SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Components of defence strategies in society's information environment: a case study based on the grounded theory

Erja Birgitta Mustonen-Ollila[1], Martti Lehto[2], Jukka Heikkonen[3]

[1] erja.mustonen-ollila@quicknet.inet.fi

[1] https://orcid.org/0000-0002-0535-3943

[1, 2] Faculty of Information Technology, University of Jyväskylä, Finland

[2] https://orcid.org/0000-0002-8122-3155

[3] https://orcid.org/0000-0002-2468-5708

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

Abstract

The goal of this study is to explore the components of defence strategies faced by society in its information environment, and how these strategies are inter-related. This qualitative in-depth case study applied past research and empirical evidence to identify the components of defence strategies in a society's information environment. The data collected was analysed using the Grounded Theory approach and a conceptual framework with the components of defence strategies and the relationships between these components was developed using the Grounded Theory. This study shows that the goal of politically and militarily hostile actors is to weaken society's information environment, and that their operations are coordinated and carried out over a long time period. The data validates past studies and reveals relationships between the components of defence strategies. These relationships increase confidence in the validity of these components and their relationships, and expand the emerging theory. First, the data and findings showed 16 inter-connected components of defence strategies. Second, they showed that the political, military, societal, power, and personal goals of the hostile actors carrying out cyber operations and cyber attacks are to weaken society's information environment. Third, they revealed that cyber operations and cyber attacks against networks, information and infrastructures are coordinated operations, carried out over a long time period. Finally, it was revealed that the actors defending society's information environment must rapidly change their own components of defence strategies and use the newest tools and methods for these components in networks, infrastructures and social media.

Keywords:

oil, energy security, maritime campaigns

Article info
Received: 2 December 2019
Revised: 7 February 2020
Accepted: 13 February 2020
Available online: 17 March 2020
DOI: http://doi.org/10.35467/sdq/118186

© 2020 E. B. Mustonen-Ollila, M. Lehto, J. Heikkonen published by War Studies University, Poland.
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License

Introduction

The goal of this study is to detect and prevent harmful attacks and operations in society's information environment, and to secure, protect, defend and maintain society's vital functions, activities and information (The Security and Defence Committee, 2006). The components of defence strategies vary according to whether attacks are physical or whether they are operations against state dependency. Society must be defended against false or incorrect information that can cause harm. Society needs to defend itself against cyber operations and cyber attacks, the goals of which are to damage society's critical infrastructure or critical information. Counter-defence strategies are also needed in society's information environment to recognise and identify operations and attacks at different levels, that is, at the state, society, organisational, company, technical, legislative, security, individual, and international levels. Information confidentiality, integrity and availability must be protected at all these levels.

In this study, information environment (IE) is defined as "Information, aggregate of individuals, organisations and systems that receive, collect, process and convey/disseminate the information, or act on information, and the cognitive, virtual and physical space in which this occurs" (NATO, 2012 p. 3, Armistead and United States and Joint Forces Staff College, 2004 pp. 13–20), and includes both military and non-military information operations (IO) and information warfare (IW) (The Security and Defence Committee, 2006).

The focus of this study is on society's IEs, and a society is defined as "a group of individuals involved in persistent social interaction, or a large social group sharing the same geographical or social territory, typically subject to the same political authority and dominant cultural expectations" (Society, 2020).

Although previous studies (Lehto *et al.*, 2017, Nimmo, 2015, Pomerantsev, 2015, Sigholm, 2013, p. 51, Mäntylä, 2014, Joint Chiefs of Staff, 2013, Armistead *et al.*, 2004 pp. 13–20, Schechtman, 1996) have shown that a great deal of components of defence strategies exist in societies' IE, qualitative research of the origins of components of defence strategies and how a society becomes aware of these is lacking. In order to obtain a clear understanding of their influence, components of defence strategies must be examined in a real society. Such an investigation would improve the ability to understand the possible new approaches of future components of defence strategies. This study tackles these issues.

Past studies and empirical evidence were applied in this qualitative in-depth case study (Benbasat *et al.*, 1987, Yin, 2003), which identifies the components of defence strategies in a society's IE. The data collected was analysed using the Grounded Theory (GT) approach, and a conceptual framework was developed with components of defence strategies and the relationships between them (Glaser and Strauss, 1967). The goal of this study was to explore the components of defence strategies of a society's IE, the extent to which these components of defence strategies are shaped by the IE context, and how these components of defence strategies are inter-related.

The study made 146 components of defence strategy observations supported by empirical evidence, and these observations were categorised using GT analysis (Glaser and Strauss, 1967). The analysis revealed 16 components of defence strategies as follows: Total Defence, Operative Capability, Cyber Defence, Defence against Cyber Space Operations, Critical Infrastructure Protection (CIP), Cyber Capability, Observation-Orientation-Decision-Action (OODA) Defence, Espionage, Cyber Intelligence, Counter Intelligence, Information Security and Defence, Information Security Breach Investigation, Recognition Primed Decision Model of Rapid Decision Making (RPD Model),

Defence with Law, Non-Physical Network Defence, and Strategic Communications (StratCom). These components of defence strategies were inter-related, and 9 higher levels of abstraction of statements based on the conceptual framework, propositions for components of defence strategies, and their relationships between the components of defence strategies were found.

The rest of the paper is organised as follows: section two discusses the related research, section three deals with the research method, section four outlines data collection and categorisation, and section five shows the data analysis. Finally, section six contains the conclusions.

Related research

Defence includes various components of strategies, such as Total Defence, which means protecting a state's independence and its citizens, trying to estimate an adversary's potential capabilities, and protecting society's vital functions from threats or actual attacks (Lehto, 2016, Ministry of Defence, 2006, p. 23). Lehto (2016) claims that an important part of total defence is military Cyber Defence, which is the combined capability of intelligence, influence and protection (Lehto *et al.*, 2017). Furthermore, network surveillance is a part of cyber defence and it means defence to protect, monitor, analyse, detect and respond to network attacks, intrusions, disruptions, or any unauthorised actions that would destroy information systems and the networks connected to them through computer networks (Lehto, 2015, p. 18; Ottis, 2013). According to Hausken (2019, p. 364 and Wei *et al.*, 2015) networks including electrical power, communication, computers, command and control, production or multiple military army networks can be under attack.

According to Yaghlane and Azaiez (2016), Wei *et al.* (2015), Sigholm (2013, p. 51), Lehto (2015), defence against Cyber Space Operations provides strategic benefits in cyberspace. Lehto *et al.* (2017, p. 33) in turn explain Cyber Capability as raising the attack threshold, efficient observation ability, situation awareness, decision-making, and management processes suitable for the cyber world.

One of the capabilities of a defence system, or part of it, is Operative Capability (Ministry of Defence, 2006). The performance of a defence system, or part of it, is affected by its skills set, material and operating principle. Operative Capability consists of effectiveness, life cycle and usability (Ministry of Defence, 2006). According to Lehto (2014, p. 54), capability is the ability to achieve the desired effectiveness and take into account threats, operating environment and other circumstances.

Critical infrastructure includes both physical structures and buildings, and digital activities and services: energy production, distribution and transfer systems, traffic and logistics, information and communication systems, and water and waste disposal. Critical Infrastructure Protection (CIP) means the protection of critical infrastructure (Mäntylä, 2014). Dunn (2005, p. 266) claims that "the objects of protection are services and their role and function for society". Geers (2011, p. 135) claims that much critical infrastructure is in private hands, outside of government protection and oversight. According to Hausken (2019, p. 364) and Quijano *et. al.* (2016), societal infrastructures that each consist of various sectors which interact can be under attack.

The Secretariat of the Security Committee (2018, pp. 16–17) states that Information Security Breach Investigation, which is a cyber operation and an organised way of managing the aftermath of a security breach or cyber attack (IT incident or computer incident or security incident), can include incident response actions such as protecting

evidence, digital forensics, malware analysis, log analysis and general investigations of the security breach's influence or scope, in order to limit the damage.

Von Clausewitz (1832) points out that Espionage is the same as Intelligence, and adversaries and their country must be investigated before the country's plans and operations.

The Secretariat of the Security Committee (2018, p. 23) and Clark (2013) define Cyber Intelligence as both communications and telecommunications intelligence and information system intelligence inside or outside the homeland state, which is state-authorised. Wihersaari (2015, p. 6), on the other hand, points out the difference between cyber security and cyber offensive from two perspectives, that is, the role and manifestation of intelligence. In the former, cyber security is perceived "from a threat awareness and vulnerability management perspective, whereas in the latter, cyber intelligence is treated as an enabling and target designating element." Geers (2011, p. 100) states that attackers should be forced to lose time, wander into digital traps, and betray information regarding their identity and intentions. According to the Secretariat of the Security Committee (2018, p. 26), cyber spying is part of cyber intelligence. The spying of networks, their devices and software, is targeted at states, citizens or any organisation or company using targeted malware attacks. Spyware is a malware program that collects data from the information system executing the spyware. It can also be called as a digital spy (Geers, 2011). The data can be IP and Domain Name System (DNS) information, credit card information, bank account ID, passwords, browser history or the content of documents (Mäntylä, 2014 p. 14).

Joint Publication 1–02 (2010, p. 53) states that in Counter Intelligence (CI), information is gathered and defence activities are conducted against hostile actors for several purposes, "such as to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted."

Cline (1993, p. 147) and NATO StratCom COE (2016) state that the Recognition Primed Decision (RPD) Model of Rapid Decision Making helps experienced decision-makers apply their past experience to make the right decisions the first time round, thus eliminating the need to make other decisions.

Nimmo (2015) and Pomerantsev (2015) state that Information Security and Defence means protecting credible sources of information. Raggad (2010) and Mäntylä (2014) claim that confidentiality means protecting information from unauthorised access or disclosure, integrity means protecting information from unauthorised modification, and availability means that information security is achieved when users receive the required information from the appropriate resource. Information Security and Defence means several arrangements, such as access control; locking premises; safety preservations and disposal of documents; data encryption and backups; fire-walls; antivirus programs and certificates; securing documents, hardware and software; data communications; and operational security (Secretariat of the Security Committee, 2018, p. 15; Hausken, 2019, p. 364). NATO StratCom COE (2016, p. 8) states that "hostile actors try to affect decision making by distorting the quality of information, controlling access to information or influencing people's perception and understanding of the information they are in contact with". Dunn (2005, p. 261), the Secretariat of the Security Committee (2018, p. 14) and Mäntylä (2014) claim that information, data and software of computer systems that operate critical infrastructure must be protected. In relation to this, Dunn (2005, p. 261) mentions that "information is an issue of national security, because the society is dependent on ICT. Therefore, information defence must happen on technical, legislative, organisational, or international levels."

Jackson (2015, p. 6) argues that Defence with Law means arrangements against the incorrect usage of legitimate systems and ways of doing things right – both internationally and domestically – in order to obtain political superiority or commercial benefits.

The Ministry of Defence (2016), Lehto (2015), Sillanpää *et al.* (2015), the Joint Chiefs of Staff (2013) and Schechtman (1996) claim that the Observation-Orientation-Decision-Action (OODA) loop, which is a cybernetic twin loop model of human decision-making in defence, means protecting the IE by defending it against IO and cyber operations or defending oneself against network warfare. Network warfare is quite close to cyber warfare. Cyber warfare includes cyber penetration, cyber manipulation and cyber robbery (Sigholm, 2013, p. 51, Lehto *et al.*, 2017).

Conley *et al.* (2016) state that Non-physical Network Defence is defence against security, business, intelligence, political, contact and company networks that are guided, owned and funded by a foreign state, as well as opaque foreign state networks.

Strategic Communications (StratCom*)* means defence against IO by which different information influences are controlled in a military crisis (Hollis, 2011), public diplomacy (PD), public affairs (PA), military public affairs (MPA), and psychological operations (PSYOPS) (NATO StratCom COE, 2015, U.S. Department of Defence, 2008). In StratCom, IO and public relations influence are carried out and are targeted at domestic and foreign media and audiences (Luoma-aho, 2015). StratCom is connected to IW and network control and management (Jantunen, 2013). Table 1 shows the synthesis of the past studies concerning components of defence strategies.

Table 1. The synthesis of the past studies

Thematic category	Literature Source
Total Defence	Hausken, 2019, p. 364; Lehto, 2016; Ministry of Defence, 2006, p. 23
Operative Capability	Lehto, 2014, p. 54; Ministry of Defence, 2006
Cyber Defence	Hausken, 2019, 364; Lehto *et al.*, 2017; Lehto, 2016; Lehto, 2015, p. 18; Wei *et al.*, 2015; Ottis, 2013
Defence against Cyber Space Operations	Yaghlane and Azaiez, 2016; Wei *et al.*, 2015; Lehto, 2015; Sigholm, 2013, p. 51
Critical Infrastructure Protection	Hausken, 2019, p. 364; Quijano *et. al.*, 2016; Mäntylä, 2014; Geers, 2011, p. 135; Dunn, 2005, p. 266

Cyber Capability	Lehto *et al.*, 2017, p. 33
OODA Defence	Lehto *et al.*, 2017; The Ministry of Defence, 2016; Lehto, 2015; Sillanpää *et al.*, 2015; The Joint Chiefs of Staff, 2013; Sigholm, 2013, p. 51; Schechtman, 1996
Espionage	Von Clausewitz 1832
Cyber Intelligence	Secretariat of the Security Committee, 2018, p. 23, p. 26; Wihersaari, 2015, p. 6; Mäntylä, 2014, p.14; Clark, 2013; Geers, 2011, p. 100
Counter Intelligence	Joint Publication 1–02, 2010, p. 53
Information Security and Defence	Hausken, 2019, p. 364; Secretariat of the Security Committee, 2018, pp. 14–15; NATO StratCom COE, 2016, p. 8; Nimmo, 2015; Pomerantsev, 2015; Mäntylä, 2014; Raggad, 2010; Dunn, 2005, p. 261
Information Security Breach Investigation	Secretariat of the Security Committee, 2018, pp. 16–17
RPD Model	NATO StratCom COE, 2016; Cline, 1993, p. 147
Defence with Law	Jackson, 2015, p. 6
Non-Physical Network Defence	Conley *et al.*, 2016
Strategic Communications	NATO StratCom COE, 2015; Luomaaho, 2015; Jantunen, 2013; Hollis, 2011; U.S. Department of Defence, 2008

Thus, despite numerous excellent past studies on components of defence strategies, the literature has neglected the relationships of these components of strategies with each other. Therefore, this study responds to the need for further research, and offers both

practical and theoretical knowledge on components of defence strategies in a society's IE, exploring their relationships with each other.

The profound analysis of past components of defence strategy research thus led to the formulation of two research questions (RQs): 1) What are the components of defence strategies in a society's IE?; and 2) How are the components of defence strategies in a society's IE related to each other?

Research method

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

According to Markus and Robey (1988), theories are established using a variance or process theory. Process theory tries to understand the phenomena in the terms of the cause-effect events leading to an outcome. Variance theory explains phenomena in terms of the relationships that link hypotheses between the dependent and independent variables. The emergent theory, which can be a conceptual framework, the various concepts, and the concept categories and their relationships with and dependencies on each other offer a new type of theoretical construct for understanding the studied phenomena from different perspectives (Mustonen-Ollila and Heikkonen, 2009). According to Eisenhardt (1989), the combination of case study and GT approaches has three major strengths: it produces a novel theory, the emergent theory is testable, and the resultant theory is empirically valid (Mustonen-Ollila and Heikkonen, 2009). GT is used in interpretive studies, and it can be extended to inductive theory creation (Mustonen-Ollila and Heikkonen, 2009) – which is in line with this study.

The data should be categorised under several identifiable themes. These themes can also form the main categories or concepts in the data. This is a selective way of finding the concepts and categories in the data and is based on the researcher's own intuition or knowledge. The concepts must be categorised according to relevant terminology and theories that form the most referenced work in categorising concepts in the research area. After the categories have been discovered, the number of categories must be decided on. The problem with the categories is whether enough proof can be found in the data to make them and the concepts valid and reliable, and whether the concepts and categories discovered are the correct ones. Some other concepts and categories may emerge from the data later. If the concepts and categories are not correct, the researcher must return to the data and discover new concepts. After the abstract concepts are found, they can be coded according to the instructions of Glaser and Strauss (1967), using selective coding to search the data categories. The abstract concepts can also be found using the content analysis approach (Krippendorff, 1985), which is a text analysis method. The approach

requires the researcher to construct a category system, code the data, and calculate the frequencies or percentages that are used to test the hypotheses on the relationships among the variables of interest. It is assumed that the meaning of a text is objective, in the sense that a text corresponds to an objective reality.

The text is interpreted and understood without extraneous contextual knowledge. In case studies such as this study, the concepts are sharpened by building evidence that describes them. The data and concepts are constantly compared so that accumulating the evidence converges on simple and well-defined concepts, i.e. categories or constructs. The constructs are either ancillary or focal. In theory building, special focus is placed on dependent variables, that is, society and its IE. These concepts were the focal concepts (constructs) in the theory. The ancillary concepts (constructs) in the theory were the independent variables, which were associated with the changes in the value of the dependent variables. The conceptual framework tried to explain the changes in the values of these concepts. In this theory, the ancillary constructs were the defence strategies. The emergent relationships between the constructs were verified to fit the empirical evidence and GT was applied in their analysis. The data that confirmed the emergent relationships enhanced the confidence in the validity of the relationships.

In this study, the constant comparison between data and concepts in past studies, in order to accumulate evidence converged on simple, well-defined thematic categories, led to a higher level of abstraction of statements about the relationships between the thematic categories. This theorising was in line with Pawluch and Neiterman's (2010) suggestions of creating a GT using Glaser and Strauss's (1967) approach. The higher level of abstraction of statements is presented in the conclusions and discussion section. Glaser and Strauss' (1967) study is the original study of the GT method (See also Pawluch and Neiterman, 2010). Intuition and knowledge is also used in determining the categories, and a chain of evidence is created: the thematic categories are derived from the empirical data and then validated using past studies. In this study, Pawluch and Neiterman's (2010) GT analysis instructions, together with those of Glaser and Strauss (1967), support the finding of categories from data and based on the researchers' own intuition and knowledge.

Strauss and Corbin's (1990) GT method, on the other hand, uses three phases of coding as well as a tool (for example Atlas.ti) to define categories, and finally a core category. According to Strauss and Corbin (1990), GT has three levels of coding: open, axial and selective coding. Open coding reveals similarities and differences in the data so as to unveil the concepts, classes and relationships between the concepts in the data. Similar concepts will be put into the taxonomy of categories. There is a need to set the dependencies and relationships between concepts and classes: thus, in axial coding, categories are analysed. Through this, the development of the relationships between concepts will reveal new concepts and relationships. Selective coding integrates and refines the fully developed categories into theories. The main theme of the research emerges from the data during this phase, but after the main theory is established, the researcher still refines the categories by discarding the unwanted ones and expanding on those that remain poorly developed. In this study, however, the GT method of Strauss and Corbin (1990) was not applied but the differences between Glaser and Strauss (1967) and Strauss and Corbin (1990) needed to be addressed in order to avoid any disinformation.

A qualitative case study (Yin, 2003, Creswell, 2007) using the GT approach (Eisenhardt, 1989, Glaser and Strauss, 1967) was chosen to help answer the two research questions. The sample was limited to one society's IE, because the goal of the study was

to gain a deep understanding of the selected IE and to identify components of defence strategies at this specific site. Due to resource limitations, the sample was limited to 10 interviewed experts who represented eight different organisations in Finland. When the qualitative data reached saturation point, data collection ended. Nine audio-recorded unstructured and semi-structured interviews were conducted, which investigated the experiences of components of defence strategies. These interviews (Table 2) included eight individual interviews and one two-person group interview, which took place between January and May 2018. The interviewees were or had been involved in several components of defence strategy in their own fields of expertise during their working careers, which extended over a period of six to over 30 years in different positions and organisations in Finland and abroad. Archival material was also studied, representing a secondary source of data, which included public news and past scientific studies on components of defence strategies in Finland or abroad in general. Triangulation (Yin, 2003) was used to combine different data sources simultaneously to improve the reliability and validity of the data.

Each interview transcript was analysed and the major emergent themes and concepts were identified in order to form thematic categories (Myers and Avison, 2002). The interviewees received the questions before the interviews in order to familiarise themselves with them beforehand (Creswell, 2007), and were able to check their content in order to reduce mistakes. The questions were improved after each interview to better suit the next interview. In this in-depth case study, the interviewees recommended new interviewees based on their extensive experience in the area.

Table 2. Interviewee details

Interviewee number	Role of interviewee	Length of interview in minutes	Group or individual interview
1	Chief of Cyber Division	215	Individual interview
2	Military Professor	235	Individual interview
3	Civilian Security Officer	151	Individual interview
4	Civilian Official & Senior Adviser of Security Committee	135	Group interview
5	University Teacher	31	Individual interview

6	Expert of Security Committee	66	Individual interview
7	Military Professor	117	Individual interview
8	Officer of Defence Command Finland	200	Individual interview
9	Researcher (Digitalization, Cyber Security)	181	Individual interview
Total:		1341	

Data collection and categorization

The audio recorded interviews included frequent elaboration and clarification of meanings and terms, and the recordings were transcribed, yielding over 240 pages of transcriptions. After the transcription of the interviews, a qualitative research method based on GT (Glaser and Strauss, 1967) and content analysis (Krippendorff, 1985) was applied in order to categorise data under thematic categories according to relevant terminology and theories in the studied research area. In this study, the components of defence strategies were denoted as thematic categories (Glaser and Strauss, 1967). After creating the chain of evidence in data categorization, a total of 146 different empirical observations under 16 thematic categories (see Table 3) were found using Glaser and Strauss's (1967) approach.

Thematic category	**Definition based on empirical evidence**	**Total number of observations**
Total Defence	Military and civil defence of society from foreign state's goal to destroy society's IE.	5
Operative Capability	(Military) attack strategies as premises for operational scope.	2

Table 3. Thematic category, definition based on empirical evidence, and total number of observations

Cyber Defence	Protection against foreign countries' military and civil intelligence. Cyber defence includes both offensive and defensive measures. Cyber defence includes, for example, cyber surveillance and network surveillance.	25
Defence against Cyber Space Operations	Internal exercises in which own systems are tested during peace time.	22
Critical Infrastructure Protection	Internal cyber operation designs and implements a safe infrastructure.	3
Cyber Capability	Information systems' capability and operative capability (in cyber space).	3
OODA Defence	Defence against information operations, cyber operations and network warfare in IE. Network warfare is quite close to cyber warfare. Cyber warfare includes cyber penetration, cyber manipulation and cyber robbery.	2
Espionage	Intelligence inquiries in ground, sea, air and cyber environment.	4
Cyber Intelligence	Communications or telecommunications intelligence and information system intelligence.	9
Counter Intelligence	Determination of possible (hostile) actors, routes and signs that (hostile) actor may use when entering (systems/networks).	8
Information Security and Defence	Information protection solutions, because infrastructure is attacked or operations connected to attacks are carried out.	11
Information Security Breach Investigation	Search for intruder to network/information system and search methods.	6

RPD Model	Defence through defenders' experience in decision-making.	6
Defence with Law	State's possible counter measures based on national legislation.	3
Non-Physical Network Defence	In non-physical network warfare, mental crisis tolerance, citizens and whole society must be defended.	6
Strategic Communications	Communicating the facts to everyone.	31
Total number of observations		146

Table 4 below shows an example of an observation concerning the 'Cyber Defence' thematic category. In Table 3, the first column contains a specific thematic category discovered in the empirical data; the second column contains its definition based on the empirical data; the third column contains its evidence based on the literature; the fourth column contains the literature references, and finally the fifth column contains the transcript number of the empirical evidence.

Thematic category discovered in empirical data	**Definition of thematic category based on empirical data**	**Evidence from literature**	**Literature references**	**Transcript number**
Cyber Defence	Protection against foreign countries' military and civil intelligence.	Cyber defence and cyber security are important parts of total defence. Cyber defence includes the combined capabilities of intelligence, influence and protection. It also includes both offensive and defensive measures, as well as devices and systems that are not connected to the network.	Lehto, 2016, Lehto *et al.*, 2017	TC7

Table 4. Example of observation regarding 'Cyber Defence' thematic category

Data analysis

Fragmentation and reassembling was used to classify the data into thematic categories and thus capture the components of defence strategies in society's IE (Glaser and Strauss, 1967). After the thematic categories were found, their properties and propositions (hypotheses) as to how they were related were determined. The conceptual framework (see Figure 1) shows the thematic categories as boxes, and the two-sided solid arrows with numbered small boxes describe the relationships between them. These relationships, based on empirical data, are presented in detail in Table 5. The constant comparison between the data and the thematic categories in past studies, in order to accumulate evidence convergence on simple and well-defined thematic categories, has led to a higher level of abstraction of statements about the relationships between the thematic categories. This theorising is in line with suggestions for creating a GT using Glaser and Strauss's (1967) approach. The higher level of the statements' abstraction is included in the discussion and conclusions section.

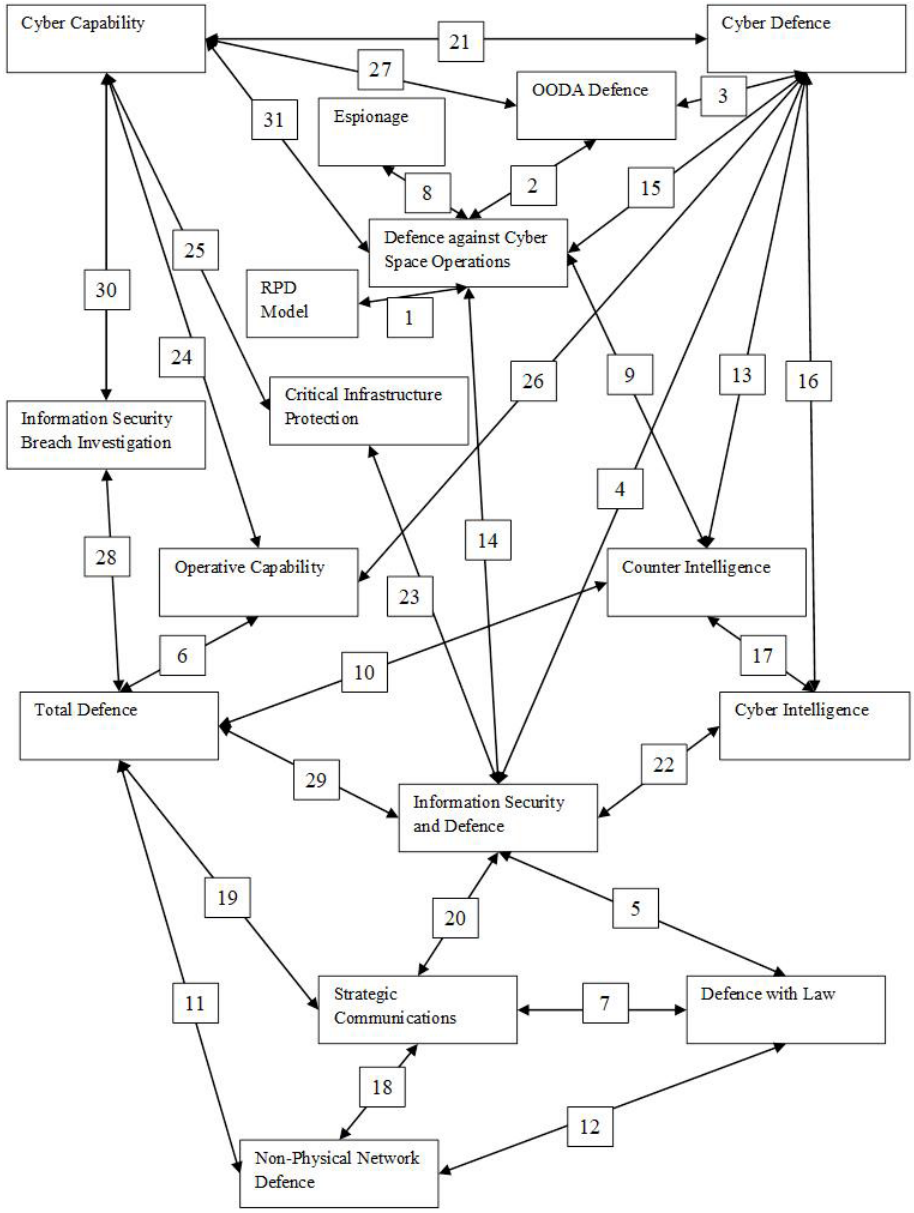

Fig. 1. Conceptual framework of thematic categories

Table 5. Properties of thematic categories and propositions (hypotheses) as to how they are related on the basis of the data

Thematic category/categories	**Properties of categories and propositions (hypotheses) as to how thematic categories are related (two-sided solid arrows in Figure 1)**	**Arrow number**
RPD Model/ Defence against Cyber Space Operations/ OODA Defence	An adversary decides on how and when to attack. Costs of attacks may be raised. In the PRD model, you must be able to act more quickly than the adversary responds. One way is acting more quickly and the other is to slow down the adversary (*testing your own things more quickly*). Both have the same effect, but if you are using both, the choice of methods can multiply. There can be hidden costs, and it is possible to increase the costs of attacks for the adversary. And here, one key point emerges which differentiates warfare carried out in the cyber environment and warfare possibly really carried out in the information environment from other means of traditional warfare. OODA defence is defence against cyber space operations *(in the cyber environment and IE).*	1, 2
OODA Defence/ Cyber Defence/ Information Security and Defence/ Defence with Law	Cyber attacks can influence the target's information or occur technically. Technical procedures are connected to implementation of IE. But if a small group is carrying it out (*cyber operation or cyber attack*) and its goal is for some foreign state to benefit from it or if it is connected to a foreign country's pressurisation method or activities or suchlike, where the group has received its guidance from a foreign state, then based on international law this is pre-warfare action. And this is the grey area. The information environment is connected to this. And it is also connected to the foreign state's goal of taking Ahvenanmaa, meaning that the greater goal is broken down in the information environment in which the sub goal is to bring down society through this operation, the implementer of which is then group A, which can be either a non-state or state group. *It is* hybrid influencing, a precursor to war if it is given guidance from a foreign state.	3, 4, 5
Cyber Defence/ Information Security and Defence/ Total Defence	A company's task is to secure its own information and internal and external network environment and their interfaces, and thus to contribute to society's total defence. But in Defence Forces (DF), the situation is different because DF must be able to protect their own networks of course, but we also have something like this abroad. If we think of defence as a defence system, such as total defence, it is defined in the strategy papers and the meetings produce more defence systems and educate people about the system and breaks into it. But I am not in that environment, I look at the system as an outsider, even if I read the material and information they have produced and know that this system exists.	4, 6
Defence with Law/ Strategic Communications	A bank can carry out internal counter measures, but not external counter measures outside the bank. If, however, all the state's data communication passes through it, counter measures are taken on the basis of national legislation. Accessories, which both criminals and states can use in strategic communications for their benefit to disseminate their own message or just to taunt or confuse situations.	7

Espionage/ Defence against Cyber Space Operations/ Counter Intelligence/ Total Defence/ Non-Physical Network Defence/ Defence with Law/ Strategic Communications	An external cyber operation has an external foreign state actor (military cyber space operation). Possible espionage or preparation to influence or implement operation. Yes, we have practised with our international partners, we practised a lot. I think it was at the beginning of 2000, when we started to carry out certain internal exercises in which we tested our own systems in peace time. So, we have a long tradition in this area. Finland responds to such information operations, for example in the Turku case ("terrorist attack in Turku"), we solved the situation very quickly. (*Later, the terrorist was prosecuted according to the law).* We want to keep people safe and we do not change our strategy, meaning that we continue peace-keeping operations in Iraq or Afghanistan or Lebanon as before.	8, 9, 10, 11, 12, 7
Counter Intelligence/ Cyber Defence/Information Security and Defence/Defence against Cyber Space Operations	If there are indications that a certain group intends to attack, this actor must be found by e.g. determining the group's possible routes of entry into (our systems) and identifying the signs of the attack. Internal (*cyber operation*) is primarily the internal cyber operation of security organisations, Defence Forces: defence, planned protective actions. So, I think it should be defined as being connected to the organisation.	13, 4, 14
Defence against Cyber Space Operations/ Cyber Defence/Cyber Intelligence/Counter Intelligence	Here, the cyber dimension or control of the electric magnetic spectrum is in focus. But in the case of network warfare, the technical level is very close to cyber. In this kind of cyber operation related to protection, you must know what is happening in your own networks. If you do not, I mean these kinds of surveillance operations, it actually means constant presence in those networks and surveillance. Then, in my opinion, it is certainly a kind of organised cyber operation, because it is connected to surveillance and I would not say that it is intelligence in this sense, but connected to arranging one's own defence.	15, 16, 17
Non-Physical Network Defence/ Strategic Communications/Total Defence	In a (non-physical) network, the centric warfare attacker influences society, mental crisis resilience and citizens. Therefore, non-physical networks such as social networks must be defended. Social media belongs to network centric influence, in the case of something operative. In network centric warfare you should influence the whole of society: you influence mental crises and citizens. Then it extends especially to *social media.*	18, 19
Strategic Communications/ Information Security and Defence/ Cyber Defence/ Critical Infrastructure Protection	Cyber attacks can also influence the target's information, or be technically based, in which case strategic communications are also connected. But, on the other hand, if you think about Finland's internal cyber operation (*cyber defence*), then it is primarily design, building infrastructure, safe infrastructure, and it is more about things connected to structure via the system, rather than actually carrying out operations.	20, 4, 21

Espionage/ Defence against Cyber Space Operations/ OODA Defence/ Cyber Defence/ Cyber Intelligence/ Information Security and Defence/ Critical Infrastructure Protection	Clients could not afford to update their information systems to newer versions and old information systems could not be corrected. All our neighbouring states have certain intelligence laws which mean that they not only have the right but an obligation to carry out intelligence. Foreign intelligence is working in Finland and they can check any person's phone. The only authority that cannot carry out intelligence on Finnish citizens, are the Finnish authorities. All other actors can do so. Internal cyber operation: implementing protection in the network is one part of cyber operation. But, then, if we are already in a war state and problems are being caused at the same time in our networks by a third partner, such as by a foreign actor, then we must raise the protection level.	8, 2, 3, 16, 22, 23
Non-Physical Network Defence/Total Defence/ Operative Capability/ Cyber Capability/Cyber Defence/Information Security and Defence	A superpower may believe that in order to gain operational scope of sovereignty maintenance, it requires huge military attack strategies. Different strategies in cyber operations and cyber attacks were used depending on what was meant by strategies and strategic goals, such as retaining and maintaining one's sovereignty and its defence strategies.	11, 6, 24, 21, 4
Cyber Defence/Information Security and Defence/Critical Infrastructure Protection/Cyber Capability	To build up safety infrastructure and information infrastructure. Let's take, for example, a management system and its cyber security and cyber defence solutions. They are operative solutions in the sense that they create infrastructure which then makes it possible to influence or enables operations connected to attacks, in the case of security organisation in particular.	4, 23, 25
Cyber Defence/Operative Capability/Cyber Capability	Possibly operative (cyber) capability, which means that we build information system capability, i.e. cyber operation capability today. Today we are on a completely different level, because all information systems and networks and (*social*) networks are on a different level of development than in 1990–2000. But functionally they had already begun then. In a way, in terms of Defence Forces, automatic field message systems emerged in field message actions, as there was this basic system (message device system) in which you could see where the bit moved.	26, 24
Espionage/ Defence against Cyber Space Operations/Counter Intelligence/Cyber Intelligence/Cyber Defence/ Information Security and Defence/Strategic Communications	If surveillance ability or intelligence ability are missing, action is not possible. Some states take advantage of this for their own purposes. Many are naïve in this matter. So, cyber security strategy requires that our strategic choice is that we are able to carry out surveillance and intelligence not only on the ground, sea and air, but also in the cyber environment. And the strategic choice is whether we do it inside the country or also outside the country. For example, if there are some disturbances in the networks, then we must decide whether we are carrying out IO, for example if there is a reason for the disturbance, such as a foreign state's hostile influence, it has installed some program code inside the network.	8, 9, 17, 16, 4, 20

Counter Intelligence/ Cyber Intelligence/Cyber Defence/OODA Defence/ Cyber Capability	Even if it is 90% the same, there is still a small difference between network defence and cyber defence. Cyber defence also includes devices and systems that are not connected to networks. Network defence protects networks, network terminals and information resources. Nowadays, people talk about cyber defence. It is not the same, there are small differences, even if 90% is the same. A network is also devices and systems that are not connected. Operations take place in networks, but why does one want to restrict it? It is not synonymous with cyber warfare, but why focus on one specific one when we should see the whole?	17, 16, 3, 27
Information Security Breach Investigation/Total Defence/Information Security and Defence/ Critical Infrastructure Protection	Via the embassy, it is possible to safely exchange secret information abroad, but alone or in a small group this is challenging, because state borders are not physical borders. Internal cyber operation: how you build it, what information you protect in that network. But DF does not defend Finland's cyber world. If we enter (*society*) further, and enter the government, their vital activities, which run Finnish society and as regards the model of total defence, then there the defender is the Ministry of Finance and its cyber unit. The goal of this unit is to defend all state institutions and maintain the infrastructure by which the Finnish state is ruled. Somebody is neglecting cyber security. It is our internal cyber operation. Somebody has leaked information, meaning that through that person, information is getting out. This can be intentional or unintentional.	28, 29, 23
Information Security and Defence/Cyber Defence/ Cyber Capability/ Information Security Breach Investigation	If a company has a break-in or finds malicious software the incident response group takes control of the situation and ensures recovery to the normal state before the break-in. So, we were able to be aware of what was happening in our networks, because when all these information systems and services etc. arrived, we lost track of what was happening in our own networks.	4, 21, 30
Information Security and Defence/Cyber Defence/ Defence against Cyber Space Operations/ Cyber Capability	Protecting the network is one branch of cyber operations. How to conduct the protection is outlined in established cyber operations. If you are think there is a problem in the western world, you classify the cyber problem, build a cyber solution, and they place it at the centre of defence. China and Russia place information in the centre to be defended and the rest are just tools. Cyber and network activities are just one device to obtain information, change it or destroy it.	4, 15, 31

Conclusion

Based on eight individual and one two-person in-depth group interviews, this qualitative, empirical case study based on the GT approach (Glaser and Strauss, 1967) tackled the thematic categories denoted as components of defence strategies in a society's IE using the inductive research approach. The interview questions were improved many times, and sometimes due to the schedule of the interviewee, the questions were shortened. The largest interview consisted of 70 questions, and the 'shortest' of 30 questions. As already mentioned, the interviewees recommended new interviewees based on their extensive experience in this area.

The thematic categories were defined by building evidence from empirical data and describing it, which according to Glaser and Strauss (1967) are the building blocks of GT. The data and categories were constantly compared so that the accumulating evidence converged into 16 simple, well-defined thematic categories. After the thematic

categories were found, their properties and propositions (hypotheses) as to how they were related were defined. Finally, a conceptual framework of the thematic categories and their relationships was developed. The comparison with past studies led to 9 higher-level abstractions of statements about the relationships between the thematic categories. This theorising was in line with suggestions for creating a GT using Glaser and Strauss's (1967) approach.

Theory building in this study gave special status to the focal categories, that is, the society and its IE. In this theory, the ancillary category (construct) was the component of defence strategy. Boundary conditions were addressed in this theory creation, because the phenomenon was so atypical that it only held in this specific society's IE. The results validated the conceptual framework, which became the discovered theory for the phenomenon. The data that confirmed the emergent relationships improved the confidence in the validity of the relationships. The past studies with similar findings were important because they tied together the underlying similarities in phenomena not associated with each other, achieving stronger internal validity.

This study is in line with the studies of Lehto (2016) and the Ministry of Defence (2006, p. 23) by finding that total defence protects a society's citizens and vital functions from threats or actual attacks. This study is also in line with Lehto (2016) that an important part of total defence is military cyber defence, which is the combined capability of intelligence, influence and protection (Lehto *et al.*, 2017). The results support the claims of Lehto (2015, p. 18) and Ottis (2013) that cyber defence needs network surveillance actions to protect the computer networks and information systems connected to the networks from cyber attacks and cyber operations. Furthermore, this study is line with Hausken (2019, p. 364) and Wei *et al.* (2015) that several networks in a society must be protected by cyber defence actions.

It also agrees with Yaghlane's and Azaiez's (2016), Wei *et al.*'s (2015), Lehto's (2015) and Sigholm's (2013, p. 51) studies observing that defence against military cyber space operations offers strategic benefits in cyberspace, and also Lehto *et al.*'s (2017, p. 33) claim that situation awareness and decision-making are better when cyber capability is at a high level.

The findings also support the claims of Lehto (2014, p. 54) and the Ministry of Defence (2006) that defence systems need operative capability to get the wanted effectiveness to fight against threats.

The findings also support Mäntylä (2014), the Secretariat of the Security Committee (2018, p. 14), Dunn (2005), Geers (2011, p. 135), Hausken (2019, p. 364) and Quijano *et. al.* (2016): that society needs to protect its critical infrastructure because of its vital activities, and this protection also includes protection of the society's services. The findings also support the claims of NATO StratCom COE (2016) that decision-making is affected by the distortion of the quality of information, not permitting access to information or decision-makers' awareness of the information that they receive.

The findings are also in line with the Secretariat of the Security Committee's (2018, pp. 16–17) view that information must be protected against breaches through investigations, and that we must learn from breaches in order to minimise damage.

The findings also agree with Von Clausewitz's (1832) claims that espionage is needed for the state's own purposes, to protect it and its society from foreign countries' operations and plans.

The outcomes are also supported with the view of the Secretariat of the Security Committee (2018, p. 23), Clark (2013), Wihersaari (2015, p. 6) and Geers (2011, p. 100): cyber intelligence is needed to protect one's own information systems and data communications, as well as the internet and other networks against hostile actors both inside and outside the state. The findings also agree with the Secretariat of the Security Committee (2018, p. 26), Mäntylä (2014, p. 14) and Geers (2011) who claim that defence against cyber spying – which is a part of cyber intelligence- is needed because networks, their devices and software targeted at states, citizens or any organisation or company using targeted malware attacks, must be protected against adversaries' cyber spying.

The findings agree with Joint Publication 1–02 (2010, p. 53) which claims that in counter intelligence, information is gathered and defence activities are conducted against hostile intelligence actors for their activities against us.

The study results are in line with those of NATO StratCom COE (2016) and Cline (1993, p. 147) in that the Recognition Primed Decision (RPD) Model of Rapid Decision Making protects decision-makers' ability to make the right decisions in a hostile environment.

This study is in line with those of the Secretariat of the Security Committee (2018, p. 15), Hausken (2019, p. 364), Nimmo (2015), Pomerantsev (2015), Mäntylä (2014) and Raggad (2010) in its finding that information security and defence protects information confidentiality, accessibility and reliability from unauthorised actions. The results agree with the Secretariat of the Security Committee (2018, p. 14), Mäntylä (2014) and Dunn (2005, p. 261) in their claim that information, data and software inside computer and information systems must be protected because they operate inside physical infrastructures. In addition, they also support Dunn's (2005, p. 261) claims that information protection is at the level of national security because information infrastructure is dependent on ICT.

The findings also agree with Jackson (2015, p. 6) that *Defence with Law* prevents the incorrect usage of legitimate systems.

The findings are also in line with the studies of the Ministry of Defence (2016), Lehto (2015), Sillanpää *et al.* (2015), the Joint Chiefs of Staff (2013) and Schechtman (1996) in that OODA is needed to defend IE, by defending it against IO, cyber operations or network exploitation.

The findings support those of Conley *et al.* (2016) that non-physical network defence is needed against networks that are guided, owned and funded by a foreign state and opaque foreign state networks.

The findings agree with Luoma-aho (2015), Jantunen (2015), NATO StratCom COE (2015), Hollis (2011) and the U.S. Department of Defence (2008) that *StratCom* is needed for protection against hostile IO and psychological operations and to carry out one's own IO and public relations influence targeted at domestic and foreign media and audiences.
In this study, these components of defence strategies were inter-related, 9 higher levels of abstraction of statements, based on the conceptual framework, the propositions for the components of defence strategies, and the relationships between the components of defence strategies were found. 1) With the right cyber capability, OODA defence and cyber defence actions, it is possible to defend and protect society's IE, and to improve cyber capability. 2) Information security and defence, critical infrastructure defence, and cyber defence must be up to date because these are the most important to defend and protect. 3) The actors working with the information must be aware of their own actions related to the information. 4)

Cyber defence needs counter-intelligence, cyber intelligence, and OODA defence to make decisions very quickly in order to defend society against cyber operations and cyber attacks. 5) Cyber defence improves cyber capability and is vital for defence against cyber operations. It is needed in operative capability and cyber defence is related to information security and defence. The means to improve cyber defence are counter-intelligence, cyber intelligence and OODA defence. 6) Information security and defence is closely related to cyber defence, and it can be protected and defended by cyber intelligence, through law and strategic communications. Information inside the critical infrastructure needs protection from information security and defence. Information security and defence is also needed in total defence and defence against cyber operations as regards the information needed in these two latter categories. 7) Defence against cyber operations needs espionage, OODA defence, counter-intelligence, and RPD. Information security and defence improves cyber capability and protects information inside one's own cyber operations. 8) Information security breach investigation helps cyber capability because this capability consists of information systems' capability and operative capability. Operative capability needs information protection and if information is under attack, military attack goals may not be achieved if one's own information is known by the adversary when it is leaked. Information security breach investigation also helps total defence because it helps find the attacker of the information and helps find what information the hostile actor now has. Information security and defence needs information security breach investigation in order to protect the information and to know what new protection solutions are needed to defend one's own information. 9) Non-physical network defence needs strategic communications, and defence with law. Non-physical network defence is part of total defence. Protecting it improves total defence from foreign states' goals to destroy society's IE.

Eleven conclusions emerged from this study. 1) The data and findings showed 16 different interconnected components of defence strategies. 2) The hostile actors' political, military, societal, power and personal goals for carrying out cyber operations and cyber attacks is to weaken society's IE. 3) Cyber operations and cyber attacks against networks, information and infrastructures are coordinated operations, carried out over a long time period. 4) The actors defending society's IE must rapidly change their own components of defence strategies, if necessary, and use the newest tools, methods and components of defence strategies in networks, infrastructures and social media networks, which connect a great deal of people. 5) The adversary uses its own espionage and intelligence to investigate important information, information systems and networks before it makes a cyber attack or cyber operation on them. Espionage and intelligence have taken a long time and, by taking these actions, the adversary can define its attack targets. 6) The network attack or cyber attack can also start very slowly with small targets, and defenders might not even see them at first, or it may not be possible to understand what is going on. The defender must distribute its components of defence strategies to many places at the same time, and this ties up the defender's resources. But, if a new, stronger attack starts to take place at the same, then the defender may lack defence resources. 7) It is also possible that not all targets under attack are even noticed, because many attacks are taking place at the same time. The defender can protect and defend its sources by preventing the adversary from going further and deeper into the information systems and networks, or not even revealing that the defender knows the adversary is there harming the systems and networks. 8) If an attack has taken place, it is not always known whether the attacker has left "something inside the systems and networks" and can carry out a new attack later by using these. The defender can use its own intelligence to find out what the attacker is going to do in the future, but the attacker can use previously unused intrusion methods and get inside. 9) The defender can protect its networks by hiding them and their traffic, or by using firewalls or their own cyber intelligence and network surveillance, which alert when they are under attack. The attacker can even use secured systems for their own purposes by buying out some individuals in a company who are actually working for them, not their employer. These inter-

nal spies are a severe threat because they can work freely inside the systems, without anybody noticing what they are really doing. These spies can harm the systems even more than a real attack. 10) One way to defend systems and networks is to build them up in such a way that an attacker can only enter restricted areas and cannot harm any information that is important and vital for society. 11) Citizens must be informed about attacks on a certain level, honestly, so that they understand that they must protect their own information, information systems and networks, and keep their own privacy in good condition so that they and their computers cannot be used as tools in attacks. How and when to inform citizens should be considered carefully. It must be also remembered that attackers will be informed at the same time because they follow the open news about attacks and also realise that their attack is not taking place in secret, but is known publicly.

The practical and managerial contribution helps defending actors outline what components of defence strategies exist in the society's IE and how these components of defence strategies are related to each other. An important practical contribution was the large number of components of defence strategy observations in practice. The managerial contribution lies in making every decision-maker in the society's IE aware of these components of decision strategies and to understand how they affect society's IE.

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

This study has several limitations. First, as components of defence strategy is very large as a research area and contains many issues, it was impossible to cover all of them. Second, trying to determine suitable thematic category definitions for 146 observations was a difficult task, and took longer than estimated. Third, for some of the observations it was challenging to determine the thematic category where it ultimately belongs to. Fourth, the use of only one society's IE affected the findings, and thus generalisation of the results may be that straightforward, although definitely not impossible. Fifth, a limited number of interviews were conducted: only 10 people were interviewed. Sixth, the problem with the thematic categories was whether there was enough proof found in the data to derive these components of defence strategies as valid and reliable, and whether the thematic categories discovered in the data were the correct ones.

In the future, a quantitative analysis of components of defence strategies will be conducted. Glaser and Strauss (1967) and Eisenhardt (1989) claim that both qualitative and quantitative data can be used for creating a new theory. These two types of data can indeed supplement each other and their comparison can result in new theory.

References

Armistead, E. L. and United States and Joint Forces Staff College (2004) *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington, D.C.: Potomac Books Inc.

Benbasat, I., Goldstein, D. K. and Mead, M. (1987) 'The Case Study Research Strategy in Studies of Information Systems', *MIS Quarterly,* 11(1), pp. 369–386.

Clark, R. M. (2013) Perspectives on Intelligence Collection. *The Intelligencer: Journal U.S. Intelligence Studies,* 20(2), pp. 47–53.

Cline, G. (1993) *A Recognition Primed Decision (RPD) Model of Rapid Decision Making*. Available at: https://www.researchgate.net/publication/235418838_A_Recognition_Primed_Decision_ RPD_Model_of_Rapid_Decision_Making (Accessed: 10 September 2019).

Conley, H. A., Mina, J., Stefanov, R. and Vladimirov, M. (2016) *The Kremlin Playbook. Understanding the Russian Influence in Central and Eastern Europe*. A Report of the Center for Strategic International Studies Europe Program and the CSD Economics Program. New York: Rowman & Littelefield.

Geers, K. (2011) Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, Tallin, Estonia: CCD COE Publication.

Creswell, J. W. (2007) *Qualitative Inquiry and Research Design: Choosing Among Five Approache*s. California, U.S.: Sage Publications.

Dunn, M. (2005) The socio-political dimensions of critical information infrastructure protection (CIIP). *International Journal of Critical Infrastructures*, 1(2/3), pp. 258–268.

Eisenhardt, K. M. (1989) Building Theories from Case Study Research. *Academy of Management Review*, 14(4), pp. 532–550.

Glaser, B. and Strauss, A. L. (1967) *The Discovery of the Grounded Theory: Strategies for Qualitative Research*. Chicago, IL: Aldine.

Hausken, K. (2019) Defence and attack of complex interdependent systems. *Journal of the Operational Research Society*, 70(3), pp. 364–376. doi: 10.1080/01605682.2018.1438763.

Hollis, D. (2011) Cyberwar Case Study: Georgia 2008. *Small Wars Journal*. Available at: http://smallwarsjournal.com/jrnl/art/cyberwarcase-study-georgia-2008 (Accessed: 30 January 2017).

Jackson, L. (2015) 'Revisions of Reality: The Three Warfares- China's New Way of War', in *Beyond Propaganda. Information at War: From China's Three Warfares to NATO's Narratives*. London: Legatum Institute: Transitions Forum, pp. 5–15.

Jantunen, S. (2013) *Strategic Communication: practice, ideology and dissonance*. National Defence University, Helsinki. Tampere: Juvenes Print.

Joint Chiefs of Staff (2013) *Joint Intelligence. Joint Publication 2-0*. Available at: https://fas.org.irp/doddir/dod/jp2_0.pdf (Accessed: 20 November 2015).

Joint Publication 1–02 (2010) *Department of Defense Dictionary of Military and Associated Terms*. Available at: https://fas.org/irp/doddir/dod/jp1_02-april2010.pdf (Accessed: 5 September 2019).

Krippendorff, K. (1985) *Content analysis. An Introduction to its Methodology*. California, CA: Sage Publications.

Lehto, M. (2014) Ilmavoimien johtamisjärjestelmän tulevaisuuskuva ('The future image of air forces' management system'). *Research report*. National Defence University, 1(12). Juvenes Print: Tampere.

Lehto, M. (2015) Phenomena in the Cyber World. In: M. Lehto and P. Neittaanmäki, (eds.) *Cyber Security: Analytics, Technology and Automation*, Intelligent Systems, Control and Automation: Science and Engineering. Springer- Verlag, pp. 3–30.

Lehto, M. (2016) Theoretical Examination of the Cyber Warfare Environment. *11th International Conference on Cyber Warfare and Security 2016*, Sonning Common, UK: Academic Conferences and Publishing International Ltd., pp. 223–230.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. and Salminen, M. (2017) Finland's cyber security: the present state, vision and the actions needed to achieve the vision, *Publications of the Government's analysis, assessment and research activities*, Series 30, Helsinki: Prime Minister's Office.

Luoma-aho, V. (2015) Understanding Stakeholder Engagement: Faith-holders, Hateholders & Fakeholders. *Research Journal of the Institute for Public Relations*, 2(1), pp. 1–27.

Markus, K.L. and Robey, D. (1988) Information technology and organizational change: Causal structure in theory and research. *Management Science*, 34(5), pp. 583–589.

Ministry of Defence. (2006) Turvallisesti tulevaisuuteen ('Safely to the future'). *Puolustusministeriön strategia 2025*. Vantaa: Kirjapaino Keili Oy.

Ministry of Defence. (2016) *Puolustusministeriön strateginen suunnitelma 2030* ('The Strategy of Ministry of Defence'). Helsinki: Ministry of Defence. Available at: http://www.defmin.fi/files/1830/plm_strateginen_suunnitelma.pdf (Accessed: 16 January 2017).

Mustonen-Ollila, E. and Heikkonen, J. (2009) 'Historical research in information system field: from data collection to theory creation', in Cater-Steel, A. and Al-Hakim, L. (eds.) *Information Systems Research Methods, Epistemology, and Applications.* Hersey, New York: Information Science reference (an imprint of IGI Global), pp. 140–160.

Myers, M. D. and Avison, D. E. (eds.) (2002) *Qualitative Research in Information Systems: Review*. London: Sage Publications.

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

NATO (2012) *NATO military policy on information operations*. Available at: https://info.publicintelligence.net/NATO-IO-Policy.pdf (Accessed: 24 January 2017).

Nato StratCom COE. (2015) *Mapping on StratCom Practices in NATO countries. Results of the Study*. Riga: NATO StratCom COE.

Nato StratCom COE. (2016) *The Moldovan Information Environment: Hostile Narratives, and their Ramifications. Executive Summary*. Riga: NATO StratCom COE.

Nimmo, B. (2015) 'The Case for Information Defence: A Pre-Emptive Strategy for Dealing with the New Disinformation Wars', in *Beyond Propaganda. Information at War: From China's Three Warfares to NATO's Narratives*. Legatum Istitute: Transitions Forum. Available at: https://linkprotect.cudasvc.com/url?a=http://www.li.com&c=E%2C10%2ChtXuWBOGbBt/RsmOXj/6ef71nlWFhC8CbcGt0a2IUzrZD7a88NHYK2QeSblturLqwBvnCDYYRE9WxtgD&typo=1&know=0 ; https://linkprotect.cudasvc.com/url?a=http://www.prosperity.com&c=E%2C10%2C/8AJE3g7qZ4/I/PTZmZ88MBSbxMZK5IogFAX9YyBrVVWB9xVV2xq5dx9LUpnpHGURfbBaw%2Bmgd6C3n8Y&typo=1&know=0 (Accessed: 6 June 2017), pp. 2–4.

Ottis, R. (2013) 'Theoretical Offensive Cyber Militia Models', in Rantapelkonen, J. and Salminen, M. (eds.) *The Fog of Cyber Defence*. National Defence University. Tampere: Juvenes Print Oy, pp. 190–199.

Pawluch, D., and Neiterman, E. (2010) 'What is Grounded Theory and Where Does it Come from', in Bourgeault, A., Dingwall, R. and De Vries, R. (eds.) *The Sage Handbook of Qualitative Methods in Health Research.* London: Sage Publications, pp. 174–192.

Pomerantsev, P. (2015) 'Introduction', in *Beyond Propaganda. Information at War: From China's Three Warfares to NATO's Narratives*. Legatum Istitute: Transitions Forum. Available at: https://linkprotect.cudasvc.com/url?a=http://www.li.com&c=E%2C10%2C9ONJrGgf6q5dlI9DV4Ac55keEDXxXOu9%2BYg16SM%2BSDReFB5AiLcOpAaqmua9T1%2BMPYrOv2Mh%2Bo2wWxrh&typo=1&know=0 ; https://linkprotect.cudasvc.com/url?a=http://www.prosperity.com&c=E%2C10%2COHaPDSXkKLdxBeY0gHZx7MXM6N9AHhwUfkhgpFJL0idC%2BeJKOczouzdK5q05BWgQzo9x1TuOK0pWTxDS&typo=1&know=0 (Accessed: 30 May 2017). pp. 29–36

Quijano, E. G., Rios Insua, D. and Cano, J. (2016) Critical networked infrastructure protection from adversaries. *Reliability Engineering and System Safety*. doi: 10.1016/j.ress.2016.10.015. Available at: https://www.sciencedirect.com/science/article/pii/S0951832016307037 (Accessed: 20 January 2020).

Raggad, Bel G. (2010) *Information security management: Concepts and practice*. CRC Press.

Schechtman, G. M. (1996) Manipulating the OODA loop: The overlooked role of information resource management in Information Warware. *Thesis*. U.S. Air Force Institute of Technology.

Secretariat of Security Committee (2018) *The Vocabulary of Cyber Security*. Helsinki: The National Emergency Supply Agency.

Sigholm, J. (2013) 'Non-State Actors in Cyberspace Operations', in Vankka, J. (ed.) *Cyber warfare*. National Defence University, Tampere: Juvenes Print, pp. 47–76.

Sillanpää, A., Roivainen, H. and Lehto, M. (2015) 'Finnish Cyber Security Strategy and Implementation', in Lehto, M. and Neittaanmäki, P. (eds.) *Cyber Security: Analytics, Technology and Automation*. Springer-Verlag, pp. 3–30.

Society (2020) Merriam-Webster [online] Springfield: Merriam-Webster Inc. Available at: https://linkprotect.cudasvc.com/url?a=https://www.merriam-webster.com/dictionary/society&c=E%2C10%2CgT7RqBE9TLMlhTkrtxnXKViHfBTVPOvGwXN/jyruGGCAq/8Dn4KK3rDadU%2B97H1ngtL68IFAmE3f6bMr&typo=1&know=0 (Accessed: 17 March 2020).

Strauss, A. and Corbin. J. (1990) *Basic of Qualitative Research: Grounded Theory Procedures and Techniques*, Newbury Park: Sage Publications.

The Security and Defence Committee (2006) The Strategy for Securing the Functions Vital to Society. *Government Resolution 23.11.2006*. Available at: http://www.defmin.fi/ (Accessed: 21 November 2019).

U.S. Department of Defence (2008) *Principles of Strategic Communication*. Available at: https://www.hsdl.org/?view&did=716398 (Accessed: 6 September 2019).

Von Clausewitz, C. (1988) *Vom Crieg*. Helsinki: Art House.

Wei, J., Zhang, R., Liu, J. Niu, X., and Yang, Y. (2015) Defense Strategy of Network Security based on Dynamic Classification. *KSII Transactions on Internet and Information Systems (TIIS),* Dec, 9(12), 5116–5134. doi: http://dx.doi.org/10.3837/tiis.2015.12.021.

Wihersaari, K. (2015) Intelligence Acquisition Methods in Cyber Domain. Examining the Circumstantial Applicability of Cyber Intelligence Acquisition Methods Using a Hierarchical Model. *Thesis*. Helsinki: National Defence University.

Wolfswinkel, J. F., Furtmueller, E. and Wilderom, C. P. M. (2013) Using Grounded Theory as a Method for Rigorously Reviewing Literature. *European Journal of Information Systems*, 22(1), pp. 45–55.

Yaghlane, A. B., and Azaiez, M. N. (2016) Systems under attack-survivability rather than reliability: Concept, results, and applications. *European Journal of Operational Research*, 258(3), pp. 1156–1164. doi: 10.1016/j. ejor.2016.09.041.

Yin, R. K. (2003) *Case study research: design and methods*. California: Sage Publications.