A Whole-of-Society Approach to Organise for Offensive Cyberspace Operations: The Case of the Smart State Sweden

Gazmend Huskaj[1,2] and Stefan Axelsson[1]
[1]Department of Computer and Systems Sciences, Stockholm University, Kista, Sweden
[2]Geneva Centre for Security Policy (GCSP), Geneva, Switzerland
g.huskaj@gcsp.ch

Abstract: Threat actors conduct offensive cyberspace operations for many purposes, such as espionage, to destroy information assets, and cybercrime. These operations are possible thanks to the innovation and development of information and communications technologies (ICT). Interconnected information systems have transformed societies positively. However, specific states exploit these systems' vulnerabilities to advance their strategic national interests. Therefore, it is important to know how a state can organise itself to defend against threat actors. The purpose of this research is to present how the smart state Sweden can through a whole-of-society approach organise for Offensive Cyberspace Operations. The intent is to conduct an active and independent foreign-, security- and defence policy, but also as a base for deterrence and defence. This article is based on a mixed methods approach. It uses the case study research strategy to discover new information. Fourteen men and women participated in individual semi-structured interviews. The respondents ranged in age from 40 to 65 with more than 20 years of experience in cyberspace operations, intelligence operations, military operations, special forces operations, and knowledge and understanding about information warfare and information operations. The analytic strategies include thematic analysis and quantitative methods to interpret the data. The results show many themes, but the article is especially focused on the themes of Operations, Capability, Policy & Governance, and Legal Frameworks. Finally, a conceptual map of a whole-of-society approach to organise for offensive cyberspace operations is presented inferred from the themes, codes, and content, and mapped to each responsible agency based on the interviews and codes. The answer to the research question is that Sweden should have a whole-of-society approach to organise for Offensive Cyberspace Operations to project power in and through cyberspace with the intent to conduct an active and independent foreign, security and defence policy and for deterrence, as described in Figure 2.

Keywords: Deterrence, Information Systems, Cyberspace capabilities, Offensive cyberspace operations, Smart State.

1. Introduction

Threat actors conduct offensive cyberspace operations for many purposes, such as espionage, to destroy information assets, and cybercrime. These operations are possible thanks to the innovation and development of information and communications technologies (ICT). Interconnected information systems have transformed societies positively. However, specific states exploit these systems' vulnerabilities to advance their strategic national interests. Examples include suppressing their population to ensure their autocratic rule [Ernst and Lee, 2021], stealing knowledge in private companies and industry [PwC and BAE Systems, 2017], and for intelligence purposes in preparation to take over another country's territory [Deibert et al., 2012, Dickinson, 2021]. Once the tanks are invading, the organisations of these states or their proxies continue to conduct offensive cyberspace operations for intelligence purposes and support the kinetic effort [Microsoft, 2022].

Cyberspace, like air, land, sea and space, has been declared a domain for military operations Command. The United States Joint Chiefs of Staff in 2004 declared it as a "'domain' of conflict alongside the air, land, sea, and space domains, and noted DoD must maintain its ability to defend against and to engage enemy actors in this new domain" (US CYBERCOM). Defending and engaging threat actors in and through cyberspace is not new. This idea was based on early discussions as early as the 1970s about computer security. In 1975, Rein Turn and W. H. Ware presented a research paper titled "Privacy and Security in Computer Systems." They argued that "the vulnerability of computerised information has prompted measures to protect both the rights of individual subjects and the confidentiality of research database" [Turn and Ware, 1975]. However, public discussions did not occur until 1983, when the movie WarGames showed "computer hacking" and its implications on national security. The result was the first U.S. Presidential Directive on computer security. Since then, computer hacking, or offensive cyberspace operations, has increased (c.f. the Cyber Operations Tracker or the CyberPeace Institute).

Researchers have identified and studied how to organise for offensive cyber operations, but this research is limited. Devanny et al. [2022] note that cyberspace operations are conducted and discuss these within the concept of "cyber power" and how states should organise themselves, but view it from the angle of a "coherent cyber strategy." Aschmann et al. [2017] discuss how threat actors can plan, prepare and "organise specific strikes." Rohret [2010] discuss how a framework may be used to organise offensive operations. Finally, Kaplan [2017] notes that the U.S. pondered where to organise the new combatant command for offensive cyberspace

operations. During those discussions, the U.S. identified the National Security Agency (NSA) as the best-suited organisation. According to Kaplan, the motive was that the NSA were best equipped to conduct offensive cyberspace operations and because the U.S. was not big enough to have multiple institutions for cyberspace operations. Therefore, to use resources wisely, the conclusion was to establish the United States Cyber Command on "top" of the NSA [Kaplan, 2017].

Identifying how a state should organise itself for offensive cyberspace operations is challenging. Kaplan [2017] is the only author who gives some insights on how policymakers discuss how to organise for offensive cyberspace operations and other researchers (e.g., van Haaster, Willett, Hunker) discuss cyber power. Our research question is, therefore: how can Sweden, a smart state, through a whole-of-society approach, organise for Offensive Cyberspace Operations? The intent is to conduct an active and independent foreign-, security- and defence policy, but also as a base for deterrence and defence. The notion of a "Smart State" is a state that "seek[s] influence based on the power of ideas" (Sundelius, 1995, as cited in Eriksson, 2019).

The starting point for this research article is identifying a framework to measure national power linked to the rapid technological and social changes Tellis et al. [2000a]. The framework provides the base for semi-structured interviews with experienced security professionals in Sweden's intelligence, security and defence sectors. The interviews were analysed through thematic content analysis. The theme size is based on a quantitative analysis of the codes. Based on the interviews and the themes, a conceptual map of a whole-of-society approach to organise for offensive cyberspace operations is described. These methodological considerations are reported in section 3, and the analysis in section 4. Section 5 presents the conceptual map of a whole-of-society approach to organise for offensive cyberspace operations, and the article ends with conclusions and future research. The contribution of this article is a conceptual map of a whole-of-society approach to how Sweden, with its agencies, private sector and academia, can organise itself for offensive cyberspace operations.

2. The Framework to Measure National Power

Rapid technological and social changes affecting national power and the balance of power are nothing new. Huskaj [2023] presents how nations considered defending the sea trade routes, leading to sea power; land power was about defending trade routes on railways; airpower became a concept with the discovery of aircraft. Ampuja and Koivisto [2014] labelled concepts and note shifts from one "time" to another "time", such as from the "post-industrial"-times to the "network society"-times. They argue that information technologies accelerate and enhance the process of information. Major companies and states that understood that having effective infrastructure could increase their competitiveness internationally [Ampuja and Koivisto, 2014].

These shifts, rapid technological and social changes, and how they affect national power, the balance of power, and the nature of warfare, concerned the U.S. Office of Deputy Chief of Staff for Intelligence. More specifically, the concerns that triggered this were:

1. A growing unease with the current aggregate measures of national power used within the intelligence community.
2. A growing suspicion that the nature of warfare itself may be changing in fundamental ways.
3. An increasing concern that the lack of an adequate methodology to assess national power might cause the United States to miss or misinterpret incipient changes in power capability that may be taking place within many countries in the international system.

[Tellis et al., 2000b, p. 1].

The result was the framework to measure national power. It consists of three levels: the national resources level, the national performance level and the military capability level. However, this research study aimed to identify how Sweden should organise itself for offensive cyberspace operations, not to measure Swedish national cyber power. Therefore, the framework was adapted to focus on organising for offensive cyberspace operations.

3. Research Design

The researchers base this research on interpretivism. Humans make meanings based on their social context, time, place, expertise, training and education. Therefore, to create a new and rich understanding of how Sweden can organise itself for offensive cyberspace operations, it was evident to approach very experienced Humans on the topic of this research article. GH approached and asked very experienced people if they wanted to be part of this research. Those were either part of GH's network or recommended by the network.

Fourteen men and women participated in individual semi-structured interviews. The respondents ranged in age from 40 to 65 with more than 25 years of experience in cyberspace operations, intelligence operations, military operations, special forces operations, and knowledge and understanding of information warfare and information operations. Semi-structured interviews lasting between one and two hours enabled data collection. All interviews were conducted and moderated by GH. The researcher presented the cases in Table 2 to the respondents to drive the discussion because [Mandel, 2017] provided extensive detail. He categorises the cases by case name, type of attack, who initiated the attack, and whether the initiator had state support. Although his book provides more details about each case, the respondents are, and were, well aware of each case. Therefore, visualising the cases in this format stimulated the discussion during the semi-structured interviews.

Thematic analysis, as described by Braun and Clarke [2006], is the applied analytic strategy. Thematic analysis is a qualitative analytic strategy that looks for "themes or patterns" [Braun and Clarke, 2006, p. 77] in the data set. The researcher is actively looking for themes or patterns in the dataset by generating a list of codes. These codes, in turn, are analysed and together form a theme broader than the unit of analysis (code) [Braun and Clarke, 2006]. Table 1 presents data extracted from the data set and its coding, followed by how the codes are inferred into a theme: Operations.

Table 1: Data extract with codes applied and resulting theme.

Data Extract	Coded for	Theme
Then you need offensive capability so that you can, in those cases, which many times are about shutting down cyber infrastructure, shutting it down, best, because it costs money to destroy a bunch of servers, costs money and time.	offensiveOperations	Operations
Of those I know in more detail, I would say that I would not use the term enhance, but support. Support to the operations, or to the campaign.	supportOperations	

These qualitative techniques and procedures to interpret the data result in 'a relatively systematic and comprehensive summary or overview of the dataset as a whole' [Wilkinson, 1997, 170]. Thus, applying these techniques and procedures results in a long list of codes. These codes are, as mentioned above, inferred into themes. The result of coding and inferring is a thematic map of 25 themes.

Table 2: The cases presented to the respondents. (Source: [Mandel, 2017]).

Case	DataCorruptionErasure	DataCorruptionviaWormInsertion	DataTheeft	DenialofService	DisruptingPhones	InsertVirus	MalwareInsertion	Defacement	ViolencePresence	InitiatorType	StateSupport
Estonia				X					X	NSG/Gov	Russia
Gaza				X				X	X	Terror Group	N/A
Georgia			X	X				X	X	NSG	Russia
Saudi Aramco	X					X				NSG	Iran
Sony							X			NSG	North Korea
Stuxnet		X								Govs	N/A
Ukraine				X	X			X	X	NSG	Russia

4. Analysis - A Whole-of-Society Approach to Organise for Offensive Cyberspace Operations

This section summarises the major themes of the thematic content analysis, illustrating them with quotes from the respondents. Although figure 1 presents all identified themes, this section will cover only the themes of Operations, Capability, Policy & Governance, and Legal Frameworks.

4.1 Offensive Cyberspace Operations

With its 61 codes, the operations theme is the most prominent theme. The theme has multiple sub-themes on cyberspace operations. The first sub-theme is about operations in general. Here, the respondents talk about offensive and defensive cyberspace operations and that offensive cyberspace operations are not the same as information operations. For example, one respondent notes that an offensive cyberspace capability should be able to conduct "all types [of operations], affect CIA [Confidentiality, Integrity and Availability], steal information, manipulate, and to turn off availability." Another respondent notes that an offensive cyberspace capability should be able to conduct "Attacks on CNI, [and] one must develop the capability to reach as deep as possible on CNI or make it possible that one can do these kinds of attacks, to turn off the power on whoever is threatening us." CNI refers to "Critical National Infrastructure", such as the financial, transportation, and energy sectors.

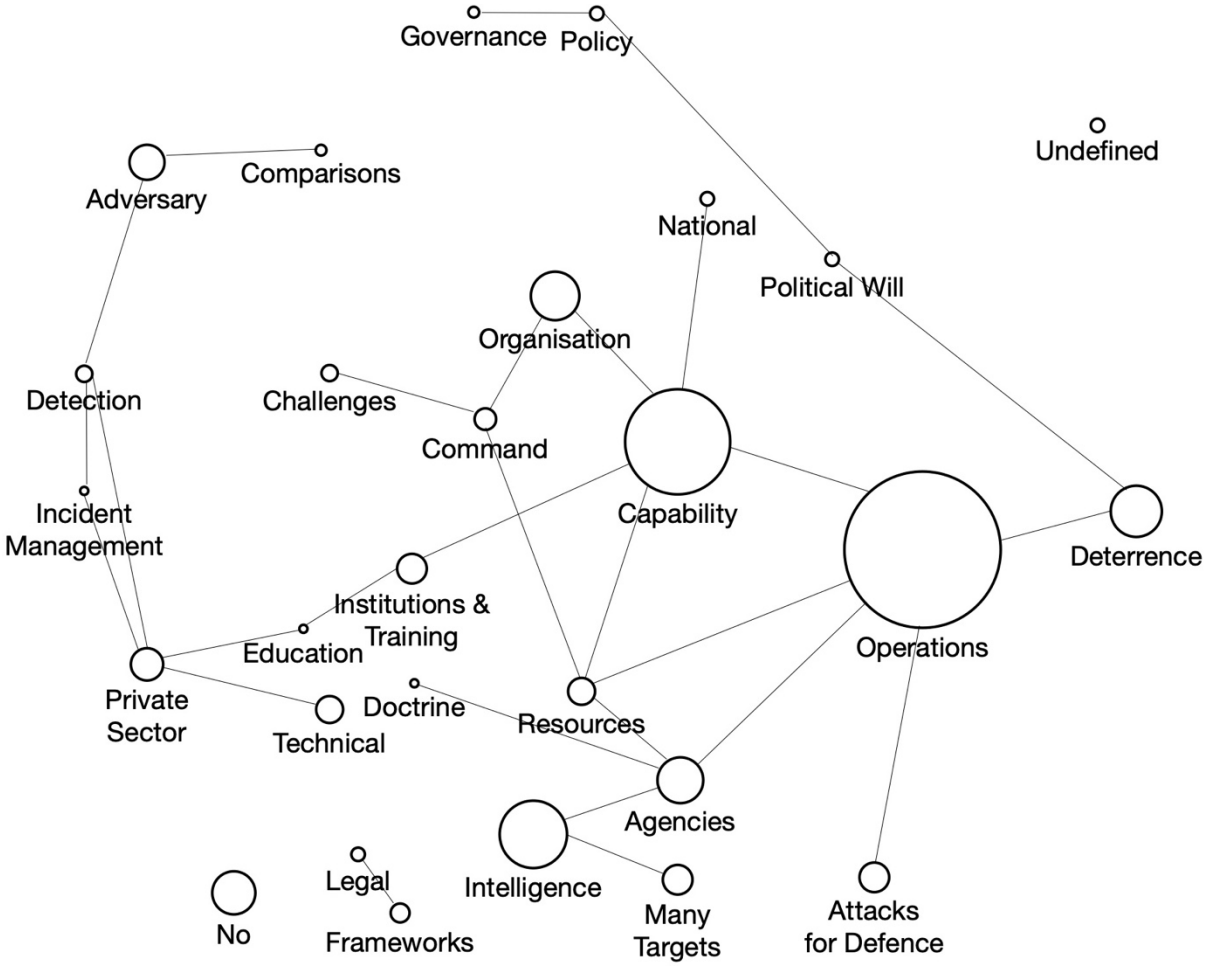

Figure 1: The Developed Thematic Map. Theme size is based on the number of codes. For example, the operations-theme has 61 codes.

In conducting defensive cyberspace operations, a unit must be able to conduct offensive operations. In other words, to defend, one must attack. Four respondents note that to defend; one must be able to attack: to "have an offensive capability to attack for defensive purposes."

One respondent notes that offensive cyberspace operations are not information operations. The respondent notes that "it is interesting to talk about domains. If Russia is trying to affect the election in the US or Sweden,

one should not consider it equal to they [Russia] have conducted a cyber operation. The domains go into each other, but it is a good example to keep them separated. Think of a Venn diagram with a joint space."

The second sub-theme concerns how offensive cyberspace operations should be integrated into information and multi-domain operations. Here, one respondent notes having the ability to conduct offensive cyberspace operations as part of an overall information operation. An example could be to "Combine an information operation with a cyber attack targeting a water cleaning facility to ensure more bacteria in the water could lead to a very effective part." Integration in multi-domain operations is about integrating cyber into the other domains: air, land, sea and space. The purpose is to exploit cyber to the maximum to achieve advantages in other domains.

The third sub-theme is about how to use offensive cyberspace operations. Some examples include influencing the adversary for command-and-control warfare, defensive purposes, sabotage, as a force multiplier, as a support function, for deception, competitive advantages, and to generate cognitive effects. One respondent notes that it is possible to influence the adversary by conducting cyberspace operations and "see" parts or the whole of the adversary's situation awareness: "If you can influence and interfere with the adversary's situation awareness, you can gain an advantage." The respondent counties:

"Whatever adversary information system you can access and interfere or destroy leads to throw the adversary off balance, such as to turn off telecommunication services, payment functions or other parts of communication of the societal structure."

Command and control warfare uses offensive cyberspace operations to impact command and control. One respondent notes:

"You depend on information to conduct command and control. If you limit information through cyber operations or through secondary effects, by not striking directly on the weapon systems, but on supply chains. You are not destroying the weapon system but ensuring [the adversary] does not receive the weapons or fuel."

Offensive cyberspace operations are also a support function. Some examples include supporting other operations, companies in critical national infrastructure, and police investigations.

The fourth sub-theme is about risks related to offensive cyberspace operations. Some examples include unintended secondary and tertiary effects (=cascading effects) and risks leading to a diplomatic crisis. Conducting offensive cyberspace operations that do not lead to secondary and tertiary effects is essential. Should that occur, there are risks the adversary may realise they are under attack and could retaliate: this cannot happen.

4.2 The Cabinet Office and the Policy Level

The respondents noted that an effective cyber capability requires some form of governance, and the governance model differs if operations are for offensive, defensive or collection purposes. The highest national level, the Cabinet Office and the policy level govern the use of offensive cyberspace operations. Governing the use of offensive cyberspace operations requires, according to one respondent, "someone" on the policy level that can "make decisions, [understands] legal frameworks, [with] a legal position on international law, linked to legal frameworks." Another respondent noted that the same person must have "a basic education in college; through that understanding and experience, one can understand the operational parts and then work on the policy level." A third respondent emphasises, "I do not believe you can only educate policy people to understand these things. Things can turn bad. Being at the policy level means being on the strategic level, which means a person on that level is senior: There are no shortcuts in the cyber-area."

The implication is that the "someone" working on the policy level must at least have a primary education on the college level and then get experience with cyberspace capabilities. The road to the policy level is long, and being on that policy/strategic level also means an individual is of senior rank. The "there are no shortcuts in the cyber-area" implies that an individual must have this "basic college education" and, through working experience, understand cyberspace capabilities' positive and negative effects: the highest level must always answer to the political level if something goes wrong. Therefore, anyone working with offensive cyberspace operations on the policy level needs an understanding of the entire chain: from the target, the offensive capability chosen for that target, potential secondary and tertiary effects (also known as cascading effects), legal aspects, to potential risks. Although this may sound complicated and new, it is not. Similar experiences exist in Sweden: the Special Operations Forces (SoF) organisation.

Special Operations Forces Command (SOFC) directs the Special Operations Forces. The strategic level must understand how to leverage the Special Operations Forces to achieve strategic and security policy goals and this capability's strengths and weaknesses. The history of the Swedish Special Operations Forces and the challenges it had to overcome to become the organisation it is today were many (and will not be covered here). Those with insights into that journey can provide examples to extrapolate the cyber-domain. One respondent notes that SF operators "cannot get caught because the politicians on the strategic level will react." To mitigate this, the respondents note that a closed community should know about ongoing SoF operations, but a general community should know that the SoF-capability exists.

4.3 Capability

Capability is about having the power to do Etymonline [2023]. Therefore, cyber capability is about having the necessary institutions, policy, doctrine, training, education and organisation to have the power to conduct cyberspace operations. A capability to conduct cyberspace operations needs to be agile. The necessary institutions range from the policy level down to the individual. The policy level should have experienced people who are senior and understand the technology level and related strengths and weaknesses. The individual level is related to the individual's role concerning his/her expertise within the unit.

The policy, technology, legal and operations domains require their respective institution to provide training and education. This is because the strategic, operational, and tactical levels differ in scope. One respondent notes that "in addition to the unit itself, the whole training system: school, academia, recruitment, training facilities, training and testing will require much coordination. Then the organisation needs its capability for competence development." Another respondent notes:

"You need technical, organisational skills, a unit, with the required capability. Then you need a regulatory framework, legal position, international law linked to the regulatory framework, and rules for peace and war. If you have those two, then you need decision-making mechanisms to evaluate a CONOPS for a cyber operation, take a position, OPSEC, and then be able to make decisions, follow up on implementation, and effects."

The cyber-organisation can have a command-like structure for offensive and defensive cyberspace operations. One respondent notes that "the command-like structure should protect the Armed Forces' systems. The armed forces and the National Defence Radio Establishment (FRA) should develop and organise the capability. It is close to SIGINT; those resources should probably be pooled. We have Network Collection and Offensive capabilities, capability-wise there is not much difference." The unit should consist of "typical roles: infrastructure specialists, intelligence analysts, a lawyer at the tactical level to give direction based on current legislation [that] 'we have the following possibilities.' Otherwise, the whole system fails." Part of the institutional structure is the role of the private sector.

The cyber security private sector has a role, primarily a defensive one. The private sector can conduct red-team exercises and be "posted" in different departments or teams. Giving them additional context, they can become "a reserve organisation like, for example, the British Army LIAG, or like the Estonian Cyber Home Guard, supporting other things than just offensive." LIAG is the British Army Land Information Assurance Group "which comprises professionals selected for their professional skills. This reduces the training burden on the military such that only military skills need to be provided to these volunteers - their technical skills are the main selection criteria" Military Wiki [2023]. LIAG is under the Operational Command of the Joint Cyber Reserve Force [Gov.uk, 2023].

4.4 Legal Frameworks

The importance of regulatory frameworks, legal positions and international law has been mentioned above. Another respondent notes, "There is no legal expertise, as a field, it is less developed than, e.g., cluster bombs and risk distances to the civilian population." The respondent notes, "an operational, legal function that can evaluate [legal frameworks] is important."

5. A conceptual map of a whole-of-society approach to organise for offensive cyberspace operations

The conceptual map results from the researchers' interpretation of the data, coding and inferring, and is based on the research philosophy of interpretivism. It is important to note that different researchers may conclude differently. However, the researchers of this article have extensive professional and academic experience in the

Swedish security system. The combination of interpreting and inferring the collected data and professional and academic experiences justifies this analysis.

Sweden should have a whole-of-society approach to organise for Offensive Cyberspace Operations to project power in and through cyberspace to conduct an active and independent foreign, security and defence policy and for deterrence, as described in Figure 2. The figure results from conceptualisation and inference, as mentioned in Section 3. Each theme is associated with an icon or figure belonging to an agency responsible for that theme (for example, FRA, MPF, SÄPO) or a generic icon or figure such as academia, private sector & industry, and capabilities.

These qualitative techniques and procedures to interpret the data result in 'a relatively systematic and comprehensive summary or overview of the dataset as a whole' [Wilkinson, 1997, 170]. Thus, applying these techniques and procedures results in a long list of codes. These codes are, as mentioned above, inferred into themes. The result of coding and inferring is a thematic map of 25 themes.

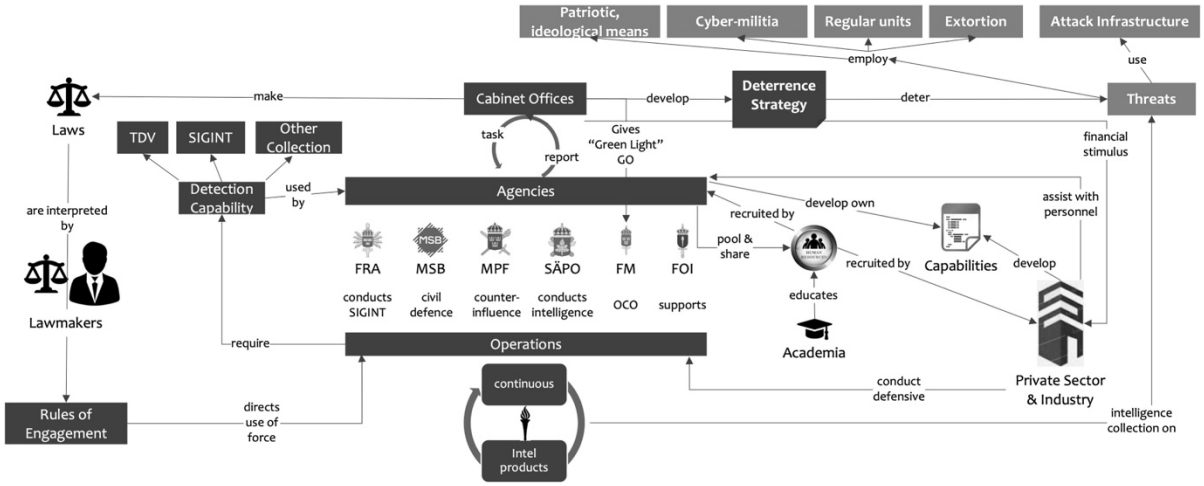

Figure 2: The conceptual and inferred map of all themes, codes, and content, mapped to each responsible agency based on the interviews and codes.

This section describes each concept. Threats use or provide attack infrastructure to their entities, employ patriotic, ideological means, and use extortion to recruit human resources. These entities can take the form of cyber-militia and regular units. A deterrence strategy is required, developed by the Cabinet Offices to deter the threats. Furthermore, an effective cyber capability requires engaging all national resources. This begins at the top level, at the Cabinet Office, by establishing a vision for the cyber capability. This vision also presents that the Cabinet Offices are the ultimate authority for offensive cyberspace operations. Next, the Cabinet Offices share that vision with the agencies, academia, private sector and industry. The vision can take the form of a strategy, such as a cyber security strategy, with discussions on offensive and defensive measures.

The Cabinet Office also makes laws interpreted by lawmakers that break them down into Rules of Engagement (RoE). The RoE's direct use of force for offensive cyberspace operations. The Cabinet Offices hold command over the cyber capability and are responsible for giving FM the "green light" to conduct offensive cyberspace operations.

The Cabinet Offices enable and direct how agencies should work through instructions to the agencies. For the agencies, it is essential to adhere to the Cabinet Offices' instructions and note the differences between these and various principles. The principle of responsibility, while giving good guidance, should receive the attention it requires in the form that it is currently having a fragmenting effect: regardless of how many resources the various agencies receive, the risk is that these are unsatisfactory.

Next, organisation, pooling and sharing resources are critical enablers for the organisation of an effective cyber capability. Organising the capability by co-locating it with other agencies with similar capabilities is an excellent first step to ensure that human and infrastructure resources are wisely managed.

The Cabinet Office provides financial stimulus to the private sector & industry to develop capabilities for the agencies and to pool and share Human Resources. The private sector & industry conduct defensive operations and share threat intelligence with the agencies to increase situational awareness. Additionally, the private sector

and industry can conduct defensive cyberspace operations to protect their own infrastructure. Furthermore, they can support FM, FRA, MPF, MSB and SÄPO with intelligence and software/hardware capabilities.

The private sector and industry can also conduct offensive cyberspace operations when the Cabinet Offices require them to do so from government-related infrastructure. This clearly defines that the smart state is in charge, and one possible scenario when this would happen is when the smart state requires to conduct offensive cyberspace operations. However, the key competencies are within the private sector & industry.

This type of integration between the private and public sectors for defensive and offensive operations is unheard of in the pre-cyberspace era: cyber operators with the required skills to conduct offensive cyberspace operations do not grow on trees, and many different skill sets are needed. For example, training military operators to operate a main battle tank can take up to 7 months, while training a cyber operator for offensive operations can take years.

The National Defence Radio Establishment (FRA) conducts cyber intelligence, surveillance, and reconnaissance (ISR) operations on the threats. They use this intelligence for future cyber intelligence operations and provide intelligence support to other agencies. MSB conducts defensive cyberspace operations. The psychological defence agency (MPF) is responsible for information operations and counter influence-operations.

SÄPO conducts intelligence cyberspace operations on internal threats.

FM conducts offensive cyberspace operations, with support from other agencies, but primarily from FRA. FM targets a threat's attack infrastructure and other cyberinfrastructure. Other targets include telecommunications services, communications channels, communications to air, sea or other societal functions. Additional targets include supply chains, command and control systems, critical national infrastructure, and payment functions. Conducting pure defensive cyberspace operations will probably lead to failed deterrence.

FOI provide support for training and education through their CRATE environment and research. At the same time, academia educates and trains human resources that, in turn, are recruited by the agencies, the private sector & industry. The agencies pool and share the recruited human resources to mitigate the lack of human resources: there must be more competencies in cyberspace operations. Pooling, sharing, and maximising the use of resources requires co-locating the cyber capability at FRA. The nature of offensive cyberspace operations and SIGINT operations are very similar. Co-location also enables a quick deconfliction mechanism and short decision-making lines.

Co-location is essential because offensive cyberspace operations and intelligence collection operations differ from a risk perspective: the military commander takes some risk executing offensive operations when generating effects; the commander conducting intelligence collection may not accept any risk because those operations should go unnoticed. This setup makes it possible to deconflict time-critical operations quickly.

Another way of organising could be as in the USCYBERCOM case: the Director of the NSA is also the Director of US CYBERCOM, a dual-hatted position. The USCYBERCOM case has, until the writing of this article, showed very positive results with empirical evidence such as Operation Glowing Symphony [Darknet Diaries, 2019] and 28 so-called Hunt-Forward Operations, a part of "CYBERCOM's 'persistent engagement,' an effort aimed at proactively defending the U.S. against malicious cyber activity [U.S. Cyber Command, 2022].

6. Conclusions & Future Research

The study builds on an adapted framework for describing national power and extends it by applying it in the cyber domain. Based on the cases, the offensive cyberspace operations, and their impact, the respondents agree there is a need to organise for offensive cyberspace operations. However, some challenges exist, such as needing more human resources with the necessary skills. However, public-private partnerships can overcome these challenges.

The answer to the research question is that Sweden, the smart state, should have a whole-of-society approach to organise for Offensive Cyberspace Operations to project power in and through cyberspace with the intent to conduct an active and independent foreign, security and defence policy and for deterrence, as described in Figure 2. Co-locating the cyber capability at FRA enables the pooling and sharing of Human Resources and maximising the use of other resources. Furthermore, co-location enables the ability to deconflict time-critical operations between the offensive and intelligence roles, which are critical for mission success.

With support from the private sector, the national cyber capability conducts defensive and offensive operations at an age where private companies are leading the technological development, which in a pre-cyberspace era were led by national military establishments and related supporting industries.

Multiple areas for further research exist. One area is to give further insights into how the private sector could be engaged in offensive operations at the government's will. What problems may arise, and how can these problems be solved?

7. Glossary

AI:	Artificial Intelligence.	MISP:	Malware Information Sharing Platform.
AV:	Anti-Virus.	ML:	Machine Learning.
C2:	Command & Control.	MSB:	Swedish Civil Contingencies Agency (Myndigheten för Samhällsksydd och beredskap)
CNI:	Critical National Infrastructure.	OPS:	Operations
CSA:	Cyber Situational Awareness.	OSI Stack:	The Open Systems Interconnection Stack/Model.
DDoS:	Distributed Denial of Service.	OSINT:	Open Sources Intelligence.
FM:	The Swedish Armed Forces (Försvarsmakten)	PFP:	Partnership for Peace.
FRA:	The National Defence Radio Establishment (Försvarets radioanstalt)	PSYOPS:	Psychological Operations.
GCHQ:	Government Communications Headquarters.	SÄPO:	Swedish Security Service (Säkerhetspolisen).
IDS:	Internal Detection System.	SIGINT:	Signals Intelligence.
IOC:	Indicators of Compromise.	TDV:	Technical Detection- and Warning system (Tekniskt detekterings- och varningssystem).
IPB:	Intelligence Preparation of the Battlefield.	USCYBERCOM:	United States Cyber Command.
IPOE:	Intelligence Preparation of the Operational Environment.		

References

CyberPeace Institute. (2023). Cyber threats. Retrieved from https://cyberconflicts.cyberpeaceinstitute.org/threats.

R. J. Agard. AFSC 1B4X1 CYBER WARFARE OPERATIONS CAREER FIELD EDUCATION AND TRAINING PLAN. Technical report, 2018.

M. Ampuja and J. Koivisto. From ‘post-industrial’ to ‘network society’ and beyond: The political conjunctures and current crisis of information society theory. Journal for a Global Sustainable Information Society, 12(2):447–463, 2014.

M. Aschmann, L. Leenen, and J. Van Vuuren. The utilisation of the deep web for military counter terrorist operations. pages 15–22, 2017

V. Braun and V. Clarke. Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2):77–101, 2006. ISSN 14780887. doi: 10.1191/1478088706qp063oa.

U. C. Command. Our history. Retrieved from https://www.cybercom.mil/About/History/.

Darknet Diaries. Ep 50: Operation glowing symphony, 2019. Retrieved from https://darknetdiaries.com/ episode/50/.

R. Deibert, R. Rohozinski, and M. Crete-Nishihata. Cyclones in cyberspace: Information shaping and denial in the 2008 russia–georgia war. Security Dialogue, 43(1):3–24, February 2012.

J. Devanny, L. Goldoni, and B. Medeiros. Strategy in an uncertain domain: Threat and response in cyberspace. Journal of Strategic Security, 15(2):33–47, 2022. doi: 10.5038/1944-0472.

P. Dickinson. The 2008 Russo Georgian war: Putin’s green light, 2021. Retrieved from https://www.atlanticcouncil.org/blogs/ukrainealert/ the-2008-russo-georgian-war-putins-green-light/.

E. Ernst and S. Lee. Countering cyber asymmetry on the korean peninsula: South korea’s defense against cyber attacks from authoritarian sates. Journal for Intelligence, Propaganda and Security Studies, 15(1):165–179, 2021.

Etymonline. Capability, 2023. Retrieved from https://www.etymonline.com/word/capability.

Gov.uk. Joint cyber reserve force, 2023. Retrieved from https://www.gov.uk/government/groups/ joint-cyber-reserve-force.

T. Grant, C. van‘t Wout, and B. van Niekerk. An ontology for cyber ISTAR in offensive cyber operations. In European Conference on Information Warfare and Security, ECCWS, volume 2020-June, pages 117– 125, 2020. ISBN 9781912764617. doi: 10.34190/EWS.20.066.

J. Hunker. ”Cyber war and cyber power - Issues for NATO doctrine”, Reseach Division. NATO Defense College, no. 62, pp. 1–12, 2010. https://www.files.ethz.ch/isn/124343/rp_62.pdf, (2022-03-07).

G. Huskaj. Digital Geopolitics: A Review of the Current State. In International Conference on Cyber Warfare and Security, volume 18, pages 152–161, feb 2023. doi: 10.34190/iccws.18.1.955.

F. Kaplan. ‘wargames’ and cybersecurity’s debt to a hollywood hack. Retrieved from https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html.

F. Kaplan. Dark Territory: The Secret History of Cyber War. Simon Schuster Paperbacks, Harlow, 1 edition, 2017. ISBN 1476763267.

R. Mandel. Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks. Georgetown University Press, 2017.

Microsoft. Defending ukraine: Early lessons from the cyber war. Technical report, Microsoft, June 2022.
Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Military Wiki. Land information assurance group, 2023. Retrieved from https://military-history.fandom.com/wiki/Land_Information_Assurance_Group.

C. on Foreign Relations. Cyber operations tracker. Retrieved from https://www.cfr.org/cyber-operations/.

PwC and BAE Systems. Operation Cloud Hopper. Technical Report April, 2017. Retrieved from https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

D. Rohret. Proactive cyber initiative: An expert system framework. In the 9th European Conference on Information Warfare and Security 2010, ECIW 2010, pp. 378–388.

A. Tellis, J. Billy, C. Layne, M. McPherson, and J. Sollinger. Measuring National Power in the PostIndustrial Age. RAND Corporation, first edition, 2000a.

A. J. Tellis, J. M. Sollinger, C. Layne, J. L. Bially, and M. McPherson. Measuring National Power in the Post-Industrial Age. RAND Corporation, first edition, 2000b. ISBN 0833027921.

R. Turn and W. Ware. Privacy and Security in Computer Systems: The vulnerability of computerizedinformation has prompted measures to protect both the rights of individual subjects and the confidentiality of research data bases. American Scientist, 63(2), 1975. Retrieved from https://www.jstor.org/ stable/27845364.

U.S. Cyber Command. U.S. conducts first hunt forward operation in lithuania, 2022. Retrieved from https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/.

J. van Haaster. ”Assessing cyber power.” In 2016 8th International Conference on Cyber Conflict (CyCon), vol. 61, pp. 7–21, May 2016. doi: 10.1109/CYCON.2016.7529423.

S. Wilkinson. Qualitative research: Theory, method and practice. Sage Publications Ltd., London, 1 edition, 1997.

M. Willett. ”Assessing cyber power”, Survival, vol. 61, no. 1, pp.85–90, 2019.