.50	0.50	0.55	0.60		
	Social engineering	0.50	0.50	0.65	0.90	0.75	0.60	0.50	0.85	0.75	0.60	0.40	0.85		
	Physical surveillance	0.20	0.25	0.55	0.70	0.50	0.55	0.30	0.45	0.15	0.60	0.45	0.40		
	Network surveillance	0.60	0.00	0.55	0.75	0.50	0.20	0.45	0.65	0.50	0.55	0.55	0.55		
	Malware	0.75	0.20	0.65	0.70	0.90	0.45	0.45	0.80	0.95	0.70	0.65	0.80		
	Physical attack	0.00	0.10	0.55	0.80	0.25	0.10	0.30	0.20	0.05	0.10	0.45	0.30		
	Alterations in the supply chain	0.00	0.20	0.55	0.60	0.10	NA	0.15	0.10	0.15	0.05	0.40	0.35		

Verifiability	Cyber-OSINT			1.00	0.35	0.75	0.25	0.75	0.35	0.90	0.60	0.75	0.75	0.80	0.60	
	Scanning and enumeration	in public domain		1.00	0.25	0.70	0.40	0.75	0.85	0.90	0.70	0.50	0.65	0.80	0.65	
		in restricted domain		0.85	0.00	0.65	0.30	0.75	0.10	0.45	0.60	0.25	0.75	0.55	0.70	
	Intrusion			0.25	0.10	0.65	0.75	0.50	0.60	0.60	0.70	0.65	0.70	0.65	0.80	
	Exploiting privileged information			0.30	0.00	0.50	0.75	0.25	0.60	0.55	0.80	0.50	0.70	0.65	0.85	
	Exfiltration of data			0.10	0.05	0.55	0.70	0.25	0.55	0.55	0.90	0.25	0.70	0.55	0.85	
	Obfuscation			0.35	0.00	NA	0.35	0.25	0.35	0.40	0.40	0.50	0.25	0.50	0.40	
	Sustaining access			0.30	0.10	0.50	0.75	0.50	0.55	0.40	0.75	0.00	0.45	0.50	0.80	
	Network mapping			0.90	0.15	0.60	0.40	0.75	0.50	0.55	0.50	0.50	0.45	0.50	0.65	
	Social engineering			0.90	0.35	0.65	0.70	0.75	0.50	0.65	0.70	0.75	0.55	0.45	0.85	
	Physical surveillance			0.20	0.15	0.55	0.75	0.75	0.50	0.60	0.50	0.15	0.55	0.45	0.45	
	Network surveillance			0.70	0.00	0.55	0.70	0.75	0.45	0.60	0.50	0.45	0.35	0.45	0.55	
	Malware			0.85	0.25	0.55	0.65	0.75	0.45	0.55	0.85	0.50	0.20	0.55	0.75	
	Physical attack			0.35	0.25	0.50	0.65	0.75	0.70	0.45	0.30	0.05	0.80	0.45	0.30	
	Alterations in the supply chain			0.10	0.00	0.50	0.30	0.75	NA	0.45	0.10	0.25	0.05	0.45	0.15	
Performance	Validity	Cyber-OSINT			0.50	0.25	0.50	0.50	0.50	0.70	0.75	0.55	0.75	0.80	0.50	0.75
		Scanning and enumeration	in public domain		0.50	0.50	0.50	0.50	NA	0.75	0.65	0.60	0.50	0.65	0.55	0.75
			in restricted domain		0.50	0.05	0.45	0.65	NA	0.10	0.65	0.65	0.50	0.65	0.55	0.85
		Intrusion			0.50	0.25	0.45	0.90	NA	0.50	0.60	0.85	0.00	0.75	0.60	0.90
		Exploiting privileged information			1.00	0.25	0.60	0.90	0.75	0.35	0.55	0.85	0.95	0.75	0.65	0.95
		Exfiltration of data			1.00	0.25	0.60	0.90	0.75	0.25	0.45	0.85	0.95	0.75	0.65	0.90
		Obfuscation			0.50	0.25	NA	0.45	0.75	0.25	0.50	0.40	0.60	0.75	0.65	0.45
		Sustaining access			0.10	0.25	0.60	0.85	NA	0.25	0.50	0.75	0.00	0.75	0.60	0.75
		Network mapping			0.85	0.20	0.60	0.50	NA	0.45	0.55	0.50	0.50	0.45	0.50	0.65
		Social engineering			0.20	0.30	0.70	0.85	1.00	0.55	0.45	0.85	0.50	0.75	0.40	0.80
		Physical surveillance			0.75	0.05	0.45	0.85	0.25	0.45	0.40	0.55	0.20	0.55	0.50	0.30
		Network surveillance			0.75	0.00	0.60	0.70	0.75	0.25	0.45	0.65	0.50	0.40	0.65	0.35
		Malware			0.60	NA	0.55	0.85	NA	0.25	0.45	0.75	0.75	0.40	0.65	0.80
		Physical attack			0.25	0.05	0.45	0.65	NA	0.40	0.45	0.25	0.10	0.70	0.65	0.20
		Alterations in the supply chain			0.45	0.00	0.45	0.30	0.75	0.25	0.45	0.10	0.30	0.05	0.50	0.20
Reliability	Reliability	Cyber-OSINT			0.90	0.20	0.70	0.70	0.50	0.75	0.75	0.65	0.50	0.75	0.65	0.75
		Scanning and enumeration	in public domain		0.90	0.25	0.70	0.60	0.75	0.75	0.75	0.65	0.75	0.65	0.60	0.75
			in restricted domain		0.90	0.05	0.80	0.80	0.75	0.25	0.70	0.75	0.75	0.65	0.60	0.80
		Intrusion			0.90	0.05	0.80	0.85	NA	0.25	0.70	0.85	0.75	0.65	0.65	0.85
		Exploiting privileged information			0.90	0.15	0.70	0.85	0.75	0.25	0.65	0.85	0.75	0.65	0.65	0.85
		Exfiltration of data			0.60	0.10	0.75	0.90	0.75	0.40	0.65	0.80	0.90	0.65	0.65	0.85
		Obfuscation			0.70	0.15	NA	0.15	0.75	0.40	0.60	0.45	0.60	0.40	0.65	0.40
		Sustaining access			0.65	0.10	0.75	0.65	NA	0.35	0.60	0.80	0.00	0.70	0.65	0.80
		Network mapping			0.95	0.45	0.60	0.60	0.75	0.65	0.55	0.50	0.50	0.30	0.65	0.70
		Social engineering			0.95	0.35	0.45	0.80	0.90	0.50	0.40	0.80	0.75	0.50	0.40	0.85
		Physical surveillance			0.35	0.50	0.45	0.75	0.30	0.50	0.45	0.30	0.25	0.50	0.60	0.40
		Network surveillance			0.25	0.05	0.60	0.70	0.75	0.55	0.45	0.40	0.50	0.30	0.60	0.50
		Malware			0.35	0.05	0.55	0.85	NA	0.25	0.55	0.75	0.95	0.25	0.60	0.80
		Physical attack			0.20	0.15	0.45	0.60	NA	0.65	0.55	0.20	0.20	0.75	0.50	0.20
		Alterations in the supply chain			0.60	0.15	0.55	0.30	NA	0.10	0.55	0.05	0.50	0.00	0.50	0.20

Technology	Cyber-OSINT		0.85	0.50	0.90	0.85	0.75	0.75	0.95	1.00	1.00	0.75	1.00	1.00
	Scanning and enumeration	in public domain	0.85	0.60	0.85	0.80	0.75	0.75	0.85	0.90	1.00	0.75	0.95	0.95
		in restricted domain	0.60	0.25	0.40	0.85	0.25	0.80	0.80	0.80	0.85	0.95	0.95	0.95
	Intrusion		0.80	0.25	0.35	0.60	0.75	0.90	0.80	0.80	0.75	0.95	0.85	0.85
	Exploiting privileged information		0.90	0.25	0.35	0.85	0.75	0.90	0.65	0.90	0.95	0.85	0.90	0.95
	Exfiltration of data		0.95	0.20	0.45	0.85	0.75	0.60	0.60	0.85	0.95	0.85	0.85	0.95
	Obfuscation		0.70	0.25	0.15	0.50	0.75	0.75	0.45	0.70	0.95	0.90	0.75	0.80
	Sustaining access		0.85	0.25	0.20	0.65	0.50	0.80	0.40	0.70	0.75	0.90	0.65	0.85
	Network mapping		0.85	0.50	0.45	0.55	0.75	0.35	0.55	0.75	1.00	0.50	0.70	0.80
	Social engineering		0.85	0.35	0.50	0.75	0.50	0.55	0.55	0.35	0.75	0.75	0.50	0.60
	Physical surveillance		0.50	0.35	0.40	0.55	0.25	0.60	0.40	0.20	0.90	0.40	0.55	0.45
	Network surveillance		1.00	0.35	0.40	0.55	0.75	0.65	0.45	0.45	0.95	0.40	0.70	0.45
	Malware		1.00	0.30	0.30	0.40	0.90	0.75	0.55	0.45	1.00	0.95	0.75	0.75
	Physical attack		0.50	NA	0.45	0.85	0.25	NA	0.10	0.20	0.75	0.50	0.35	0.45
	Alterations in the supply chain		0.50	0.25	0.10	0.35	0.25	NA	0.10	0.10	0.75	0.05	0.45	0.45
Resources	Cyber-OSINT		0.75	0.75	0.65	0.90	0.75	0.95	0.75	0.90	1.00	0.90	1.00	0.80
	Scanning and enumeration	in public domain	0.75	0.50	0.65	0.65	0.75	0.75	0.70	0.90	1.00	0.40	0.90	0.95
		in restricted domain	0.15	0.25	0.60	0.55	0.75	0.75	0.50	0.70	0.90	0.60	0.90	0.85
	Intrusion		0.80	0.25	0.40	0.55	0.75	0.70	0.45	0.70	0.75	0.75	0.75	0.85
	Exploiting privileged information		0.80	0.25	0.40	0.85	0.75	0.55	0.45	0.90	0.75	0.75	0.75	1.00
	Exfiltration of data		0.90	0.25	0.35	0.85	0.75	0.55	0.45	0.90	0.75	0.40	0.75	1.00
	Obfuscation		0.90	0.25	0.20	0.45	0.75	0.35	0.30	0.70	0.75	0.40	0.75	0.75
	Sustaining access		0.90	0.25	0.20	0.50	0.75	0.60	0.40	0.75	0.75	0.60	0.75	0.85
	Network mapping		0.90	0.35	0.35	0.55	0.75	0.50	0.45	0.60	0.75	0.25	0.75	0.80
	Social engineering		0.95	0.55	0.40	0.70	0.75	0.60	0.45	0.40	0.75	0.60	0.65	0.50
	Physical surveillance		0.10	0.55	0.30	0.45	0.25	0.75	0.40	0.20	0.75	0.65	0.70	0.45
	Network surveillance		0.80	0.55	0.30	0.45	0.75	0.25	0.45	0.50	0.75	0.65	0.70	0.60
	Malware		0.95	0.25	0.20	0.35	0.75	0.25	0.40	0.30	0.75	0.70	0.80	0.50
	Physical attack		0.05	NA	0.20	0.45	0.10	0.95	0.20	0.10	0.75	0.70	0.60	0.10
	Alterations in the supply chain		0.15	0.05	0.10	0.20	0.25	NA	0.15	0.10	0.75	0.25	0.50	0.10
Leadership	Cyber-OSINT		0.85	0.75	0.60	0.90	0.95	0.85	0.55	0.90	0.90	0.90	0.75	0.90
	Scanning and enumeration	in public domain	0.75	0.50	0.65	0.90	0.75	0.85	0.45	0.90	0.95	0.75	0.75	0.95
		in restricted domain	0.25	0.50	0.45	0.90	0.75	0.85	0.35	0.90	0.95	0.80	0.75	0.85
	Intrusion		0.65	0.60	0.35	0.85	0.75	0.85	0.35	0.80	1.00	0.80	0.70	0.90
	Exploiting privileged information		0.75	0.60	0.35	0.90	0.75	0.55	0.40	0.90	1.00	0.90	0.70	0.95
	Exfiltration of data		0.90	0.60	0.35	0.85	0.75	0.45	0.40	0.90	1.00	0.55	0.70	0.95
	Obfuscation		0.90	0.25	0.20	0.75	0.75	0.45	0.30	0.75	1.00	0.50	0.70	0.85
	Sustaining access		0.90	0.35	0.15	0.75	0.75	0.60	0.25	0.75	1.00	0.75	0.70	0.90
	Network mapping		0.90	0.40	0.35	0.70	0.75	0.50	0.40	0.75	1.00	0.25	0.70	0.85
	Social engineering		0.90	0.60	0.40	0.65	0.75	0.45	0.35	0.50	0.90	0.25	0.55	0.75
	Physical surveillance		0.60	0.55	0.40	0.85	0.75	0.45	0.35	0.50	1.00	0.50	0.70	0.70
	Network surveillance		0.90	0.15	0.35	0.80	0.75	0.65	0.45	0.60	1.00	0.25	0.70	0.85
	Malware		0.95	0.15	0.20	0.80	0.75	0.10	0.30	0.65	1.00	0.50	0.75	0.75
	Physical attack		0.30	0.70	0.20	0.75	0.75	0.90	0.15	0.55	1.00	0.90	0.60	0.50
	Alterations in the supply chain		0.60	0.15	0.10	0.80	0.75	0.05	0.05	0.45	1.00	0.25	0.50	0.60

Capability					Support from other INTEL																			
					Cyber-OSINT	Scanning and enumeration	in public domain	in restricted domain	0.75				0.85				0.65				0.90			
									0.75	0.85	0.65	0.90	0.75	0.85	0.65	0.90	1.00	0.50	1.00	0.95				
Expertise	Technical	Cyber-OSINT	Scanning and enumeration	in public domain	in restricted domain	0.60	0.90	0.85	0.90	0.80	0.75	0.90	1.00	1.00	0.80	1.00	0.95							
						0.80	0.75	0.70	0.75	0.75	0.75	0.90	0.85	1.00	0.75	0.90	0.95							
						0.80	0.70	0.45	0.80	0.75	0.80	0.70	0.80	0.95	0.95	0.80	0.90							
		Intrusion	1.00	0.65	0.45	0.60	0.75	0.90	0.60	0.70	1.00	0.95	0.80	0.85										
		Exploiting privileged information	0.90	0.65	0.40	0.85	0.75	0.90	0.50	0.85	1.00	0.75	0.75	0.95										
		Exfiltration of data	0.90	0.45	0.40	0.85	0.75	0.75	0.50	0.80	1.00	0.75	0.80	0.95										
		Obfuscation	0.80	0.60	0.25	0.35	0.75	0.85	0.55	0.65	1.00	0.85	0.65	0.80										
		Sustaining access	1.00	0.65	0.20	0.70	0.75	0.80	0.45	0.65	1.00	0.85	0.70	0.80										
		Network mapping	1.00	0.50	0.45	0.55	0.75	0.15	0.60	0.55	1.00	0.20	0.70	0.80										
		Social engineering	0.80	0.40	0.45	0.80	0.50	0.60	0.45	0.30	0.90	0.50	0.55	0.65										
		Physical surveillance	0.60	0.20	0.30	0.55	0.25	0.60	0.45	0.20	1.00	0.15	0.65	0.45										
		Network surveillance	1.00	0.15	0.40	0.60	0.60	0.60	0.45	0.55	1.00	0.35	0.80	0.50										
		Malware	1.00	0.50	0.30	0.45	0.90	0.75	0.40	0.45	1.00	0.90	0.80	0.50										
		Physical attack	0.50	NA	0.35	0.65	0.25	NA	0.25	0.10	1.00	0.25	0.65	0.40										
		Alterations in the supply chain	0.55	0.25	0.10	0.30	0.50	NA	0.05	0.05	1.00	0.00	0.50	0.45										
	Contextual	Cyber-OSINT	Scanning and enumeration	in public domain	in restricted domain	0.50	0.90	0.65	1.00	1.00	0.75	0.75	0.80	0.95	0.90	0.85	0.95							
						0.05	0.40	0.60	0.75	0.15	0.50	0.65	0.70	0.95	0.55	0.85	0.85							
						0.05	0.15	0.45	0.75	0.10	0.50	0.55	0.70	0.95	0.55	0.80	0.90							
		Intrusion	0.05	0.25	0.55	0.75	0.10	0.15	0.55	0.75	0.00	0.60	0.80	0.85										
		Exploiting privileged information	0.75	0.25	0.40	0.90	0.10	0.15	0.45	0.80	0.95	0.75	0.75	0.90										
		Exfiltration of data	0.75	0.25	0.45	0.90	0.75	0.15	0.55	0.85	0.95	0.75	0.80	0.95										
		Obfuscation	0.75	0.25	0.25	0.65	0.60	0.15	0.60	0.70	0.95	0.50	0.65	0.50										
		Sustaining access	0.10	0.25	0.25	0.80	0.05	0.15	0.40	0.70	0.00	0.30	0.70	0.85										
		Network mapping	0.05	0.50	0.40	0.80	0.00	0.15	0.55	0.60	0.00	0.25	0.70	0.70										
		Social engineering	0.05	0.50	0.40	0.85	1.00	0.50	0.45	0.40	1.00	0.75	0.60	0.65										
		Physical surveillance	0.05	0.50	0.45	0.75	0.05	0.50	0.45	0.30	0.95	0.40	0.40	0.50										
		Network surveillance	0.05	0.25	0.40	0.75	0.75	0.30	0.55	0.45	0.00	0.40	0.75	0.60										
Malware	0.80	0.15	0.35	0.50	0.00	0.15	0.55	0.45	0.00	0.15	0.60	0.65												
Physical attack	0.00	NA	0.45	0.80	0.00	NA	0.45	0.20	0.75	0.15	0.50	0.30												
Alterations in the supply chain	0.20	0.15	0.15	0.35	0.10	NA	0.45	0.10	0.75	0.85	0.50	0.25												

Risk	Jurisdiction	Cyber-OSINT		NA	0.10	0.95	1.00	NA	0.15	1.00	1.00	1.00	0.20	1.00	1.00
		Scanning and enumeration	in public domain	0.90	0.10	0.40	0.90	0.25	0.15	0.75	1.00	0.75	0.25	0.75	0.95
			in restricted domain	0.90	0.10	0.45	0.85	0.20	0.15	0.75	0.90	0.50	0.80	0.75	0.80
		Intrusion		0.90	0.10	0.35	0.80	0.25	0.15	0.75	0.90	0.75	0.90	0.70	0.60
		Exploiting privileged information		0.90	0.10	0.40	0.90	0.25	0.15	0.75	0.95	0.75	0.95	0.75	0.60
		Exfiltration of data		0.90	0.10	0.45	0.90	0.25	0.15	0.75	0.95	0.75	0.90	0.75	0.80
		Obfuscation		0.60	0.10	0.45	0.85	0.25	0.00	0.50	0.95	0.75	0.50	0.75	0.60
		Sustaining access		0.85	0.10	0.40	0.75	0.25	0.15	0.55	0.90	0.75	0.85	0.75	0.60
		Network mapping		0.85	0.10	0.35	0.80	0.25	0.00	0.55	0.95	0.75	0.40	0.75	0.70
		Social engineering		0.30	0.10	0.60	0.70	0.25	0.15	0.75	0.75	0.75	0.25	0.75	0.60
		Physical surveillance		0.30	0.10	0.30	0.85	0.25	0.45	0.75	0.25	0.75	0.25	0.75	0.70
		Network surveillance		0.30	0.10	0.30	0.80	0.25	0.10	0.75	0.85	0.75	0.25	0.75	0.70
		Malware		0.90	0.10	0.30	0.75	0.25	0.10	0.60	0.90	0.75	0.85	0.75	0.50
		Physical attack		1.00	0.10	0.20	0.50	0.25	0.45	0.45	0.15	0.10	0.95	0.45	0.10
		Alterations in the supply chain		1.00	0.10	0.30	0.45	0.25	0.10	0.50	0.35	0.75	0.25	0.45	0.25
	Exposure of operative	Cyber-OSINT		1.00	0.15	1.00	1.00	0.75	0.65	1.00	1.00	1.00	0.15	1.00	1.00
		Scanning and enumeration	in public domain	0.75	0.75	0.45	0.90	0.75	0.60	0.75	1.00	0.75	0.20	0.75	0.95
			in restricted domain	0.50	0.95	0.40	0.65	0.75	0.90	0.55	0.75	0.50	0.70	0.50	0.85
		Intrusion		0.25	0.85	0.40	0.55	0.75	0.85	0.45	0.65	0.50	0.65	0.40	0.75
		Exploiting privileged information		0.25	0.85	0.35	0.65	0.75	0.85	0.50	0.75	0.50	0.75	0.40	0.85
		Exfiltration of data		0.85	0.85	0.45	0.75	0.75	0.70	0.45	0.80	0.50	0.75	0.40	0.85
		Obfuscation		0.65	0.55	0.70	1.00	0.70	0.55	0.45	0.80	0.50	0.45	0.60	0.85
		Sustaining access		0.90	0.80	0.65	0.50	0.95	0.75	0.35	0.65	0.50	0.70	0.60	0.70
		Network mapping		1.00	0.50	0.55	0.80	0.90	0.55	0.65	0.80	0.75	0.20	0.50	0.85
		Social engineering		0.50	0.50	0.50	0.40	0.75	0.65	0.40	0.50	0.75	0.20	0.50	0.50
		Physical surveillance		0.90	0.35	0.45	0.50	0.55	0.65	0.50	0.50	0.75	0.20	0.50	0.60
		Network surveillance		0.50	0.40	0.45	0.50	0.70	0.45	0.50	0.75	0.75	0.20	0.50	0.70
		Malware		1.00	0.80	0.40	0.45	0.90	0.85	0.40	0.65	0.50	0.75	0.35	0.60
		Physical attack		0.20	0.95	0.25	0.20	0.10	0.90	0.20	0.15	0.05	0.75	0.25	0.10
		Alterations in the supply chain		0.75	0.50	0.55	0.20	0.10	0.50	0.50	0.25	0.50	0.00	0.45	0.20
	Exposure of method	Cyber-OSINT		1.00	0.45	0.90	1.00	NA	0.45	1.00	1.00	1.00	0.10	1.00	1.00
		Scanning and enumeration	in public domain	1.00	0.85	0.70	1.00	0.50	0.80	0.65	1.00	1.00	0.20	0.75	0.95
			in restricted domain	1.00	0.95	0.45	0.95	0.50	0.85	0.35	0.90	1.00	0.90	0.45	0.85
		Intrusion		0.75	0.85	0.40	0.80	0.75	0.85	0.45	0.70	0.95	0.90	0.45	0.75
		Exploiting privileged information		0.50	0.85	0.40	0.80	0.90	0.85	0.50	0.75	0.95	0.90	0.45	0.85
		Exfiltration of data		0.50	0.75	0.35	0.85	0.90	0.45	0.45	0.75	0.90	0.75	0.45	0.85
		Obfuscation		0.75	0.50	0.60	0.95	0.85	0.60	0.65	0.85	0.90	0.60	0.65	0.70
		Sustaining access		0.75	0.75	0.45	0.65	0.95	0.80	0.45	0.60	0.75	0.75	0.65	0.70
		Network mapping		0.75	0.70	0.45	0.75	0.75	0.80	0.45	0.80	0.80	0.30	0.45	0.75
		Social engineering		1.00	0.65	0.55	0.45	0.95	0.50	0.35	0.45	0.80	0.25	0.45	0.50
		Physical surveillance		1.00	0.65	0.35	0.40	0.35	0.50	0.55	0.45	0.80	0.25	0.45	0.60
		Network surveillance		0.75	0.65	0.45	0.60	0.75	0.65	0.45	0.70	0.75	0.25	0.45	0.70
		Malware		0.75	0.90	0.40	0.55	0.95	0.90	0.45	0.65	0.75	0.90	0.40	0.60
		Physical attack		0.00	1.00	0.10	0.10	0.10	1.00	0.30	0.10	0.75	1.00	0.30	0.15
		Alterations in the supply chain		0.50	NA	0.40	0.15	0.75	0.25	0.45	0.20	0.75	0.00	0.45	0.20

Risk	Exposure of target	Cyber-OSINT				1.00	0.55	1.00	1.00	NA	0.40	1.00	1.00	1.00	0.10	1.00	1.00
		Scanning and enumeration		in public domain		0.25	0.80	0.45	0.95	0.75	0.60	0.50	0.95	1.00	0.20	0.75	0.95
				in restricted domain		0.25	0.90	0.40	0.70	0.75	0.90	0.25	0.90	0.75	0.85	0.45	0.90
		Intrusion				0.75	0.85	0.40	0.70	0.95	0.75	0.30	0.75	0.50	0.90	0.40	0.75
		Exploiting privileged information				0.75	0.80	0.35	0.85	0.95	0.65	0.40	0.85	0.50	0.90	0.40	0.85
		Exfiltration of data				0.75	0.50	0.35	0.80	0.95	0.65	0.35	0.85	0.50	0.75	0.40	0.85
		Obfuscation				0.75	0.25	0.55	0.95	0.75	0.35	0.40	0.95	0.50	0.35	0.75	0.80
		Sustaining access				0.50	0.85	0.40	0.60	1.00	0.75	0.40	0.65	0.50	0.95	0.50	0.70
		Network mapping				0.75	0.80	0.45	0.90	0.75	0.70	0.45	0.70	0.75	0.15	0.50	0.80
		Social engineering				0.50	0.60	0.45	0.50	0.75	0.40	0.35	0.50	0.75	0.35	0.45	0.50
		Physical surveillance				0.75	0.65	0.60	0.60	0.50	0.40	0.40	0.60	0.75	0.15	0.45	0.60
		Network surveillance				0.50	0.30	0.40	0.70	0.80	0.15	0.60	0.65	0.75	0.10	0.55	0.65
		Malware				0.80	0.85	0.45	0.55	0.90	0.75	0.45	0.65	0.50	0.85	0.40	0.55
		Physical attack				0.00	0.80	0.15	0.15	0.05	0.95	0.35	0.10	0.05	1.00	0.25	0.10
		Alterations in the supply chain				0.75	NA	0.45	0.25	0.95	0.25	0.45	0.20	0.50	0.25	0.45	0.25

RESULTS OF AHP SURVEY

The computed priorities of the cyber intelligence acquisition methods and normalized local and global weights of the assessment criteria are presented in Tables A6.1–3. In calculating the values, data points deemed ‘Not Applicable’ by the participant were excluded from the data grid. The data is presented in Ideal Mode, meaning that it “preserves rank by dividing the score of each alternative only by the score of the best alternative under each criterion,”[107] and unnormalized, meaning that “the priority is the sum of the products of each covering objective's global priority times the priority of the alternative with respect to each covering objective” [8]:

$$T = \sum_{i=0}^n a_i g_i$$

Where :

T = Total priority

n = number of objective

a_i = Ratio score for the alternative on the i th objective

g_i = Global priority score for the the i th objective

Table A6.1 Criteria Weights and Method Priorities for Scenario 1

			Criteria															
			Performance						Capability					Risk				
			Speed	Efficiency	Resolution	Verifiability	Validity	Reliability	Technology	Expertise		Resources	Leadership	Support from other INTEL	Jurisdiction	Exposure of operative	Exposure of method	Exposure of target
										Contextual	Technical							
Criteria weight	Local	0.218	0.218	0.158	0.129	0.099	0.178	0.242	0.600	0.400	0.182	0.202	0.131	0.190	0.300	0.260	0.250	
	Global	0.063	0.063	0.046	0.037	0.029	0.052	0.082	0.049	0.033	0.062	0.069	0.045	0.070	0.111	0.096	0.093	
Method	Total priority	Criteria priority																
Cyber-OSINT	0.734	0.650	0.688	0.425	0.587	0.438	0.625	0.775	0.813	0.762	0.763	0.775	0.788	0.683	0.788	0.837	0.887	
Scanning and enumeration in public domain	0.673	0.783	0.587	0.563	0.588	0.500	0.612	0.775	0.750	0.450	0.637	0.700	0.625	0.575	0.712	0.887	0.613	
Scanning and enumeration in restricted domain	0.574	0.412	0.650	0.550	0.450	0.412	0.637	0.525	0.688	0.350	0.387	0.525	0.638	0.575	0.625	0.838	0.563	
Intrusion	0.573	0.425	0.637	0.613	0.438	0.525	0.650	0.500	0.675	0.400	0.500	0.613	0.625	0.538	0.512	0.700	0.675	
Exploiting privileged information	0.601	0.487	0.663	0.587	0.387	0.688	0.650	0.587	0.700	0.575	0.575	0.650	0.625	0.575	0.525	0.637	0.688	
Exfiltration of data	0.622	0.612	0.663	0.538	0.350	0.688	0.587	0.612	0.650	0.587	0.587	0.675	0.733	0.587	0.725	0.613	0.600	
Obfuscation	0.516	0.350	0.463	0.425	0.233	0.400	0.333	0.400	0.500	0.475	0.450	0.525	0.667	0.500	0.725	0.700	0.625	
Sustaining access	0.560	0.462	0.600	0.563	0.412	0.450	0.538	0.488	0.637	0.350	0.463	0.538	0.650	0.525	0.712	0.650	0.587	
Network mapping	0.608	0.650	0.512	0.525	0.512	0.538	0.650	0.587	0.625	0.438	0.538	0.587	0.637	0.525	0.712	0.663	0.725	
Social engineering	0.574	0.413	0.600	0.637	0.650	0.513	0.637	0.613	0.613	0.450	0.650	0.637	0.800	0.425	0.475	0.663	0.512	
Physical surveillance	0.476	0.188	0.275	0.425	0.413	0.525	0.512	0.450	0.413	0.438	0.350	0.600	0.663	0.388	0.550	0.600	0.650	
Network surveillance	0.493	0.425	0.512	0.475	0.488	0.512	0.400	0.575	0.538	0.363	0.525	0.550	0.475	0.375	0.462	0.612	0.475	
Malware	0.560	0.475	0.550	0.575	0.575	0.667	0.450	0.500	0.563	0.450	0.438	0.525	0.563	0.512	0.663	0.650	0.663	
Physical attack	0.388	0.338	0.250	0.363	0.438	0.350	0.350	0.600	0.500	0.417	0.233	0.488	0.538	0.450	0.400	0.300	0.275	
Alterations in the supply chain	0.344	0.150	0.212	0.338	0.225	0.300	0.400	0.300	0.300	0.213	0.125	0.413	0.413	0.463	0.500	0.350	0.483	

Table A6.2 Criteria Weights and Method Priorities for Scenario 2

			Criteria															
			Performance						Capability					Risk				
			Speed	Efficiency	Resolution	Verifiability	Validity	Reliability	Technology	Expertise		Resources	Leadership	Support from other INTEL	Jurisdiction	Exposure of operative	Exposure of method	Exposure of target
Technical	Contextual																	
	Criteria weight	Local	0.166	0.227	0.146	0.140	0.156	0.166	0.280	0.567	0.433	0.162	0.183	0.098	0.164	0.296	0.264	0.275
		Global	0.087	0.118	0.076	0.073	0.081	0.086	0.112	0.063	0.048	0.065	0.073	0.039	0.013	0.023	0.021	0.022
Method	Total priority	Criteria priority																
Cyber-OSINT	0.717	0.563;0.625;0.538;0.650;0.625;0.663;0.863;0.862;0.825;0.837;0.813;0.788;0.717;0.850;0.817;0.800																
Scanning and enumeration in public domain	0.711	0.625;0.737;0.625;0.800;0.667;0.725;0.813;0.813;0.500;0.775;0.737;0.538;0.538;0.775;0.737;0.700																
Scanning and enumeration in restricted domain	0.586	0.412;0.625;0.488;0.475;0.467;0.613;0.662;0.762;0.463;0.675;0.712;0.538;0.500;0.738;0.650;0.700																
Intrusion	0.647	0.512;0.638;0.725;0.600;0.650;0.600;0.813;0.738;0.387;0.650;0.688;0.613;0.512;0.675;0.688;0.688																
Exploiting privileged information	0.621	0.450;0.538;0.725;0.550;0.625;0.625;0.800;0.750;0.375;0.663;0.650;0.487;0.525;0.712;0.750;0.712																
Exfiltration of data	0.606	0.450;0.513;0.725;0.563;0.575;0.650;0.700;0.700;0.575;0.663;0.625;0.463;0.525;0.675;0.637;0.700																
Obfuscation	0.515	0.400;0.425;0.475;0.350;0.475;0.550;0.663;0.700;0.512;0.525;0.563;0.388;0.425;0.625;0.737;0.613																
Sustaining access	0.562	0.425;0.637;0.575;0.550;0.500;0.583;0.600;0.663;0.325;0.625;0.587;0.400;0.463;0.675;0.700;0.700																
Network mapping	0.555	0.500;0.600;0.538;0.575;0.500;0.613;0.600;0.512;0.325;0.575;0.600;0.425;0.438;0.725;0.700;0.650																
Social engineering	0.578	0.438;0.625;0.675;0.650;0.712;0.650;0.487;0.462;0.588;0.550;0.513;0.675;0.475;0.575;0.563;0.500																
Physical surveillance	0.409	0.338;0.237;0.450;0.587;0.413;0.387;0.363;0.375;0.325;0.400;0.513;0.663;0.425;0.550;0.463;0.475																
Network surveillance	0.520	0.450;0.463;0.450;0.575;0.525;0.538;0.575;0.550;0.512;0.488;0.612;0.400;0.488;0.600;0.637;0.550																
Malware	0.542	0.438;0.538;0.650;0.650;0.483;0.517;0.663;0.625;0.288;0.425;0.450;0.488;0.463;0.700;0.737;0.688																
Physical attack	0.335	0.350;0.200;0.212;0.550;0.367;0.467;0.183;0.200;0.217;0.338;0.587;0.488;0.325;0.338;0.375;0.363																
Alterations in the supply chain	0.251	0.167;0.217;0.117;0.433;0.388;0.233;0.150;0.200;0.217;0.167;0.325;0.350;0.300;0.338;0.413;0.463																

Table A6.3 Criteria Weights and Method Priorities for Scenario 3

			Criteria															
			Performance						Capability					Risk				
									Technology	Expertise		Resources	Leadership	Support from other INTEL	Jurisdiction	Exposure of operative	Exposure of method	Exposure of target
			Contextual	Technical														
	Criteria weight	Local	0.125	0.199	0.147	0.139	0.213	0.178	0.226	0.493	0.507	0.208	0.214	0.138	0.246	0.264	0.257	0.234
		Global	0.039	0.063	0.046	0.044	0.067	0.056	0.076	0.036	0.037	0.070	0.072	0.047	0.085	0.091	0.089	0.081
Method	Total priority	Criteria priority																
Cyber-OSINT	0.777	0.525;0.575;0.575;0.725;0.700;0.663;0.938;0.938;0.912;0.925;0.862;0.863;0.800;0.788;0.775;0.775																
Scanning and enumeration in public domain	0.718	0.700;0.500;0.512;0.650;0.613;0.688;0.913;0.900;0.800;0.813;0.850;0.775;0.675;0.663;0.725;0.725																
Scanning and enumeration in restricted domain	0.733	0.587;0.487;0.663;0.563;0.638;0.700;0.925;0.900;0.800;0.813;0.837;0.900;0.712;0.638;0.800;0.737																
Intrusion	0.719	0.488;0.663;0.813;0.700;0.563;0.725;0.850;0.900;0.563;0.775;0.850;0.925;0.737;0.575;0.762;0.637																
Exploiting privileged information	0.774	0.625;0.713;0.813;0.675;0.825;0.725;0.912;0.863;0.837;0.813;0.887;0.925;0.763;0.625;0.788;0.663																
Exfiltration of data	0.757	0.625;0.738;0.825;0.587;0.813;0.762;0.900;0.875;0.863;0.725;0.800;0.925;0.800;0.625;0.737;0.625																
Obfuscation	0.639	0.488;0.487;0.575;0.412;0.613;0.512;0.850;0.825;0.650;0.663;0.763;0.688;0.650;0.600;0.713;0.600																
Sustaining access	0.660	0.425;0.700;0.512;0.438;0.525;0.537;0.788;0.837;0.463;0.737;0.837;0.750;0.737;0.625;0.713;0.663																
Network mapping	0.597	0.625;0.462;0.538;0.525;0.525;0.538;0.750;0.675;0.412;0.637;0.700;0.737;0.650;0.575;0.575;0.550																
Social engineering	0.594	0.400;0.563;0.650;0.650;0.613;0.625;0.650;0.650;0.750;0.625;0.613;0.837;0.587;0.488;0.500;0.512																
Physical surveillance	0.531	0.363;0.350;0.400;0.400;0.387;0.438;0.575;0.563;0.563;0.637;0.725;0.875;0.613;0.513;0.525;0.487																
Network surveillance	0.570	0.575;0.575;0.537;0.450;0.475;0.475;0.625;0.663;0.438;0.675;0.700;0.688;0.613;0.538;0.538;0.513																
Malware	0.663	0.550;0.713;0.775;0.500;0.650;0.650;0.863;0.800;0.350;0.688;0.750;0.688;0.712;0.550;0.663;0.575																
Physical attack	0.459	0.425;0.350;0.225;0.400;0.413;0.413;0.512;0.575;0.425;0.538;0.750;0.788;0.400;0.287;0.550;0.350																
Alterations in the supply chain	0.376	0.150;0.213;0.238;0.225;0.263;0.300;0.425;0.488;0.587;0.400;0.587;0.775;0.425;0.287;0.350;0.363																