Expertise
and insight
for the future

Ilmari Luoma

Strategic Threat Modelling

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

December 20th, 2023

PREFACE

In the process of writing this thesis I had trouble writing the abstract concept of permanently contested hostile cyberspace just behind one network socket in the wall of the office. I asked AI what that looks like and I think the picture sums it up perfectly. Like any art it's up for interpretation: It has beauty in it and at the same time it fills me with a level of unease. The idea of everything being connected to that one single point from everywhere. At the same time most wonderful and most terrifying.

This thesis was a way for me to try to quantify a really complicated, bias-prone and complex topic into something standardized, comprehensive, and actionable. I think the subject matter matured with time as I matured with my career in cybersecurity. Taking me a quite a bit longer to comprehend this as I'd like but after I was finished with this thesis, I felt that I had finally understood something profound of cybersecurity and of my own thinking as well.

I really appreciate my colleagues for sparring this with me and formulating these thoughts and I admire the patience of my instructor with my slow~ish pace of getting this ready.

Helsinki, December 20th, 2023
Ilmari Luoma

Author Title Number of Pages Date	Ilmari Luoma Strategic threat modelling 45 pages 20 December 2023
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Ville Jääskeläinen, Principal Lecturer

Threat modelling is the process of identifying and communicating information about threats that may impact a particular system or network. On strategic level this concept is expanded to include the entirety of the organization: What threats may realistically impact the organization.

In security management, it is a common difficulty to address how many security controls are required for the organization to be 'adequately protected'. Strategic threat modelling aims to provide information regarding how the organization is situated in relation to the current information security threat landscape. This provides a common baseline of threat actors, their capabilities and most common attack types which can be communicated throughout the organization. This will provide the different teams a standardized starting point for their own system- or network threat modelling, creating more consistent risk assessment results since everyone has the common strategic threat model as a base, which will then be taken into practice in their respective systems.

This thesis consists of background information into the aspects of what affects how organizations are situated in the information security threat landscape and a methodology how this assessment can be made and communicated.

This methodology was put into practice and audited by a Finnish Transport and Communications Agency (Traficom) accredited information security inspection body who were very satisfied by the quality of the threat model.

Keywords	Information Security, Cybersecurity, Threat Modelling, Security Governance, Security Management, Risk Management, Cyberwar, Geopolitics, APT, Nation-State, Hacktivist, Cyber-Terrorism

Tekijä Työn nimi Sivumäärä Päiväys	Ilmari Luoma Strategic threat modelling 45 sivua 20.12.2023
Tutkinto	Master of Engineering
Koulutusohjelma	Information Technology
Ohjaaja(t)	Ville Jääskeläinen, Principal Lecturer

Uhkmallinnuksessa tunnistetaan ja kommunikoidaan tietoa uhista, jotka voivat vaikuttaa tiettyyn tietojärjestelmään tai tietoverkkoon. Strategisella tasolla tämä käsite laajennetaan koko organisaation kattavaksi: Mitkä sisäiset ja ulkoiset uhat voivat realistisesti vaarantaa organisaation päätehtävän toteutumisen ja miten paljon erilaisia suojautumiskeinoja ovat tarpeen.

Strateginen uhkamallinnus tarjoaa yhteisen lähtökohdan uhkatoimijoista, uhkatoimijoiden kyvykkyyksistä ja todennäköisimmistä hyökkäystavoista, jotka voidaan sitten viestiä organisaatiolaajuisesti.

Tämä antaa eri tiimeissä organisaation sisällä vakioidun lähtökohdan kullekin järjestelmätai verkkokohtaiselle uhkamallinnukselle, minkä johdosta syntyy tasalaatuisempia riskiarviointituloksia, koska kaikilla on käytössä yhteinen uhkamalli, jota vastaan riskejä arvioidaan.

Tämä opinnäytetyö koostuu taustatiedoista siitä, mikä vaikuttaa organisaatioiden sijoittumiseen tietoturvauhkaympäristössään sekä metodologiasta, miten tämä sijoittautuminen voidaan määrittää ja viestiä organisaation sisäisesti.

Metodologian auditoi Suomen Liikenne- ja viestintäviraston (Traficom) akkreditoima tarkastuslaitos hyvin lopputuloksin.

Avainsanat	Tietoturvallisuus, Kyberturvallisuus, Uhkamallinnus, Turvallisuusjohtaminen, Geopolitiikka, APT, Valtiollinen Toimija, Haktivisti, Kyberterrorismi

Contents

Preface
Abstract
List of Abbreviations

1 Introduction 1

2 Organization Introduction 4

3 Method and Material 5

3.1 Reliability and Validity 5

4 Introduction to The Threats of Cyber 6

4.1 Target Acquisition 6
4.2 Threat Actor Categories 7
4.2.1 Threat Actor Sub-Categories 8
4.3 Attack Tools 9
4.4 Tactics Techniques and Procedures 10
4.5 Attacker Motivations 11
4.5.1 Financial Motivation 12
4.5.2 Political Motivation 22
4.5.3 Other Motivations 36

5 Strategic Threat Modelling 39

5.1 Establishing the Organizational Presence 40
5.2 Establishing the Threat Actor Landscape 40
5.3 Establishing the Threat Actor Capabilities 41
5.4 Form Synthesis 41
5.5 Conduct a Risk Assessment 41
5.6 Prepare a Mitigation Strategy 43

6 Results and Analysis 43

6.1 Discussions and Conclusions 44
References

List of Abbreviations and terminology

Abbreviations

APT	Advanced Persistent Threat
API	Application Programming Interface
BEC	Business Email Compromise
CaaS	Crime-as-a-Services
CEO	Chief Executive Oficer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CVV	Card Verification Value
DDoS	Distributed-Denial-of-Service
ENISA	The European Union Agency for Cybersecurity
EUROPOL	European Union Agency for Law Enforcement Cooperation
ICS	Industrial Control System
ISF	Information Security Forum
IOCTA	Internet Organized Crime Threat Assessment
MSP	Managed Service Provider
PHI	Protected Health Information
PII	Personal Identifiable Information

TDS	Traffic Direction Systems
VPN	Virtual Private Network
OSINT	Open Source Intelligence

Terminology

Doxxing	Publishing PII on the internet
Useful Idiot	a naive or credulous person who can be manipulated or exploited to advance a cause or political agenda
Zero-Day	A vulnerability that is not known publicly

1 Introduction

The Strategic Threat Modelling provides answers to the fundamental question of: “Are we secure enough?”

Modern organizations can have hundreds, thousands or tens of thousands different assets running instances of services which all have unique process weaknesses, configuration flaws and inherent software coding errors. These are all called collectively “vulnerabilities”. The aim for threat modelling is to identify where the attacker could exploit the existing vulnerabilities and then, as the threat scenarios have been identified, threat mitigation activities can be planned and implemented as part of the development or administration cycle.

There is no one all-encompassing method to secure every variation of implementing a specific system or technology. Often best practices are available; however, they don’t consider the unique implementation that each organization has with the specific technology. Threat modelling helps in bridging the gap of the best security practices and the practical implementation of the system or technology within the context of the unique use-case of the organization in question.

Threat modelling uses different techniques to create a model or a scenario of a threat that impacts a system, a group of systems or a network. In a specific system there could be a design flaw in authentication which would enable the attacker to bypass a systems user login screen and gain access to an administration panel they shouldn’t have access to. Another instance could be that trusted third party sends malicious code through an approved API (Application Programming Interface) and as a result the third party receives data, that they shouldn’t be able to. These situations are threat scenarios, which could be discovered using threat modelling. This would be carried out by examining the system architecture and assessing ways how an unauthorized person could misuse the existing capabilities assigned to regular users or break/circumvent the security controls currently in place.

On average, a cyberattack is detected once every 39 seconds and 44 records are stolen every second[2,49], which gives perspective on the permanently contested state of cyberspace. However, these attacks don't impact every organization and are not performed by an equally skilled and similarly motivated homogeneous group of people. There are individual hackers, hacktivists, loosely organized criminal groups, professional cybercriminal organizations and nation-state actors all who have different skillsets and targets. Just as there are thousands of different criminals and hundreds of different types of criminal groups, there are also hundreds or thousands of assets in an organization and dozens, hundreds or thousands of software engineers, software architects and system administrators with each having different backgrounds, skillsets, and differing views on the relevant threats targeting the system they're constructing or maintaining and what security controls are adequate in securing them.

Strategic threat modelling aims to raise level of abstraction from a system or network perspective to the organizational perspective while retaining the core concept of threat modelling:

> Threat modelling is the process of identifying and communicating information about threats that may impact a particular system or network, or on strategic level, the organization.

On strategic abstraction level this means examining the organization as one big ecosystem and identifying where the organization is situated in the bigger threat landscape. The threat landscape is an overlap of multiple different threat profiles such as follows:

- The size of the organization
- The industry the organization operates in
- The clientele they have
- How they are situated in different supply chains
- How they are perceived publicly
- Their Geographical footprint

Each of these present their own portfolio of threat actors and associated risks. For example, if the organization has a lot of clients that are part of national critical infrastructure that would place them more susceptible to attacks from a nation state, that is targeting their clients or if the organization is perceived publicly as favouring a controversial political or ecological topic, they are more susceptible to attacks from hacktivist groups.

When the organization has oriented themselves on the threat landscape they can prepare organization-wide mitigation strategies that bridge their threat portfolio, organizational culture, and their security management approach as the teams inside the organization have a common understanding what is the threat they are securing against.

This thesis produced a methodology to establish the organizational position in the bigger threat landscape, identify the most relevant strategic threats to the organization and prepare mitigation strategies to reduce the information security related risks to fit the risk appetite of the client.

The basis for this type of approach requires identifying the information security related risks associated with the new venture the organization is participating in. The strategic threat modelling task in this project consisted of the following deliverables:

- Identification of the most relevant threat actors
- Assessment of the capabilities of the threat actors
- Assessment on the likelihood of initiating the attack(s)
- Assessment of the most likely attack strategy
- Assessment of business impact of the attack(s)
- Risk analysis based on the assessments
- Mitigation strategy for reducing the risk to meet the organizational risk appetite

The deliverable for CGI was the standardized methodology for performing Strategic Threat Modelling.

The deliverable for the Client was a risk assessment and a mitigation strategy. The actual implementation of the strategy is out-of-scope for the purposes of this thesis.

The thesis has been divided into three (3) logical sections, the first of which presents the differences of different threat actor types, the second section covers how to address these different types of groups utilizing Strategic Threat Modelling and the third section consists of the end results and the analysis of the findings.

2 Organization Introduction

CGI Suomi Oy is a subsidiary of the international IT service provider CGI Inc. The name is abbreviation from French and stands “Conseillers en Gestion et Informatique” (Information Systems and Management Consultants). In English the acronym stands for Consultants to Government and Industry. This particular CGI regional subsidiary is internally called a Strategic Business Unit of Finland Poland and Baltics (FPB) which covers CGI regional offices in Finland, Poland, Estonia, Latvia, and Lithuania. [3]

CGI Suomi Oy Clients can be either regional from one of the forementioned regional countries or global organizations with regional operations in Europe, especially in the Nordics or Baltic region.

In Helsinki, CGI has a regional Cyber Security Center, which is a part of the Cyber Clients unit in CGI that provides services to CGI Clients either as direct contracts from the Cyber Clients unit or as part of the services provided by other units in CGI like managed IT services, software development or consultancy services.

The Client is a large global ICT Managed Service Provider (MSP) operating with public and private sector clients and this project is part of the supply chain for national critical infrastructure.

The Client organization has a contractual requirement to provide a new service in adherence to a strict security framework that requires a risk-based approach into information security instead of more traditional ‘control-based’ security.

The geographical region is in Europe with focus on the operations in Finland.

3 Method and Material

The prepared methodology relies on several external sources for information that require contextual and allegiance analysis. Especially matters related to nation-state actors, the reports and announcements can have a bias towards a specific coalition or national interests.

The content of the assessment was mostly a cross-reference, compilation and analysis of reports, and official studies of different types of phenomena gathered from a variety of sources that are generally considered as reliable sources of information in the field of information security. Two examples of these types of sources are The European Union Agency for Law Enforcement Cooperation (EUROPOL) and The European Union Agency for Cybersecurity (ENISA).

3.1 Reliability and Validity

There were three general guiding principles in ensuring the reliability and validity of the information in the Strategic Threat Model:

1. The source needs to be acknowledged in the field of Information Security

2. Two mutually independent sources must align with the statement for it to be accepted into the threat model

3. In case of conflicting data the source closer to the event takes precedence (usually the target or the organization investigating the event)

Some of the material is confidential from the Finnish Security and Intelligence Service, the National Cyber Security Centre, from the Client and from our own organization. These sources are considered highly reliable for the context of this thesis.

The results and methodology were peer-reviewed inside our own organization, then presented to the Finnish Security and Intelligence Service and to the National Cyber Security Centre. After that they were approved by the responsible organization, and finally

audited by a Finnish Transport and Communications Agency (Traficom) accredited information security inspection body with the following comments (excerpt from the classified report, published with Client permission):

> "Threat assessment composed by [redacted] describes comprehensively and analytically threats related to the project. Threat modelling utilizes extensively the available national material and has identified threats related to [redacted] , [redacted] and [redacted]. Threat assessment provides good foundation for risk management. Based on the threat assessment [redacted] has prepared a mitigation strategy to reduce the threats."

Original statement in Finnish:

> "[redacted] laatimassa uhka-arviossa on kuvattu kattavasti ja analyyttisesti projektiin liittyviä uhkia. Uhkamallinnuksessa on käytetty laaja-alaisesti saatavilla olevaa kansallista aineistoa, kuten viranomaisten omia turvallisuustilanteeseen ja -uhkiin liittyviä aineistoja ja tunnistettu [redacted] , [redacted] ja [redacted] kohdistuvia uhkia. Uhka-arvio antaa hyvän pohjan riskienhallinnalle. Uhka-arvion perusteella [redacted] on tehnyt mitigointistrategian uhkien pienentämiselle."

4 Introduction to The Threats of Cyber

This section provides insight to how cyberattacks are carried out. This section describes how potential targets can be discovered, what level of technical capability is required and what types of targets different groups are interested in.

4.1 Target Acquisition

Services such as Shodan, Censys and ZoomEye scan the public IP address range and provide data on internet-connected devices, such as technologies in use, vulnerabilities, and asset owner data. This information is publicly available, and this information can be used to find and identify potential targets that match the attackers' skillsets.

Some attackers establish their own scanning infrastructure, and it can be accomplished with marginal expenses as many of the tools necessary are distributed under Open Source -license and servers can be deployed with little-to-no cost in cloud services.

If the attacker does not possess the technical capability to discover targets using scanning, they can use other mechanisms for finding targets, such as experience in a specific industry, willingness to go through companies public records on the status of their financial situation, or utilize an Initial Access Brokers, who sell access to organizations. Then

they can purchase different types of attack capabilities as a service from other cyber-crime vendors. This is called Crime-as-a-Services (CaaS) business model.

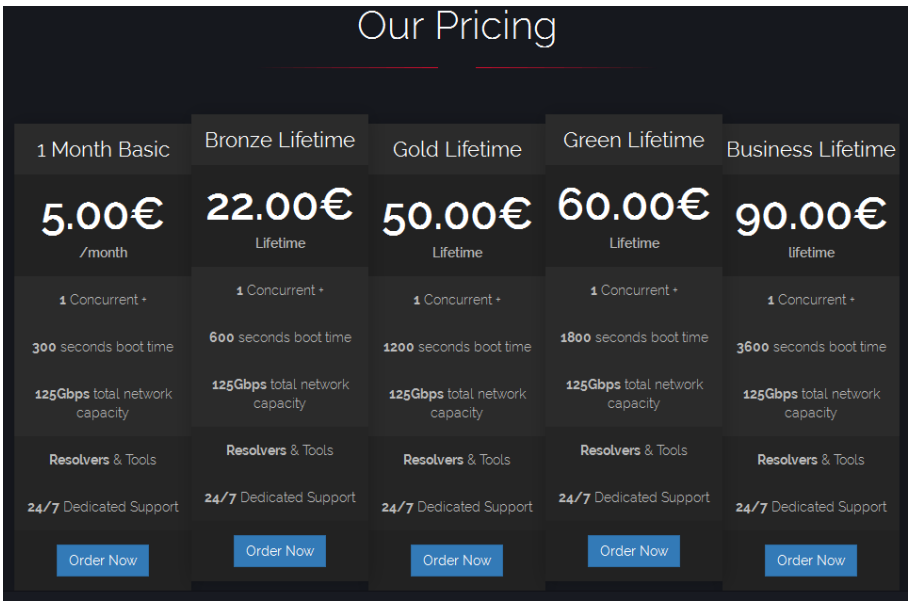


Figure 1. The price list for one of the biggest black market services offering DDoS attacks[1]

4.2 Threat Actor Categories

Certain actors operate on an opportunistic mindset, compromising any target of opportunity, big or small. These are called **Opportunistic Attackers**. Their business model operates mainly on sheer volume of automated or semi-automated attacks.

Other actors focus on a specific demographic, which can be a specific industry, a specific technology, big organizations with established revenue. These groups usually have some connection with the chosen demographic, meaning that they have insight what to target to cause the maximum amount of damage to the organization. These are called **Specialized Attackers.**

If the actor is performing cyber-attacks to promote political agenda, social change or as a form of civil disobedience then the actor is called a **Hacktivist**.

If the actor is operating on their own and the cyber-attack has no direct affiliation to a specific group or an operation performed by a group the threat actor is called an **Individual Hacker**.

If the actor is performing activities that constitute as terrorism, or provide financial support, recruitment or activities that are meant to support an ongoing terrorist attack for the benefit of a terrorist organization, these actors are called **Cyber-Terrorists.** The term Cyber-Terrorist is an ambiguous because the definition of the parent word 'Terrorist' is ambiguous, since multiple regional and international definitions exists what constitutes as terrorism, similarly as to how the term "Cyber" links to the parent word of terrorism.

In some cases, the target of the cyber-attack can be derived from the execution of objectives stated in a foreign, domestic or military policy of a nation-state. If the actor is operating as part of a nation-state governmental entity, they have governmental authority delegated to them or if they are de facto in command of the other entity that is performing the operation, they are called **Nation-State Actors.**

4.2.1 Threat Actor Sub-Categories

If the actor is operating with direction or support of a nation-state, but not in the way described in Nation-State Actor category definition, they are called **Nation-State Proxies.** These have an overlap with Nation-State Actors and Specialized Attackers and some of these groups can also be designated as APT groups. If the group is unaware that they are operating with direction or support of a nation-state and they are progressing the national policy agenda, they are called **Useful Idiots** and can overlap with any main Threat Actor Category except Nation-State Actor.

An **Advanced Persistent Threat** (APT) group is a commonly used term to define a group that operates with a high level of capability and in a professional manner. These groups are the high-tier performers from Specialized Attackers and Nation-State Actor categories and Nation-State Proxy sub-categories.

Script Kiddies are low capability hackers that use commonly used simple tools and scripts. They are part of Opportunistic Attackers or Individual Hackers main categories.

If the actor is performing activities that are damaging the organization the attacker is working for, but the attackers aren't aware that they are performing a cyber-attack they are called **Unintentional Insiders.** Whereas if they are aware that they are performing a cyber-attack, they are called **Intentional Insiders.**

Black Hat is a general term for intentionally malicious attackers. The definition does not have indication on the actual capability. Covers every Threat Actor main category mentioned before except Unintentional Insider.

Grey Hats are an ambiguous group which can mean 1) an attacker who targets organizations out of curiosity but does not have a malicious intent, or 2) they publish material on what they did but do not disclose who was the target, or 3) publish in social media what they did and tag the organization they breached but did nothing malicious inside the system. These fall into the Opportunistic Attacker, Specialized Attacker, Hacktivist, Individual Hacker, Intentional Insider main categories and the Grey Hat designation does not consider the capability of the actor.

White Hats are security professionals who operate ethically with no malicious intent. They can be part of Unintentional Insiders category. Designation does not consider the capability of the actor.

4.3 Attack Tools

There are a lot of different types of tools that are available for different sets of skills. An easy example from the lower capability tier is Armitage, which is a User Interface for Metasploit. Armitage is much more accessible for less technically capable than the command-line based interface of Metasploit.

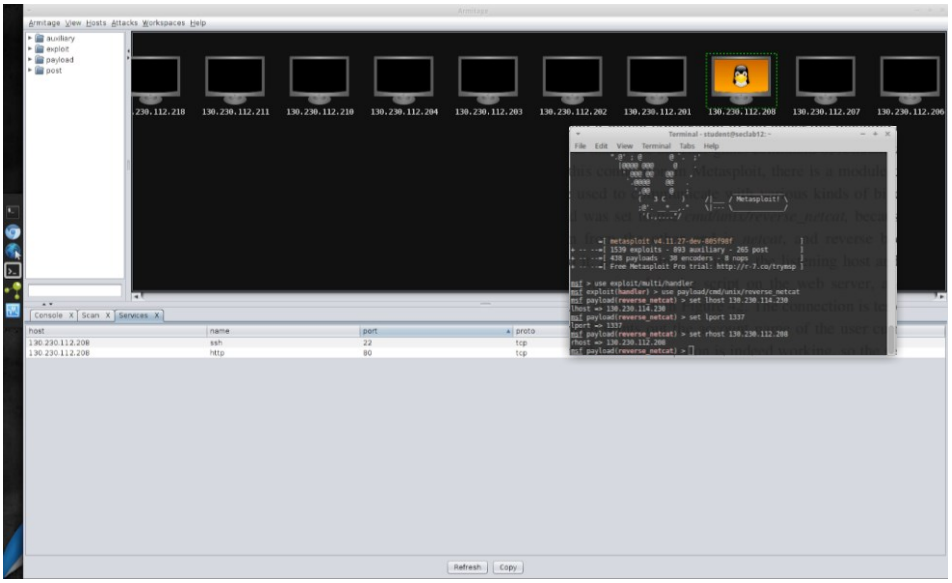


Figure 2. Armitage GUI (background) and Metasploit terminal (front)

For the attackers with higher capabilities classified nation-state developed tools can be made available for other groups after the tool has been discovered and reverse engineered.

Case in point: In 2017 a hacking group called The Shadow Brokers published hacking tools and Zero-Day (a vulnerability that is not known publicly) exploits developed by the National Security Agency (NSA) of the United States. One of the tools was an exploit that targeted Microsoft Windows file sharing services called 'EternalBlue'.[4] This exploit was then used by a hacking group 'Lazarus' in a ransomware attack which encrypted over 300 000 assets globally.[5] One month later that the exploit was used by a hacking group called 'Sandworm' to encrypt most of the Ukrainian critical infrastructure and most of the ICT assets of a logistics company Maersk.[6]

4.4 Tactics Techniques and Procedures

Different hacking groups have different compositions and as such they all operate differently. For initial access a group can choose to breach the organization directly by exploiting vulnerable systems visible on the internet. Other group may use phishing attacks to manipulate users into providing their credentials and some group may utilize malicious USB drives.

Once they are inside the propagation depends on their skillsets. If they have limited Linux Operating System knowledge, their attacks can be limited to Microsoft Windows systems. If they have no ICS (Industrial Control System) knowledge but have Linux and Windows expertise, their attacks might affect assets that operate using these traditional Operating Systems while leaving the proprietary Operating Systems of ICS systems out of scope.

Finally, the actions they perform on their objective is based on their motivation for initiating the attack.

4.5 Attacker Motivations

This chapter provides information on different motivations that the attackers have for targeting different organizations. The motivations are divided into Financial Motivation, Political motivation, and Other Motivation.[7]

Nation-State Actors derive their targets and objectives from their national policies and Specialized Attackers are motivated by financial gain. These objectives can align, and a Specialized Attacker can have one revenue stream from a nation-state, another revenue stream from their target organization and a third one from the individual people involved in the cyber-attack. [7, 8, 10]

Hactivists goal is to spread their ideology and Cyber-Terrorists fund their terrorist cell, they recruit new members, and progress their political agenda. Individual Hackers operate based on their own individual principles and ideology.[7,11]

Threat Actor Category	**Motivation**
Opportunistic Attackers	Financial gain
Specialized Attackers	Financial gain
Hacktivist	Ideology
Cyber-Terrorists	Ideology
Nation-State Actors	National policy
Individual Hacker	Financial gain Ideology Vengeance Capability demonstration

Case in point: In 2013 an American retail corporation Target suffered a security breach which exposed 110 million customers private information such as credit card details and personal information. This information can either be used in online fraud or be sold for someone else.[9]

In 2019 multiple organizations were breached as a Chinese Nation-State Actort called ‘Menupass Team’ or ‘APT10’ utilized ICT Managed Service Providers (MSP) to pivot their attack against the MSP clients in a global cyber-espionage campaign. [39]

In October 2020 it became public that a Finnish psychotherapy center had suffered a databreach in which over 33 000 patient records were exfiltrated from their database.

The Individual Hacker extorted money from the psychotherapy center and from the patients whose treatment records were leaked. [10]

4.5.1 Financial Motivation

Cybercrime can be divided into two distinct fields: Cyber-dependant and Cyber-enabled crime. Cyber-dependent crime is performed using computers and computer networks, such as Distributed-Denial-of-Service (DDoS) attacks, whereas Cyber-enabled crime is traditional crime that has shifted into computer networks such as payment fraud. Different criminals and criminal groups operate in one or both areas.

Revenue can be generated either directly or indirectly. Direct revenue models gain the revenue directly from the target, whether it is a common citizen or an organization. Indirect revenue models provide income based on actions performed by others, such as affiliate programmes. [8]

In 2023 report published by Europol described three of the most profitable revenue streams:

- Deny the use of ICT infrastructure by encrypting the assets and then perform extortion in order to the organization regain use of their assets
- Exfiltrate sensitive data prior to encryption and extort the organization and threaten to disclose the data
- Extort by threatening to launch DDoS attacks against organizational assets

In addition to these revenue models the following revenue models are also widely used by all financially motivated Threat Actor categories:

Cryptocurrency mining in Cloud Environments: If the cloud environment has been deployed so that it automatically increases capacity when the system resources exceed a set threshold, then a crypto currency miner can be very effective in converting CPU capacity into cryptocurrency.

Extorting individuals: If the attacker has exfiltrated PII (Personal Identifiable Information) or PHI (Protected Health Information) and then threaten the individual for disclosing the information

Access Brokering: Access to any vulnerable device, be it an end user workstation, an on-premises server, a cloud server, an IoT device or a network device can be sold (Initial Access Brokers). The asset can then be used as a part of a botnet, or the organization can be targeted by ransomware.

Utilize as a supply chain attack vector: Use the VPN (Virtual Private Network) and integrations available in the organization to target their partners, clients and subcontractors.

CEO fraud: Misdirect corporate funds by impersonating as the CEO (Chief Executive Officer) or CFO (Chief Financial Officer) or vendor and social engineer the employees to perform unsolicited money transfers. Can also be amplified when combined with BEC (Business Email Compromise). This will allow to use real emails and existing trust relationships between individuals from different organizations.

The Hacker Black Market Ecosystem

In the early mid 2000s the black market revolved around Cyber-Enabled Crime such as selling drugs and selling credit card data. Now the ecosystem has evolved to accommodate the rise of social media and eCommerce, global accessibility of the internet and the general progression of software maturity from hard-to-use custom scripts to easy to use graphical user interface tools. The following chart demonstrates the decline of the necessary skill-level of the intruder and the sophistication level of the attacks. [12-14]

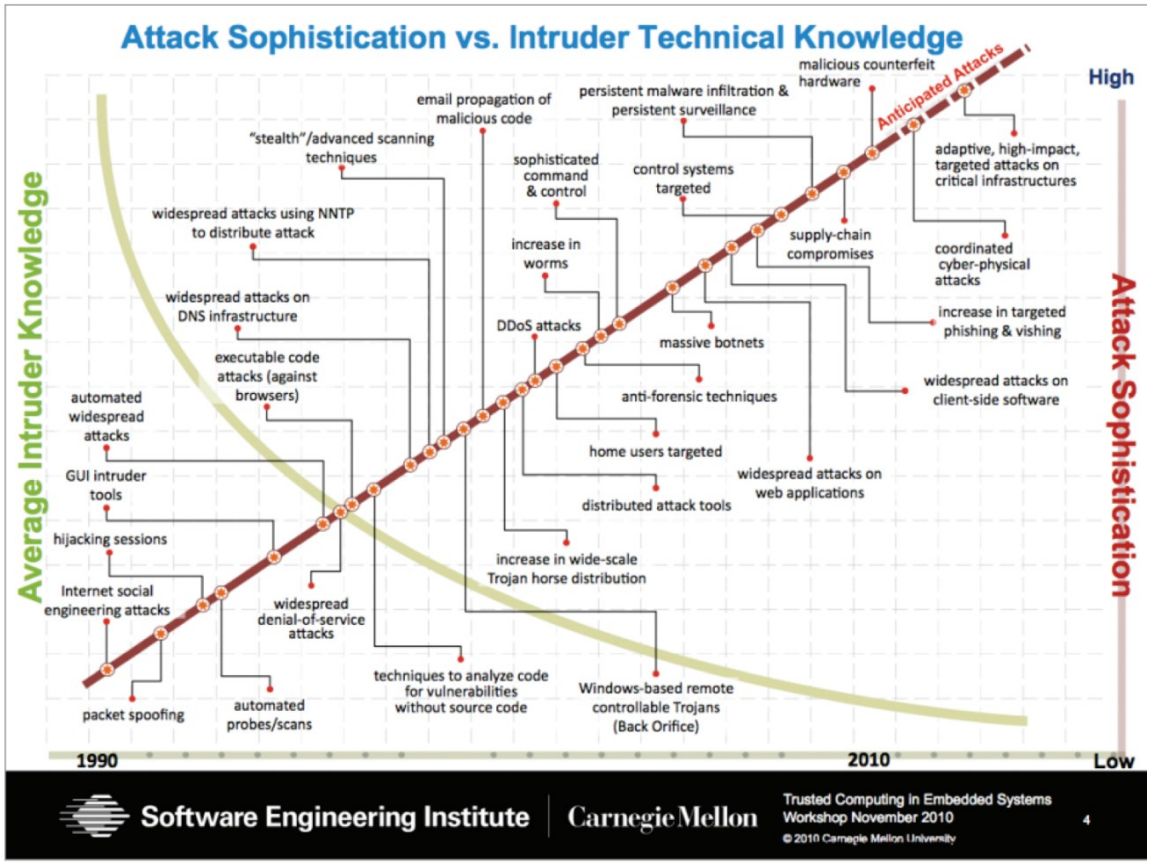


Figure 3. Increase in sophistication and reduced requirement for knowledge[13]

As the market has become more open to actors with differing level of technical capability the population operating in the black-market ecosystem also rises significantly and has made the environment more appealing to people with other talents than just hacking, such as people with more of a business acumen and group organization skills and the 'hacking' has only more of instrumental value for achieving their goals.

The trend seems to be that the ratio of individuals and criminal organizations seems to be changing rapidly. They estimate that in mid 2000s criminal organizations were responsible for approximately 20% of cybercrime activities and in the beginning of 2010s the amount was approximately 80%.[13]

A smaller number of highly skilled participants and service vendors are providing service components for intermediaries, other service providers and brokers. This can be examined as a proportion diagram below.

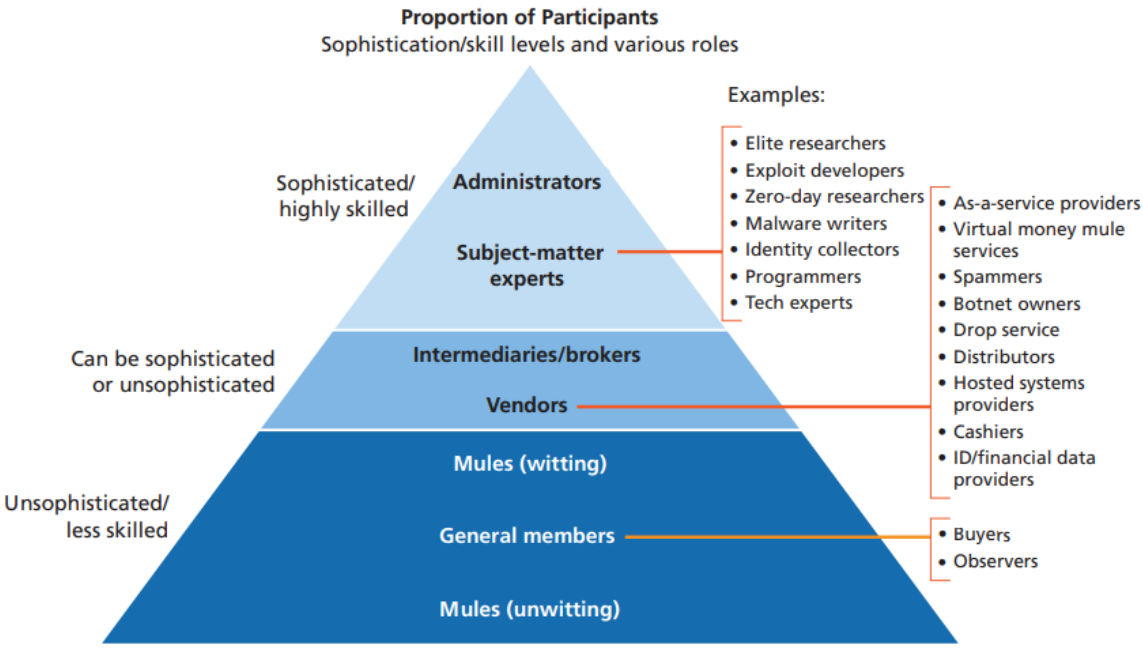


Figure 4. Proportion of different actors in cybercrime economy[13]

This observation by Juniper is reinforced later in the Crime-as-a-Service section, where I have presented an Europol infographic that is a part of the Internet Organized Crime Report 2023 that illustrates the inner workings of a modern Ransomware-as-a-Service business.[14]

In an ecosystem model there are different actors, each providing a different function for the cybercrime community. The model presented here is not intended to be exhaustive, just to help understand the key components of the ecosystem.

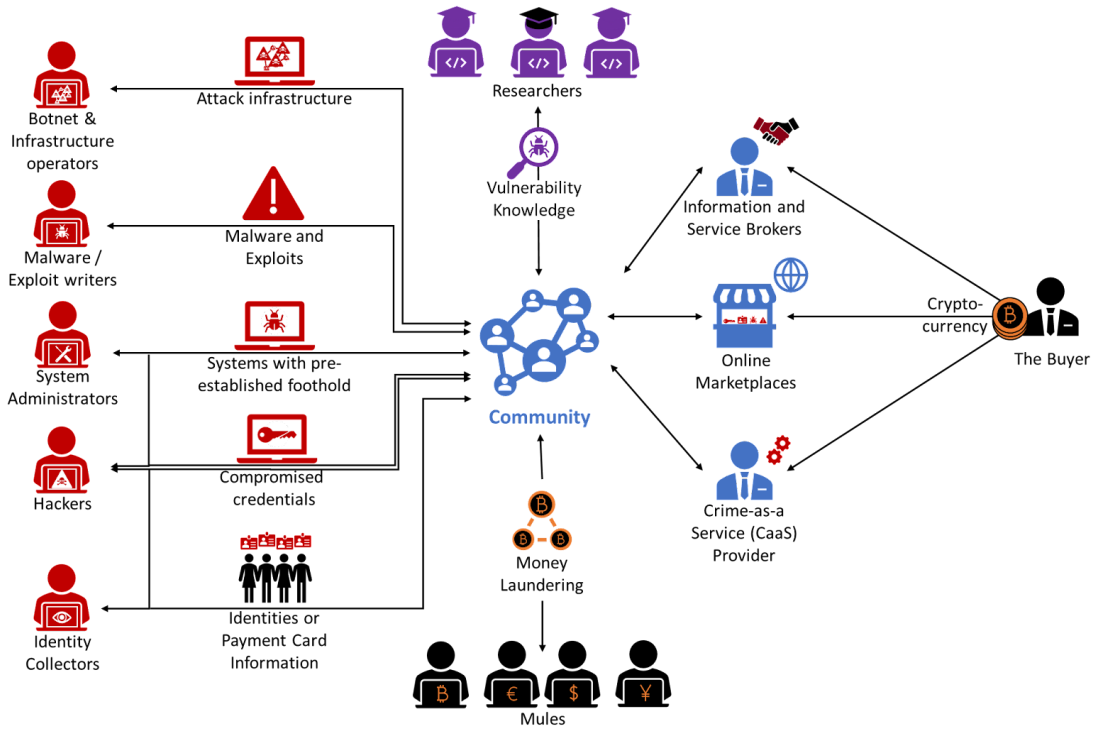


Figure 5. Illustration of the components of the ecosystem

The next section provides additional information on the key segments of the ecosystem: the Buyers, the Service Providers, Researchers and Mules.

The Buyers

Buyers are interested in obtaining illegal items such as payment card information, legitimate online and offline identities, compromised credentials, initial access points inside organizations, skillsets their group is currently lacking or other services the community can provide. For example, the buyer might be an Industrial Control System specialist who has inital access to the organization and has intricate knowledge how to compromise ICS systems but lacks the knowledge of breaching office desktop environments.

An exploit acquisition organization ZERODIUM offers 2 500 000 $ and above for certain zero-day vulnerabilities. While the legality of placing a bounty for an exploit varies country to country, there are also ethical considerations in placing a bounty for an attack tool against a commercial organizations' product. [15]

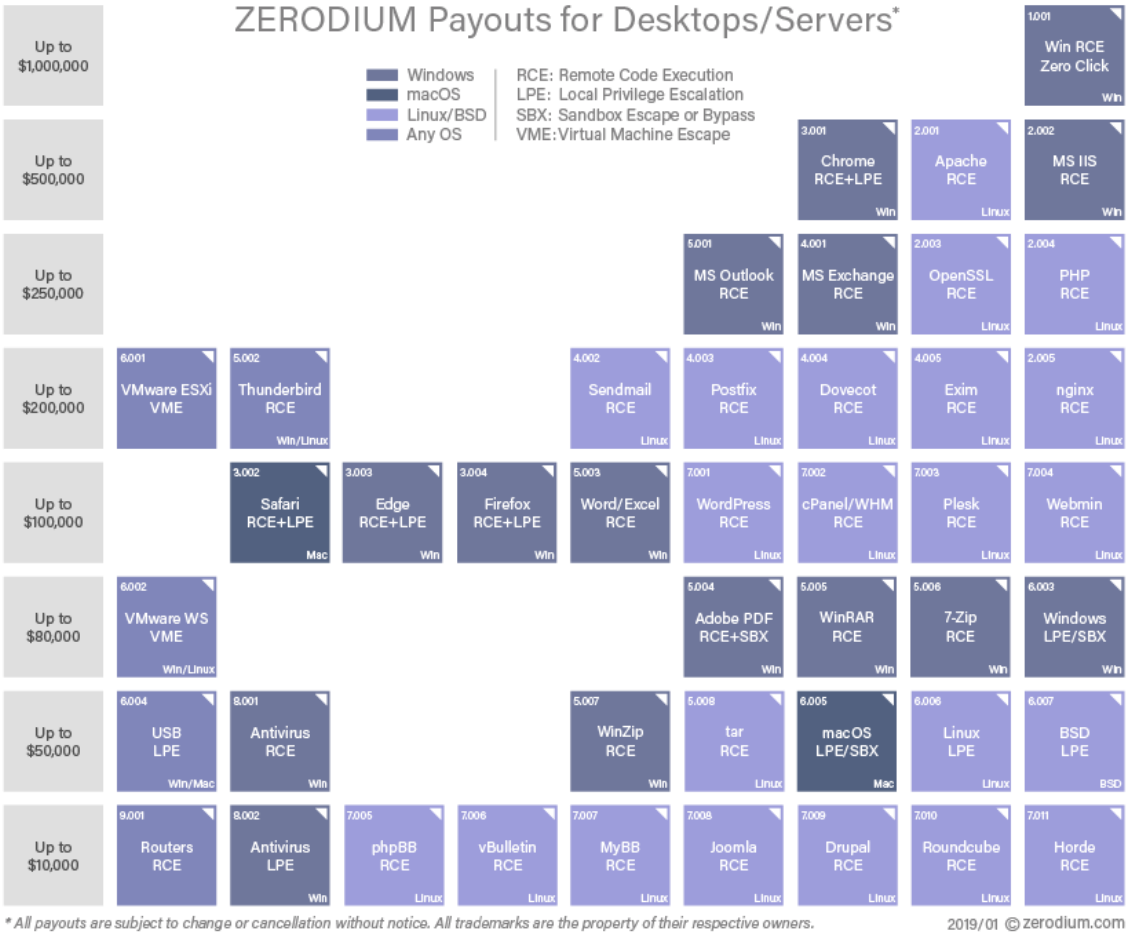


Figure 6. Picture: ZERODIUM Payouts for Desktops/Servers

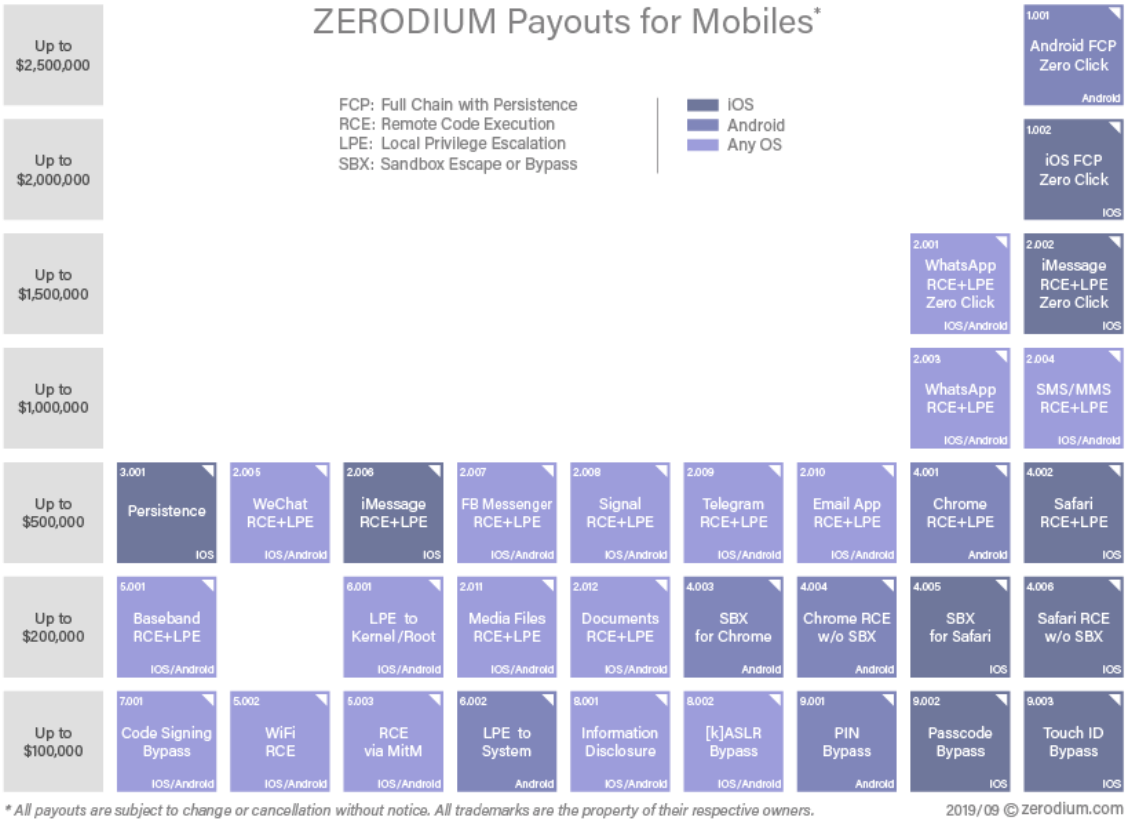


Figure 7.Picture: ZERODIUM Payouts for Mobile devices

Sometimes the organization finding an exploit has an existing collaboration with the target.

Case in point: The EternalBlue exploit, attributed to the National Security Agency of the United States of America targets a variety of Microsoft products while Microsoft was a participant of NSAs PRISM programme under the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008.[16]

Information Security Researchers

Information Security Researchers provide knowledge of vulnerabilities, and other types of phenomenon regarding information security community. Depending on the nature of the research and the position of the researcher, some research is public, some research is open for purchase and some is confidential. The people performing research are universities, national organizations, private companies and individual researchers.

Crime-as-a-Service

A cyber security software company Trend Micro published a research paper on the Russian underground black market in 2015 where they studied 78 underground markets, they renewed the research in 2017 and further analysed the underground black market in 2020. [17,18,20]

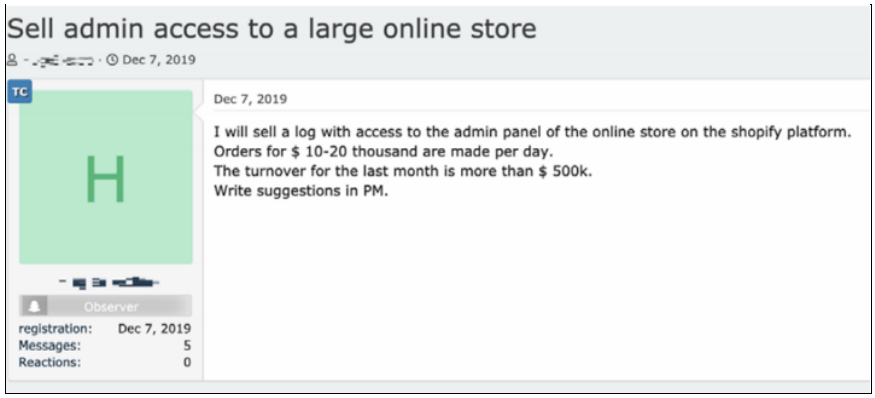


Figure 8. Advertisement for administrator level access to an online store[19]

Trendmicro and Armor have presented a large collection of hacking and support services provided on the underground market. Here are some of the services they discovered: [17-20]

- **Bulletproof hosting services:** Anonymous servers used to store malware, exploit kits, function as command-and-control channels or data exfiltration points. Located in countries which don't have a national CERT (Computer Emergency Response Team) or otherwise have limited capability to respond to cyber incidents and the company hosting the assets doesn't respond to information requests from law-enforcement.
- **Access-as-a-Service:** Access to specific organizations are offered as a service
- **Crypting services:** Different types of cryptographic ransomware services, either encrypton software only or also delivery, deployment and extortion money handling
- **Malware/Exploit writing:** Malware, rootkits and exploits are for sale and also delivery schemes
- **Account hacking:** Services are provided to hack specific accounts or acquire accounts from a specific organization
- **DDoS as a service:** High bandwith denial of service attacks

- **Money laundering:** Buying plane tickets, booking expensive villas or for a larger commission the money can be laundered using corporate accounts.
- **Translation services:** For social engineering attacks (such as phishing) translators provide services for their specific language.
- **Fake proof-of-identity call receiving:** Banks and online payment services make proof-of-identity calls to verify the owner of a bank account or payment card. These people answer the call and verify the identity.
- **Drop-as-a-service:** Rental service where people cash in payment cards or accounts.
- **Log mining:** Criminals purchase logs and analyse them if they hold some interesting information such as identities or credentials.
- **Antispam proofing:** Specialists help their clients to structure their spam e-mail in such a way that it bypasses different e-mail filtering techniques.
- **Payment card validity checking:** Services are provided to determine if a payment card is valid or not.
- **Traffic Direction System Services**: Traffic Direction Systems (TDS) are used to control traffic between websites. Parameters can be set to control traffic flow for example from a specific country of origin, or browser type and this can be used to increase the efficiency of attacks that target specific population
- **Malware delivery:** Malware delivery as a Pay Per Install basis with guarantee of a certain number of successful infections.

The marketplaces also exist for selling information, such as follows:

- **Payment card information**: Credit card numbers, owner details and CVV (Card Verification Value) numbers
- **Stolen SSH and RDP access to computers**: Usually the level of access and some general information about the device is provided
- **Desktop RDP access:** Compromised desktops (not servers) that are automatically scanned for social security numbers and account details
- **Scanned and forged passports and identification cards:** Scanned real or fake passports and identification cards for online identity verification checks
- **Full personal identity:** For assuming the identity provided, there usually is a passport or an identification card, name, address, etc.

Figure 9. Europol Infographic – Ransomware Groups (IOCTA 2023 report appendix)[8]

Based on Cobalt Labs statistics in 2023 the average ransom paid is approximately 1,5 million US dollars. [21]

The Ransomware-as-a-Service providers receive a portion of the money extorted from the victims. For example the BlackCat/ALPHV group takes 10-25% of the extorted amount, depending on the amount paid. The price points are 25% for extortions of less than 0,5 million US dollars, 20% for less than 2 million US dollars and 10 % if the amount is greater than 5 million US dollars.[22]

4.5.2 Political Motivation

This chapter provides information on Nation-State Actors, their strengths and overall capabilities and also some additional information is provided regarding some of the key players. The assessment of the Nation-State Actors is based on Harvard Belfer Center report National Cyberpower Index 2022.[23] The study utilizes Open Source Intelligence (OSINT) and ranks the different nation states with eight capabilities:

- Surveilling and Monitoring Domestic Groups (Surveillance)
- Foreign intelligence Collection for National Security (Intelligence)
- Strengthening and Enhancing Cyber Defenses (Defence)
- Destroying or Disabling an Adversary's Infrastructure and Capabilities (Destructive)
- Controlling & Manipulating the Information Environment (Information Control)
- Growing National Cyber and Commercial Technology Competence (Commerce)
- Amassing & Protecting Wealth (Financial)
- Defining International Cyber Norms and Technical Standards (Norms)

On the next pages the different nations are ranked based on their overall capability and based on their capabilities regarding the 8 different categories.

Category	Highest capability
Overall Cyber Power	1. United States 2. China 3. Russia
Surveillance	1. China 2. Vietnam 3. Iran
Intelligence	1. United States 2. China 3. United Kingdom
Defence	1. Australia 2. Ukraine 3. United States
Destructive	1. United States 2. Russia 3. China
Information Control	1. United States 2. Russia 3. China
Commerce	1. China 2. United States 3. Russia
Financial	1. Democratic Peoples Republic of Korea 2. China 3. Vietnam
Norms	1. United States 2. United Kingdom 3. Singapore

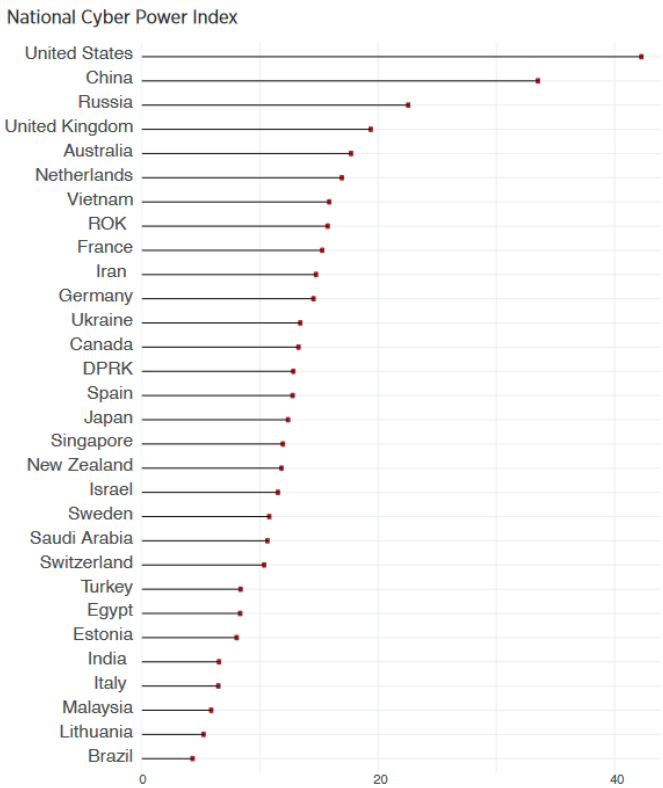


Figure 10. National Cyber Power ranking, top 30

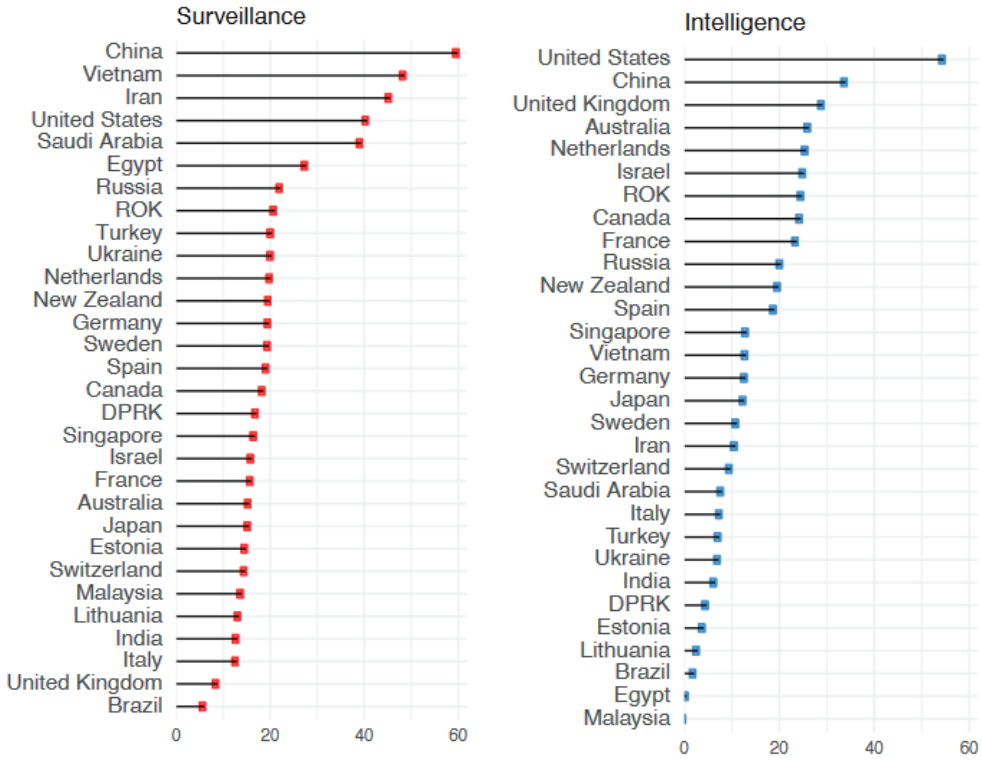


Figure 11. Surveillance and Intelligence capabilities

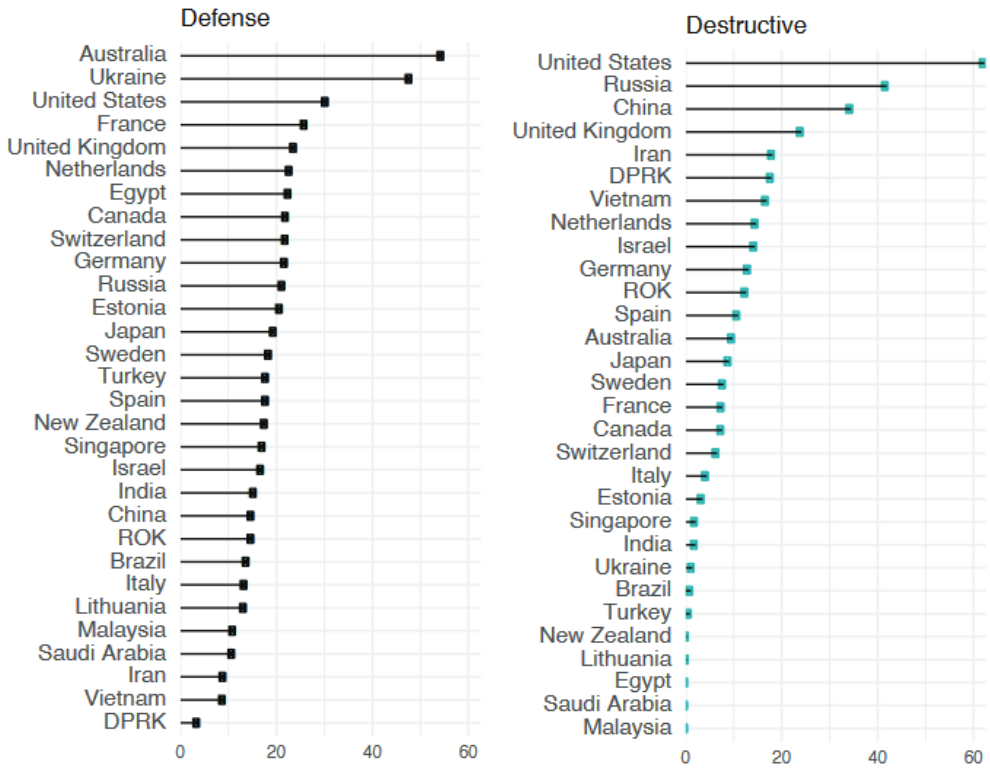


Figure 12. Defense and Destructive capabilities

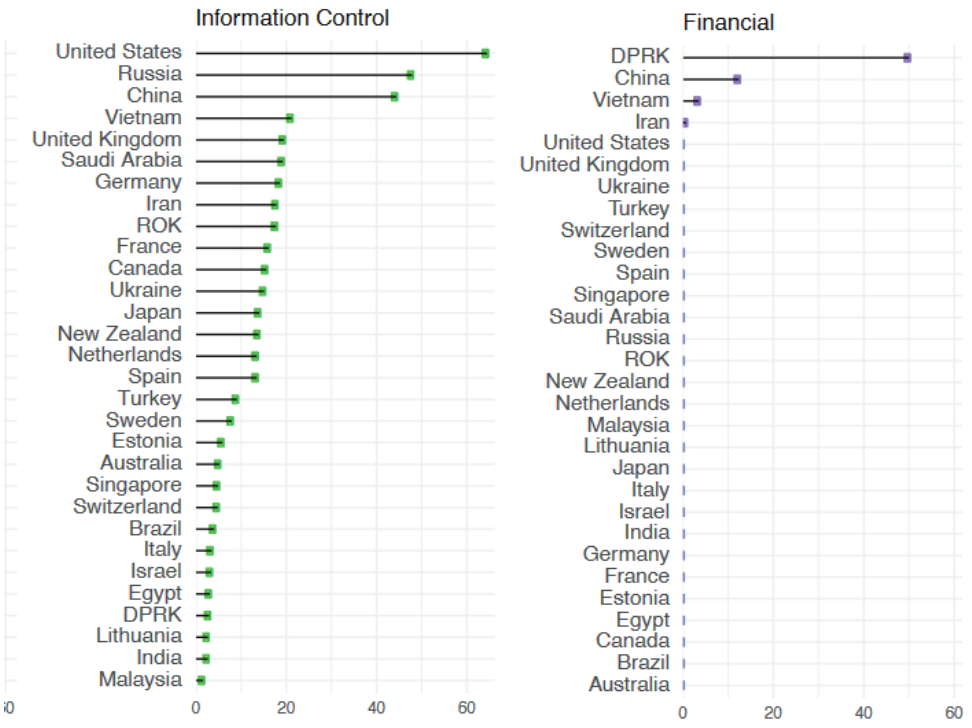


Figure 13. Information Control and Financial capabilities

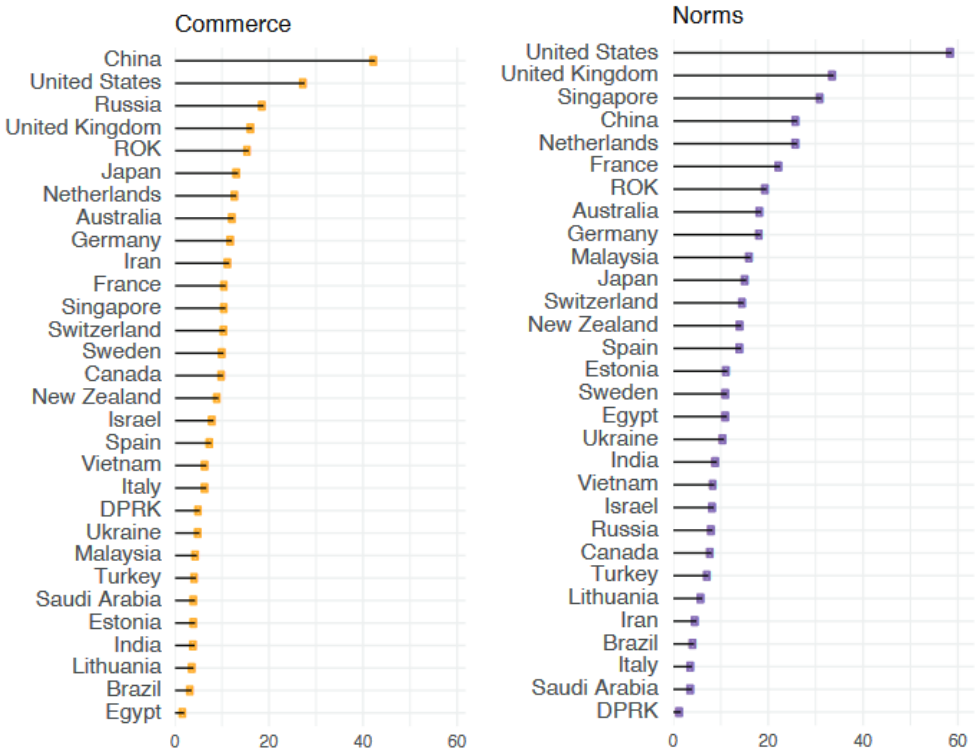


Figure 14. Commerce and Norms capabilities

These results are used in determining the capabilities of different Nation-State Actors and their potential geopolitical interests against a specific organization. It also provides insight on the focus of their political agenda.

The actions of Nation-State Actors are dependent on their national governing policies. They usually operate under their national cyber operations strategy. Depending on the function of the organizational unit, the mission objectives are different. Certain specialists are more focused on intelligence gathering and other specialists operate on destructive operations.

Figure 15. Organization of Russian cyberoperations[24]

Economics of Nation-State Cyber Operations

Cyber Operations are relatively cheap compared to kinetic operations. One Tomahawk missile without any supporting infrastructure or military support units in a kinetic operation would cost approximately 3 million US dollars.[25] If the same could be achieved using a malware like Wannacry, the operational expenses would be approximately 150 000 US dollars.[26,27]

The University of Cambridge Center for Risk Studies approaches the subject from a logistical burden perspective. Each operation requires manpower, expertise, have expenses and takes time to complete. Nation-State Actors operations are based on economics: The benefit gained from the operation must be greater than the cost of the operation. The actor must consider the cost of the operation and if they need to utilize special equipment or a zero-day vulnerability against their objectives. Special equipment and Zero-day vulnerability exploits require cost-benefit analysis because the possibility exists that the equipment or zero-day is detected during the operation and the advantage provided by that capability is lost.[26-27]

The University of Cambridge Center for Risk Studies methodology is as follows: Evaluate the relative difficulty of the cyber-attack and the related costs associated with the attack, then rank the targets that fit the objective according to the cost-benefit analysis.

$$\frac{M_b+P_b}{\mathrm{LB_c}} \geq 1{,}00$$

M_b = Monetary benefit, P_b = Psychological benefit, LB_c = Logistical burden cost

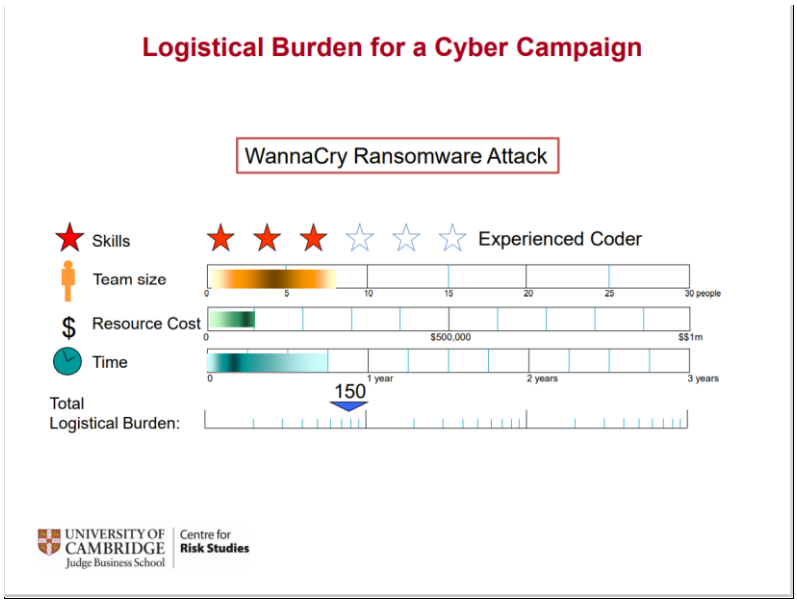


Figure 16. Logistical burden of Wannacry

The logistical burden of North-Korea attributed Wannacry[50] has been estimated to 150 000 US dollars, based on the skills required, malware development team size and time needed. They estimate that the labour costs are 50 000 US dollars to develop and team costs 100 000 US dollars and the operation takes 10 months of calendar time.

Relative Logistical Burden of Different Cyber Attacks

Cyber Attacks	Skill Level	Team Size	Labour Cost	Months	Resource Cost per Month	Team Cost	Total Cost LB Index
Financial Transaction Theft - Upper Stress Test	STOL	60	1,000,000	24	200,000	4,800,000	**5,800,000**
Financial Transaction Theft - Reference	STOL	48	750,000	18	150,000	2,700,000	**3,450,000**
Leakomania - Upper Stress Test	STOL	30	500,000	12	146,000	1,752,000	**2,252,000**
Financial Transaction Theft - Lower Stress Test	Systems Architect	36	500,000	12	100,000	1,200,000	**1,700,000**
Mass DDoS - Upper Stress Test	Systems Architect	12	500,000	12	90,000	1,080,000	**1,580,000**
Mass DDoS - Reference View	Systems Architect	8	300,000	9	90,000	810,000	**1,110,000**
Leakomania - Reference View	Systems Architect	25	250,000	9	90,000	810,000	**1,060,000**
Extortion Spree - Upper Stress Test	Systems Architect	20	250,000	12	50,000	600,000	**850,000**
Mass DDoS - Lower Stress Test	Systems Architect	6	200,000	6	90,000	540,000	**740,000**
Leakomania - Lower Stress Test	Highly Experienced Coder	16	200,000	8	32,000	256,000	**456,000**
Extortion Spree - Reference View	Highly Experienced Coder	16	150,000	8	32,000	256,000	**406,000**
Extortion Spree - Lower Stress Test	Experienced Coder	12	90,000	6	24,000	144,000	**234,000**
WannaCry Ransomware Attack	Experienced Coder	8	50,000	10	10,000	100,000	**150,000**

UNIVERSITY OF CAMBRIDGE Judge Business School | Centre for **Risk Studies**

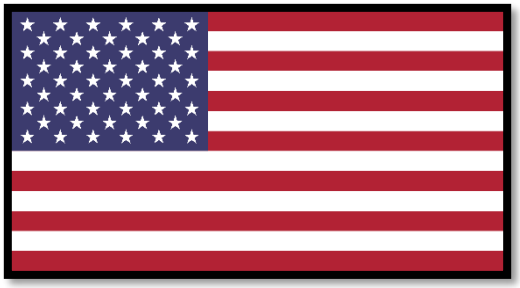
Figure 17. Logistical burden of different cyber-attacks

From organizational perspective Nation-State actors operate on a strategic level and especially when expanding organizational operations to a new region the threat landscape should be updated and Nation-State Actors considered if the new region is actively being targeted by one of the core capabilities of Nation-State Actors. The organization can be targeted as a part of the Nation-State Actor objectives, or it can be hit as a collateral just by operating in a specific region or by implementing a specific technology prominent to the region.

Nation-State Actor espionage can often be used to progress domestic research and development or disrupt the advances in a competing nation or organization. Espionage can also be used as a tool or for political leverage, or for assisting a certain party in decision making.

On the following pages are presented some key players on the nation-state cyber operations theatre. The descriptions are provided as a snippet of their background, motivations, and capabilities within the context of this thesis. They should not be considered as a thorough analysis of their capabilities.

Nation-State Actor: The United States of America



In the introduction chapter of the National Cyber Strategy of the United States of America it is stated that they are in an ongoing cyber competition against cyber criminals, terrorists, and strategic adversaries such as Russia, China, Iran and North Korea who use cyber operations to challenge the United States of America and their allies. [28]

Some of the notable activities are the intelligence sharing alliances known as the Five Eyes and the Fourteen Eyes. The five eyes are an intelligence sharing group with roots in the second world war and operating under the UKUSA Agreement. The participants are USA, Canada, New Zealand, United Kingdom and Australia. The Nine Eyes and Fourteen eyes are an expansion to the initial five participants. The Fourteen Eyes are known also as SIGINT Seniors Europe has nine additional participants in addition to the Five Eyes: Denmark, France, Netherlands, Norway, Germany, Belgium, Italy, Sweden, and Spain.[29]

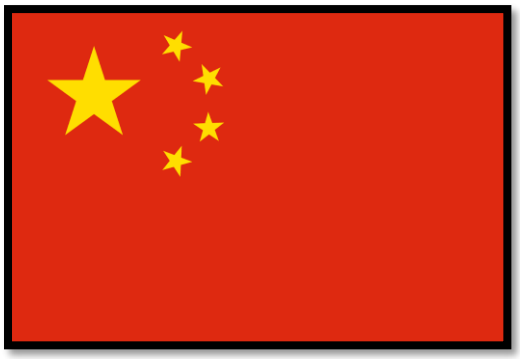
In addition to intelligence gathering the United States has launched destructive cyber operations themselves and with their allies. One of the most notable operations was a joint operation with Israeli intelligence agency Mossad to disrupt the Iranian nuclear programme using a highly sophisticated malware called Stuxnet. [30]

USA received some backlash for their global surveillance network operated by their National Security Agency. Edward Snowden disclosed intricate details about the global surveillance network in 2013 revealing certain technologies and information sharing groups that exist for mass surveillance.

One of the most famous US state sponsored groups is the Equation Group. According to Kaspersky labs the Equation group has targeted government institutions, mass media, a wide range of technology innovation companies and critical infrastructure organizations. According to Kaspersky they have been known to operate in Iran, Russia, Pakistan, Afghanistan, India, Syria, Mali, Lebanon, Yemen, United Arab Emirates, Algeria, Kenya, United Kingdom, Libya, Mexico, Qatar and Egypt.United States has a vast intel-

ligence network and has a highly advanced espionage, infiltration and disruption capability. Organizations operating with the countries mentioned in the strategy (Russia, China, Iran, North Korea) and other entities deemed American competitors in the cyber can become targeted with American cyber operations, especially if the organization can be seen as supporting the competing countries critical infrastructure or the collaboration can be seen as a challenge to American domestic or global interests. These operations can be intelligence gathering, espionage or disruptive operations, depending on the target organization. [31]

Nation-State Actor: China



According to the NATO CCDCOE report regarding Chinese Cyber Strategy in China cyber is seen as integral part of society and just one part of the society to be governed just like any other. When the free internet became available as a free and open communication platform there was never a question whether this new dimension should be controlled or not but more how it should be controlled. China is still reliant on western technology and sees this reliance as a threat.[32]

According to Statista there are currently approximately 4,7 billion active internet users in the world and of those 4,7 billion China accounts for almost 20% (903 million). For comparison, India has 560 million active internet users and USA has 284 million internet users. For the Chinese government they see the internet as a tool to control the citizens and to further the governmental agenda and to protect the internal stability of China. They also see foreign influence and dependency, especially western as a threat and aim to decrease the exposure of their nation to these elements as a part of their "Cyber sovereignty". [33-36]

There is significant evidence that China has launched multiple cyber operations against Western countries and against their neighbouring regions. They are known for targeting academia, industry and governmental organizations to gather classified information, especially technical research and development data that can be used to improve the Chinese economic competitiveness, and their political and military position.[37]

Chinese hackers are known as 'hongke' (red guest) by analogy that the Chinese word for hacker is 'heike' (black guest). Some of the most famous Chinese cyber operations are:

- In 2016 the Chinese revealed their new J-20 fighter which is strikingly similar to the US F-35, which was the most expensive US military investment to date and the specifications were highly classified at the time. It is believed that the Chinese hackers managed to obtain technological secrets regarding the new US stealth fighter. [38]
- In 2017 the Chinese Advanced Persistent Threat group 10, also known as the MenuPass team was discovered having infiltrated many of the major

ICT service providers to steal trade secrets from their clients in an operation called “Cloud Hopper”. [39,40]

- In 2015 the Chinese managed to compromise 21,6 million identities from amongst other things, US Security Clearance applications (known as SF-86’s).[41]

Organizations highly invested in technological research and development are a priority target for Chinese espionage operations. Also, organizations that can be seen as supporting the Western nations that China sees as a threat (such as USA) or operating in the Chinese border regions can become targeted by Chinese cyber operations.

If the organization is operating in China, it’s noteworthy that the connections within China and over the border can be expected to be monitored.

Nation-State Actor: The Russian Federation

According to the NATO CCDCOE report on Russian operations in cyberspace, Russia views information security quite differently than the west. The Russians have a concept called 'Informatsionnoe Prostranstvo', meaning 'influencing individual and public consciousness, information infrastructure and information itself'.[42]

Russians see cyberoperations as part of Informatsionnoe Protivoborstvo (IPb). The term does not mean specifically information warfare, but more 'counteraction' or 'confrontation'. The Russians view Informatsionnoe Protivoborstvo as capabilities for controlling the technical aspect of cyber as well as the information aspect. Meaning that the term has built in the technical cybercapabilities and information operations and electronic warfare. [42]

The UN Charter and the Geneva convention makes a clear distinction between peace and war, whereas Russians see the Protivoborstvo being constantly ongoing, sometimes escalating sometimes de-escalating from region to region. This view makes it possible to exploit the UN Charter and the Geneva conventions distinction of peace and war and pursue their strategic objectives under the threshold of the determination of 'war'. As western ideology is to provide free and unrestricted internet, Russians can expoit this openness to achive 'information superiority'. [42]

Russia has a lot of natural resources but little natural borders and thus Russians have been forced to mobilize themselves to defend against invaders. This has contributed to a profound sense of insecurity and the Russians feel that the security of Russia can be best guaranteed by making their adversaries feel insecure. This means that Russia is especially reactive in regions they identify as being within their "Sphere Of Influence". [42]

Russia feels that NATO is an aggression against their Sphere Of Influence and as an attempt to surround Russia. Thus the actions they perform utilizing their 'information weapons', a concept absent from western terminology, are acts of self defence.

The basic concepts can be split into three core concepts Active Measures, Reflexive Control and Maskirovka Active Measures effect nations policies by utilizing blackmail, bribes, disinformation, and the exploitation of a target nation's individuals and political influence. Reflexive Control guides the target to act in a predefined manner that favours Russian objectives and is detrimental to their own interests. Democratic information spaces are especially vulnerable for this type of influence. Maskirovka (deception) aims to lead the target into error, force them to take measures not corresponding to reality, and to disrupt their command and control and undermine their morale. [42]

Russia aims for high level of data sovereignty by establishing their own closed internet "RuNet", a Russian language-based, relatively closed segment of the Internet consisting of popular research engines and social media sites such as Yandex, Vkontakte and Odnoklassniki which also helps Kremlin to actively suppresses undesired information.

Western intelligence communities have linked the FSB with Turla APT and GRU Unit 26165 is suspected to be behind the activities of linked APT28 (also known as Fancy Bear). It hasbeen one of the most active APT groups. CyberBerkut is another GRU-linked hacktivist-style groups, which has been active since the beginning of Russo-Ukrainian war. [42]

Russia appears to hack for political reasons; to help or harm political candidates, to prop up Russian interests, or to more generally sow doubt around the world in democratic governance. These objectives were seen in the 2016 DNC hack, and the use of bots to spread fake news. In 2015 a cyber-attack linked to Russia shut down electricity for about a quarter-million Ukrainians and in 2017 they launched a massive cyberattack utilizing wiper malware NotPetya.

Organization operating inside Russian sphere of influence and in "unfriendly nations" can be targeted by Russian cyberoperations. Also current economic sanctions have caused the Russians to seek technological innovations from the west utilizing the means of Informatsionnoe Protivoborstvo. [42]

4.5.3 Other Motivations

Insider threats

Unintentional Insiders are people who become a threat through unintentional actions, such as clicking a phishing link, forgetting to lock their computer, or falling for social manipulation.

The most common attack vector against unintentional insiders are different social engineering based attacks, such as spear-phishing or smshing (text-message based phishing). After the initial foothold according to ENISA the most common assets targeted are databases, networks, file shares and endpoints.

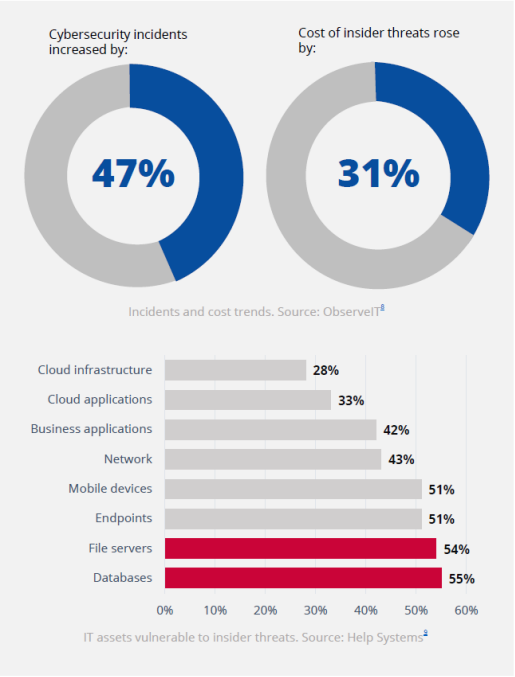


Figure 18. IT assets vulnerable to insiders

Intentional Insiders can be split into two categories: Independent Actors and Recruited Actors. Independent Actors are people who become a threat through their individual agenda, this can be ideology (political, religion etc.), disgruntlement (layoffs, disagreement at workplace), challenges in personal life (substance abuse, financial trouble, psychological issues) and are usually linked in their duties. [43]

Recruited Insiders are people who become a threat through external influence. Usually, these types of insiders are groomed into the task with a long timespan, or they can become insiders through a recruitment campaigns.

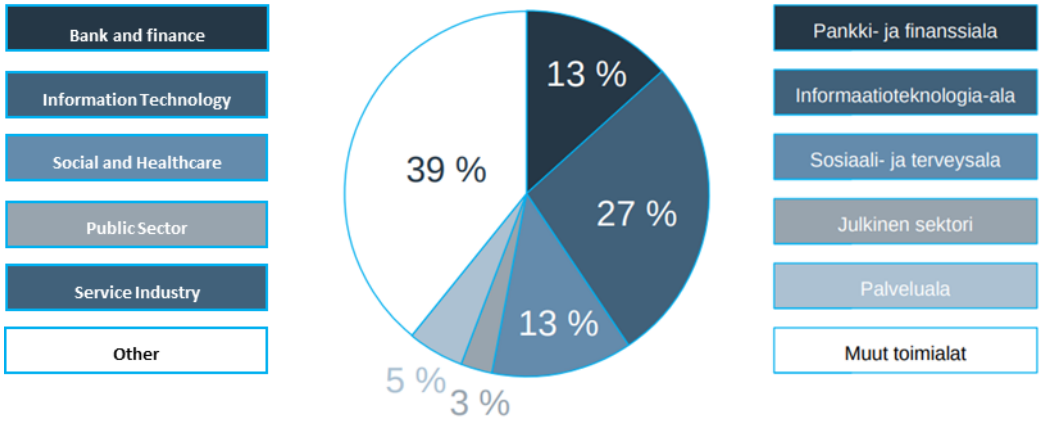


Figure 19. The prevalence of Intentional Insiders in different sectors [44]

CyberTerrorism

Terrorism and especially cyber-terrorism is an ambiguous topic, since there are multiple definitions what constitutes as 'terrorism' and whether Cyber-Terrorism is a separate entity or if it's just the cyber-element of terrorism. Regardless, terrorism in cyber-space aims to progress the 'parent' terrorist organizations objectives by spreading propaganda to gain visibility and new recruits, raising and funneling money for the organization and by performing cyber-operations that instill fear in the general populace. [45]

By nature cyberterrorists usually operate in the financial crime segment and aim to launder money and channel funds to assist in the terrorist organization goals so this part of terrorism usually is most visible in financial sector, namely banking.

Other visible aspect is social media presence, which is used to spread the terrorist organizatoins ideology and recruit new members for the group. The 'cyber' branch of terrorist organizations usually also create online communication channels accross different terrorist cells, thus playing a supporting role. These types of operations are relevant to social media platform companies, forum hosts and governmental organisations that are tasked with fighting terrorism. [46]

Cyberattacks that would achieve the 'terror amongst population' requirement of terrorism definition, would require scalability of operations and these organizations usually don't have such capabilities, and if operations can't be scaled, they are not considered especially terrifying to the general population and thus the impact remains limited.[47]

Hacktivists

Hacktivists often use attacks like Website Defacement, DDoS and Doxxing (Publishing PII on the internet) to gain publicity for their ideology. These are often amplified by utilizing social media.[7]

Hacktivism is a concept originating from traditional activist organizations and some hacktivist organizations have connections or support traditional activism organizations. Commonly activists defend an ideology utilizing smear campaigns (spray-painting, banners etc.), information spreading through protests, disrupting businesses (disabling industrial equipment) and by performing general civil disobedience.
Hacktivism aims to defend the specific ideology by utilizing similar concepts, but applied in cyberspace: The most common tool in the hacktivist arsenal is DDoS (Distributed Denial-of-Service), website defacement, propaganda spreading through social media, Doxxing (publishing private information of individuals) and leaking electric correspondence (for example by compromising an email server). [7]

Some industries are more likely to become targeted by hacktivists if they operate in a sector that has strong emotional attachments associated with it, such as animal rights, natural resources, nation-state or political connections, and controversial individuals.

Hacktivist groups are usually loosely organized groups that can have a formal leader or the group can rally behind a specific idea without a specific leader, anyone from the group can bring about the call to action and if the proposition gains enough momentum the group starts a campaign against the perceived enemy.

5 Strategic Threat Modelling

Information security is a means to manage the risks associated with the Organizational Mission and thus threat actor mapping ties directly into organizational risk management. To identify the most realistic threats and to holistically manage information security risks, organizations need to establish what their actual realistic risk profile is.

When a threat actor profile has been established the senior management can decide on an informed risk appetite. Then security controls are designed to mitigate the identified threats and resources are not spent ‘over-protecting’ the Organization or inadvertently increase the Organizational risk by ‘under-protecting’ the business.

Threat actor mapping reduces the discrepancy between organizational units that might have differentiating views on what their Threat Actor Landscape is. For example, the website application development team might see an individual hacker or hacktivists as the most relevant threat actors whereas the website infrastructure management team sees organized criminal groups as the primary threat. This can lead to a situation where the different layers of the technology stack are protected using different security baselines and this can create inconsistent security posture. Another example could be that the employees responsible for the security of the user endpoints are concerned that professional criminal groups can easily penetrate the organizations outer perimeter by breaching the end user devices and the ICT infrastructure team sees the internal network as ‘safe and trusted’ environment. This can also be described as the obsolete ‘impenetrable fortress” or ‘hard exterior, soft interior’ defensive model.

When there is a common understanding of the threat actors targeting the organization, a more accurate consistent understanding of the attackers capabilities can be created and the different teams within the organization can establish security baselines that are aligned with each other and thus provide more consistent, comprehensive and cost-efficient security baseline.

The foundation of Strategic Threat Modelling is to understand the motivations behind the most relevant threat actors, evaluate how these motivations align with the organization, determine the organizations current defensive capabilities and finally form a synthesis of how the Threat Actor could be performing such cyber-attacks against the organization

that could threaten the mission of the organization. The threat modelling follows these steps:

5.1 Establishing the Organizational Presence

- Analysis of the geographical footprint of the organization.
- Analysis of the business operational sector.
- Analysis of the clientele and subcontractor network as well as partners to identify shared or inherited threat actors and establish the position on supply chain networks.
- Analysis of the organizational reputation. This step consists of evaluating whether the organization has been target of recent controversy, if the organization has politically or publicly considerable personas or if the organization operates in a sector that is emotionally reactive.

This part of the assessment relies mostly on information provided by the Client as they have the best knowledge of their geographical footprint, clientele, and subcontractor network. The evaluation is then complemented by the security specialist insight regarding the sector and subcontractor knowledge.

5.2 Establishing the Threat Actor Landscape

- Evaluation of the national internal security landscape and the international geopolitical landscape.
- Evaluation of the most common threat actors targeting the specific operational sector.
- Evaluation of the clients, partners and subcontractors using the steps in Establish the Organizational Presence and Establish the Threat Landscape steps
- Determining the threat actors that might react based on the organizational reputation

This part of the assessment complements the information from the Client with the information from the security specialist's knowledge of the threat landscape to the context of the organization involved. This usually relies extensively on the security specialist's knowledge of the Threat Actors related to the geographical footprint, operational sector, subcontractor network and controversial topics affecting the organization.

In this phase a lot of research is to be expected to identify current trends, most prevalent actors and the techniques used. There are a lot of organizations that provide different

types of threat landscape evaluations, such as Interpol, Europol, ENISA, The European Union Agency for Cybersecurity, National Computer Emergency Response Teams (CERT), National Intelligence Agencies and private companies such as Information Security Forum and security companies.

5.3 Establishing the Threat Actor Capabilities

Assess the Likelihood of Attack Initiation by determining:

- The alignment of Threat Actor(s) motivation and the organization
- The capability tier of the Threat Actor(s)
- The existence of historical precedence between the organization and the Threat Actor(s)
- The level of commitment the Threat Actor(s) have
- The attack vectors the Threat Actors have the capability to utilise

The capability assessment is the most complex synthesis to form as the capability metrics need to be established first and then the threat actor capabilities need to be evaluated. The evaluation requires research to evaluate the capabilities of the Threat Actors. The capability can be assessed by evaluating previous incidents and published statements regarding the identified Threat Actors. Some frameworks for Threat Actor capability assessments are available from the SANS Institute, The MITRE Corporation and Information Security Forum.

5.4 Form Synthesis

Organizational Presence and Threat Actor Landscape are cross referenced to identify where these two overlap. Then the resulting actors are prioritized by ranking the Threat Actors by their established Capabilities, prioritizing the Threat Actors with the Highest Capabilities. This will result in a list with Threat Actors from highest Likelihood of Attack Initiation to the lowest.

5.5 Conduct a Risk Assessment

To get the full benefit from the Strategic Threat Modelling the potential impact of the Threat Actors need to be established. There are multiple ways how to implement the findings into the organizational risk management framework. In this Thesis the connection between the different components are demonstrated utilizing the ideology from Information Security Forums Information Risk Assessment (IRAM) tool.

The classic formula for calculating risk is

P * I = R, where

P = Probability, I = Impact, R = Risk

As the cyberspace is permanently contested environment the probability is determined by cross-referencing the Likelihood of Attack Initiation and evaluation of the Organizational Security Posture. This will result in a list of Threat Actors with an associated Likelihood of Success, which is the probability of the attack.

This refined formula for Cybersecurity Risk is based on Information Security Forums Information Risk Assessment Model revision 2.[48]

P = Threat Actor Capability * Organizational Vulnerability Multiplier * Control Strength Multiplier

Where

Threat Actor Strength is structured into the following components

- Capability: What is the level of attacker capability
- Commitment: How committed the attacker is
- Motivation: How aligned are the attackers motives with the organization
- History: Is there a precedence of the Threat Actor targeting the specific organization

Organizational Vulnerability Multiplier

- Vulnerability: What are the organizations vulnerabilities

Control Strength Multiplier

- Mitigating controls: The controls the organization uses to mitigate vulnerabilities
- Control implementation: How widely and maturely the controls are implemented

The impact component is evaluated utilizing a Business Impact Reference Table to determine the Risk Level. Risk level is then compared to the Organizational Risk Appetite.

Should the Risk Level exceed the Organizational Risk Appetite, Mitigation Strategies are prepared.

5.6 Prepare a Mitigation Strategy

Mitigation Strategies are prepared to address the risks that exceed the Organizational Risk Appetite. To determine effectiveness of security controls mitigating the risks, a model for mapping different control effectiveness to specific attack vectors is a good practice.

6 Results and Analysis

The deliverable was two powerpoint presentations, first of which was the Strategic Threat Assessment and the second one was the Mitigation Strategy. In addition a third more condensed version was prepared. The Strategic Threat Model and the mitigation strategy is classified and is not attached to this thesis. The index slide from the threat Modelling is presented here.

The base material used in the Strategic Threat Modelling were the Contractual Requirements of the project, National Threat Assessment from the Finnish Ministry of Interior, The Security Reports from the Finnish Security and Intelligence Service, Crime Studies by Finnish universities, Reports from ENISA, the Finnish Security and Intelligence Service and Europol.

This particular assessment utilized a total of 19 bibliographical references, over a dozen discussions with different governmental information security intelligence entities, CGI global threat intelligence and research on client sector of operations. As a result, two major threat actor landscape clusters were identified: One related to the sector of the operations and another related to prevalent trends of cybercrime. A total of 19 threat scenarios exceeding organizational risk appetite were identified by analysing 39 threat actors with differing capabilities and 58 unique attack vectors with different prerequisites for successful completion of the attack.

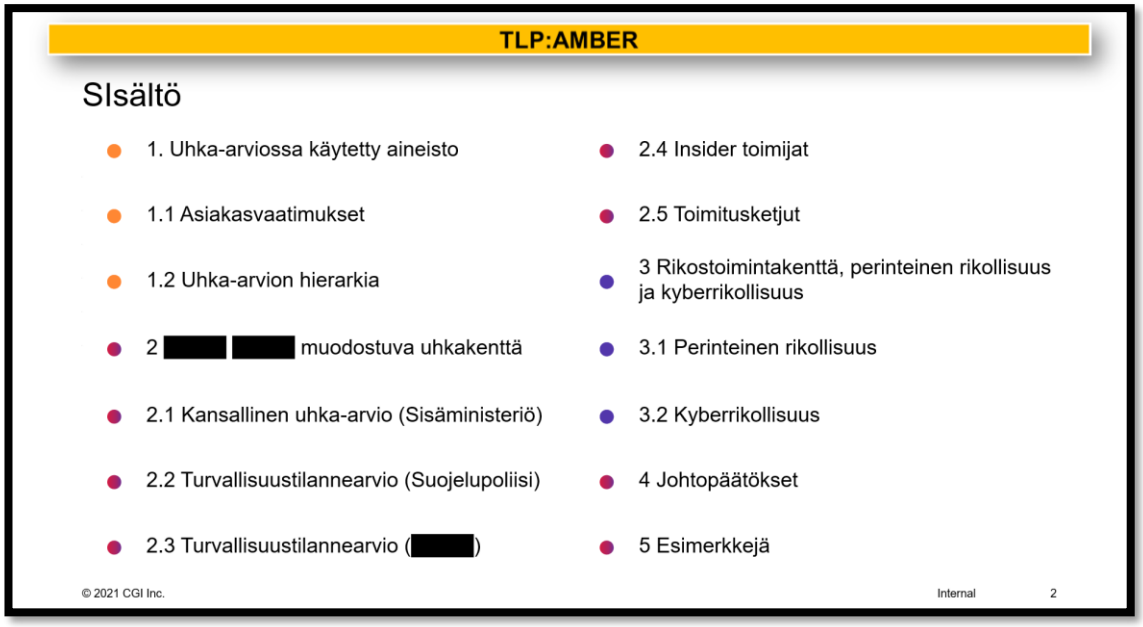


Figure 20. Index of the Strategic Threat Assessment (69 slides)

Translation of the picture:

1. Material used in the threat assessment
1.1 Client Requirements
1.2 Threat Assessment hierarchy
2. [redacted] threat landscape
2.1 National risk assessment
2.2 Security situation assessment
2.3 Security situation assessment ([redacted])
2.4 Insider actors
2.5 Supply-chains
3 Criminal field-of-operations, traditional crime, and cybercrime
3.1 Traditional crime
3.2 Cybercrime
4 Conclusions
5 Examples

6.1 Discussions and Conclusions

The Strategic Threat Assessment created a solid foundation for the project and the mitigation strategy implemented in the beginning of the project remained current until the

end of the project. The Strategic Threat Assessment was used as foundation for individual risk assessments with all the teams working with the project and the end result was that the security compliance was achieved approximately 50% faster than in a similar reference project.

The Strategic Threat Assessment methodology and results were reviewed and challenged multiple times along the formation of the methodology and the end result was approved an finally audited and passed the strict audit criteria without any observed defects. Based on these facts I would consider this model functional and actionable and that the required results were achieved.

This way of Strategic Threat Modelling is resource intensive, especially if the Strategic Threat Modelling is complemented with the related Risk Assessment. However the Client found it very useful in communicating the Security Requirements to the different teams in the project.

References

1 https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/
Accessed 9.12.2023

2 https://ung.edu/continuing-education/news-and-media/cybersecurity.php
Accessed 9.12.2023

3 https://www.cgi.com/en/article/overview/cgi-history
Accessed 9.12.2023

4 https://www.chappell-university.com/post/spies-espionage-ransomware-and-harold-part-1-of-2
Accessed 9.12.2023

5 https://www.okta.com/identity-101/wannacry/
Accessed 9.12.2023

6 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
Accessed 9.12.2023

7 Samuel Chng, Han Yu Lu, Ayush Kumar, David Yau, Hacker types, motivations and strategies: A comprehensive framework, Computers in Human Behavior Reports 5 (2022) 100167, 2022

8 Internet Organised Crime Threat Assessment (IOCTA) 2023, European Union Agency for Law Enforcement Cooperation, 2023

9 A “Kill Chain” Analysis of the 2013 Target Data Breach, COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, United States Senate, MARCH 26, 2014

10 Matti Kortesoja, Tapaus Vastaamo, Symptomaattinen luenta potilastietosuojan murtumisen yhteiskunnallisista syistä ja seurauksista, Tutkimus & Kritiikki 2(1)|2022, 2022

11 https://online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/
Accessed 9.12.2023

12 https://www.govtech.com/security/Cybercriminals-Becoming-Increasingly-Professional.html
Accessed 9.12.2023

13 Lillian Ablon, Martin C. Libicki, Andrea A. Golay, Markets for Cybercrime Tools and Stolen Information: Hackers’ Bazaar, RAND Corporation, 2014

14 From Underground City to Thriving Metropolis An Economic Analysis of the Cyber Black Markets, Juniper, 2014

15 https://zerodium.com/program.html
Accessed 9.12.2023

16 https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data
Accessed 9.12.2023

17 Mayra Rosario Fuentes, Shifts in Underground Markets – Past, Present, and Future, Trend Micro Research, 2020

18 Max Goncharov, Russian Underground 101, TrendMicro 2012

19 THE BLACK MARKET REPORT, ARMOR.COM, 2018

20 Max Goncharov, Russian Underground 2.0, TrendMicro, 2015

21 https://www.cobalt.io/blog/cybersecurity-statistics-2024
Accessed 9.12.2023

22 Lin William Cong, Campbell R. Harvey, Daniel Rabetti, Zong-Yu Wu, An Anatomy of Crypto-Enabled Cybercrimes, Lancaster University, November 2022

23 Julia Voo, Irfan Hemani, Daniel Cassidy, National Cyber Power Index 2022, HARVARD Kennedy School BELFER CENTER for Science and International Affairs, 09/2022

24 INTERNATIONAL SECURITY AND ESTONIA 2018, Estonian Foreign Intelligence Service, 2018

25 Office of the Under Secretary of Defence (Comptroller)/Chief Financial Officer, Project Acquisition Cost By Weapons System, United States Department of Defence Fiscal year 2017 Budget request, 02/2016

26 Andrew Smith, CYBER THREAT ACTORS: HACKONOMICS, University of Cambridge, Centre for Risk Studies, 2017

27 Andrew Smith, THREAT ACTORS IN THE CYBER BLACK ECONOMY, University of Cambridge, Centre for Risk Studies, 2018

28 Joe Biden, NATIONAL CYBERSECURITY STRATEGY, The White House, MARCH 2023

29 https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc

30 https://www.theguardian.com/world/2021/apr/11/israel-appears-confirm-cyberattack-iran-nuclear-facility
Accessed 9.12.2023

31 https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
Accessed 9.12.2023

32 Mikk Raud, China and Cyber: Attitudes, Strategies, Organization, NATO CCD-COE, 2016

33 https://www.statista.com/statistics/617136/digital-population-worldwide/
Accessed 9.12.2023

34 https://www.statista.com/statistics/325645/usa-number-of-internet-users/
Accessed 9.12.2023

35 https://www.statista.com/statistics/265140/number-of-internet-users-in-china/
Accessed 9.12.2023

36 https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/
Accessed 9.12.2023

37 Journal of Political Sciences & Public Affairs : New Cyber Strategy of China and the Alterations in the Field, 2017

38 https://www.dailymail.co.uk/sciencetech/article-3888942/Chinese-stealth-fighter-shed-cloak-secrecy.html
Accessed 9.12.2023

39 https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-cloud-hopper-what-you-need-to-know
Accessed 9.12.2023

40 Operation Cloud Hopper – Exposing a systematic hacking operation with an un-precedented web of global victims, PWC, April 2021

41 SEMIANNUAL REPORT TO CONGRESS OCTOBER 1 2014 – MARCH 31 2015, United Stated Office of Personnel Management, 2015

42 Janne Hakala, Jazlyn Melnychuk, RUSSIA'S STRATEGY IN CYBERSPACE, NATO STRATCOM COE, NATO CCDCOE, 2021

43 Insider threat - ENISA Threat Landscape, The European Union Agency for Cy-bersecurity, 2020

44 Ville Jääskeläinen, LIIKESALAISUUKSIIN KOHDISTUVIEN INSIDER-RISKIEN HALLINTA, Suojelupoliisin julkaisusarja 1/2018, 2018

45 Z Yunos and S Sulaman, Understanding Cyber Terrorism from Motivational Perspectives, Journal of Information Warfare vol. 16 No. 4, 2017

46 https://www.un.org/counterterrorism/cybersecurity
Accessed 9.12.2023

47 Gabriel Weimann, UNITED STATES INSTITUTE OF PEACE, Cyberterrorism How Real Is the Threat?, 2004

48 Eeva-Riina Pelkonen, Creating a guidebook for IRAM2 information risk assess-ment methodology, Laurea, 2023

49 https://www.getastra.com/blog/security-audit/cyber-crime-statistics/
Accessed 9.12.2023

50 https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
Accessed 9.12.2023