The Ukraine cyber war: an analysis of the Russian cyber doctrine for comparing the Ukraine National Cyber Security Strategy with those of other western countries

July 2023

University of Glasgow ID: 2685539b

Dublin City University ID: 21109621

Charles University ID: 85545841

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence and Strategic Studies

Word Count: 21986
Supervisor: Dr David Erkomaishvili
External Supervisor: Matthieu Paques
Date of Submission: 24/7/2023

Abstract

Since the start of the Ukraine war Ukraine has experienced a threefold increase of cyber-attacks from Russia. Ukraine, the United States, Germany, and France have already experienced continuous cyber-attacks from Russia since 2014. Although the National Cyber Security Strategies (NCSSs) from the latter three have already been compared amongst each other and others in academic literature, the NCSS of Ukraine has not. No NCSS has also been analysed for resiliency against the Russian cyber doctrine. The main research question answered was: what can states and organisations learn from the NCSS of Ukraine, compared to the United States, Germany and France assessed on their resiliency against the Russian cyber-attack doctrine since 2014? The question was answered with the help of three research questions. The first aimed to analyse the Russian cyber doctrine before and after the start of the war and develop a framework with the most common targets and Tactics, Techniques and Procedures (TTPs) with which NCSSs can be compared against each other on scores based on their resilience. The most common targets have been those of critical infrastructure sectors and TTPs being DDoS, phishing, and ransomware. The second research question aimed to see which NCSS was most resilient, which was the one of Ukraine. This was due to its recent strategic initiatives it implemented to defend itself. The third research question aimed to give recommendations based on the comparison. The answer to the main research question is based on the recommendations that states and organizations can learn from regarding their cyber security strategy which is to give attention to the most common used TTPs and implement a holistic approach to cyber security to defend against them.

Key words: National Cyber Security Strategy, Ukraine cyber war, cyber security, Russian cyber doctrine

Contents

Overview of abbreviations

APT:	Advanced Persistent Threat
CISA:	Cybersecurity and Infrastructure Security Agency
DDoS:	Distributed Denial of Service
DNS:	Domain Name System
DoD:	Department of Defence
ICS:	Industrial Control Systems
JCSA:	Joint Cyber Security Advisory
MISP:	Malware Information Sharing Platform
NCSS:	National Cyber Security Strategy
OT:	Operational Technology
SCADA:	Supervisory Control and Data Acquisition
SMEs:	Small and Medium-sized Enterprises
SSLT:	State, Local, Territorial, and Tribal
SSSCIP:	the State Service for Special Communications and Information Protection
TTPs:	Tactics, Techniques, and Procedures
U.S.:	United States

1. Introduction

Ukraine has since the start of the war in 2022 seen an increase of cyber-attacks by threefold. Although the country has been victim of such cyber-attacks since 2014, other western countries have experienced an increase of attacks from (pro-)Russian hacker groups. The United States (U.S.) for example, has still been experiencing successful cyber-attacks on critical national infrastructure. An example of such cyber-attack happened early in the morning of the 10th of October 2022 when numerous airports such as Los Angeles International, Chicago O'Hare, and Atlanta International airport, had their websites unexpectedly taken down. This made it impossible for travellers to check their flight schedules (Toulas, 2022b). That morning, the information technology team of the Los Angeles International airport scrambled together to alleviate the disruption and investigate the problem. The authorities were notified and by 1PM, notified the public in turn that the website was “up and running” again (Romo, 2022). What was later revealed from the investigation is that this “incident” was in fact a Distributed Denial of Service (DDoS) attack (an attack where multiple computers bombard one website with requests until it is overloaded and inaccessible) launched by the pro-Russian hacker group called KillNet (Romo, 2022). This hacker group is well known for launching such attacks against government and private websites relating to critical national infrastructure. Moreover, the group is also known for having a Pro-Russian sentiment towards the war in Ukraine and has targeted the critical national infrastructure of countries before who side with Ukraine such as Italy and Romania.

On the Monday morning of the attack the group send out a Telegram message with a list of U.S. airport websites and encouraging hackers to participate in the attack. Although it has targeted only European countries early in the war it has now shifted its scope to the U.S as it is the main provider for Ukraine when it comes to intelligence and artillery (Toulas, 2022b). Only a few days

before KillNet had already attacked numerous state websites which took days to recover from (*Several state websites disrupted by Killnet DDoS attacks*, 2022). These attacks show that protection against such Russian cyber-attacks have not been strategically and uniformly put in place for critical national infrastructure systems of the U.S., something that a former general counsel of the National Security Agency, Glenn S. Gerstell, had already predicted since the beginning of the war in an interview with the Guardian. He also said that the U.S. has "an extraordinary offensive capability" (Paul, 2022) when it comes to the cyber space but due to growing number of advanced cyber-attacks the U.S. has not yet mastered the speed to keep up to defend itself. It approaches have mostly been reactive and decentralized. He added, that if a cyber-attack would ever cause damage to human beings, it could potentially be seen as an act of war as it would be treated in the same way as say, a bomb attack (Paul, 2022).

1.1. The case of Ukraine vs. other western countries

Although, research for this dissertation has only started shortly after the one-year anniversary since its inception (the 24th of February 2022), with the number of cyber-attacks and organizations working to protect Ukraine, much information about how Russia deals out cyber-attacks has been made public. Before the war, the threat posed by Russia on the digital front of Ukraine and other western countries has been persistent since at least 2014. According to a briefing of the European parliament about the timeline of cyber-attacks on Ukraine, the first major cyber-attack against Ukraine was on the 13th of March 2014 with a DDoS-attack that took eight minutes in response to a referendum on the status of Crimea (Przetacznik, 2022). It can be argued that the first real cyber threat Russia posed against the west was in 2007 against Estonia when the country experienced many DDoS attacks on websites of, including but not limited to, the government, political parties, news organizations and banks (*2007 cyber attacks on Estonia*, no date). However, an increase of Russian

cyber-attacks has started since 2014 for western countries such as Estonia, Romania, Georgia, the U.S., France, Germany, and Poland.

These countries all have had their chance to learn from each other and adapt their National Cyber Security Strategies (NCSSs) to it. According to the European Union Agency for Cybersecurity (ENISA), a NCSS is "the main documents of nation states to set strategic principles, guidelines, and objectives and in some cases specific measures in order to mitigate risk associated with cybersecurity" (*National Cybersecurity Strategies Guidelines & tools*, no date) These strategies are generally updated once every four years. These NCSSs have been compared with each other in the academic literature but the selection of countries in this comparison have often been random and have not yet included the country of Ukraine. At the time of writing the NCSS of Ukraine has not been compared with any other NCSS in academic literature. Meanwhile western countries such as the U.S., France, Germany, Estonia, Australia, Canada, the United Kingdom, and the Netherlands have been compared amongst each other (among others) on their NCSS. These comparisons have been based on general aspects such as perceived threats and identified strategies and stakeholders. There thus appears a gap in academic research where the NCSS of Ukraine has not yet been compared with other (western) countries and that this comparison is not based on the Russian cyber doctrine.

Ukraine has experienced three times more cyber-attacks in the last year than before the war according to an official at the State Special Communications Service of Ukraine (SSSCIP) (Sabbagh, 2023). This war has also shown to be the first time "that cyber operations have played such a prominent role in a world conflict" according to a report made by Google ('Fog of war: how the Ukraine conflict transformed the cyber threat landscape', 2023). Many of the cyber-attacks it had to endure were targeted its organizations, governments

and national infrastructure which made it necessary for Ukraine to learn and adopt its NCSS in rapid fashion. This has made Ukraine and its allies who helped protect their most valuable IT-systems a very important case from which many western countries can learn from. One of such strategic decisions made by Ukraine to defend against Russian cyber-attacks is the creation of the 'IT Army'. This army was created by Ukraine by calling out on underground hackers in its country and abroad to defend against the Russian cyber threat (Schectman and Bing, 2022). Moreover, perhaps such strategy could also be beneficial in other countries facing cyber threats from nation states.

1.2. Main research question and research questions

It would therefore be helpful and important for governments and organizations to compare the NCSS and cyber operations of Ukraine with the U.S., France, and Germany as they have experienced a similar increase of Russian cyber-attacks since 2014 and would therefore have different approaches to (or maybe lack thereof) protect their IT-systems against these attacks. By comparing them, recommendations can be made for these countries and other governments and organizations on where their strategy may be improved. Thus, the main research question this research aims to answer is: *what can states and organisations learn from the NCSS of Ukraine, compared to the United States, Germany and France assessed on their resiliency against the Russian cyber-attack doctrine since 2014?*

To answer the main research question this research needs to answer three sub research questions:

1. The first research question is: what are the most common targets and TTPs used of the Russian cyber doctrine since 2014? The purpose of this research question is to make a framework with which the NCSSs of the U.S., France and Germany are compared with. The points of comparison which this framework consists of are the targets and TTPs of the Russian

cyber-attack doctrine. The NCSSs of the U.S., France and Germany have been chosen as these countries have all been targeted by Russian cyber-attacks since 2014 thus having the equal time to adapt their NCSS making the comparison fair.

2. The second research question is: which NCSS of Ukraine, U.S., Germany, and France scores the highest on the Russian cyber doctrine framework? A score will be given based on mentioning and formulating strategies around the targets and TTPs to compare there more easily. Recent strategic initiatives taken by Ukraine will also be considered in this comparison.

3. The third research question is: what recommendations can be given to governments and organizations based on the resiliency of their NCSS compared to other NCSSs? These recommendations are strategic in nature but also provide practical means in how to bolster resilience against Russian cyber-attacks. The key findings and recommendations found in this dissertation are that states should mention common TTPs of Russia but also implement a holistic approach to cyber security.

To gather more recent information regarding the cyber war, interviews will be held with experts and practitioners regarding their insight of the Ukraine cyber strategy.

1.3. Structure of the dissertation

First, a literature review of the current academic literature surrounding the topic of this dissertation and where it feels in the gap is given followed by a substantiation of the research methodology. This is followed by a substantiation of the case study selection. The next section covers limitations of this dissertation to specifically highlight what is not part of the research. After these sections each research question is answered where section 6 will

cover the first, 7 the second and 8 the third sub research question with the final answer to the main research question covered in the conclusion.

2. Literature review

In this section an overview is given of the current knowledge in academic literature surrounding the topic of this dissertation. Firstly, an overview is given of the Russian cyber doctrine followed by the comparison of the NCSSs of the selected countries and closing with the analysis of the Ukraine NCSS. This dissertation will fill in a big gap in academic literature surrounding the topic of comparing the NCSS of Ukraine with other western countries and analysing the most recent Russian cyber threat. Although Russian cyber-attacks against Ukraine and the west have started since 2014 there appears to be no study that has compared the NCSS of Ukraine to any country. As motivated in the introduction, this is significant as Ukraine has experienced a huge increase in cyber-attacks unlike any other country and could have therefore improved their NCSS in many ways which other western countries could learn from. The NCSS of Ukraine has also been in continuous improvement according to the NCSI (*Ukraine*, no date). In this section relevant academic literature regarding the topics of this research is discussed and gaps identified.

2.1. Russian cyber doctrine

Regarding analysis on the Russian cyber-attack doctrine, academic literature has provided many. The study of Jensen, Valeriano and Maness (2020) analysed the means and motivation behind the Russian cyber doctrine. To understand this however they first give an important overview on why nation states use cyber as a means to strategically influence other nations. A cyber strategy in general is often seen and used as a practice for covert action. “They reflect concealed means to achieve a political end.” (Jensen, Valeriano and Maness, 2020: 3). They are used not to escalate conflict but to manage it and

distract the adversary. To categorise the different means states can use to achieve strategic objectives, Jensen, Valeriano and Maness (2020) propose three strategic logics that states can use to gain strategic objectives in cyber space. These are disruption, espionage, and degradation. Using cyber-attacks as a form of disruption is also a very cost-effective way to execute the grand strategy of a country compared to other actions in other spaces such as land, sea, and air. Examples of such cyber-attacks can be DDoS-attacks and website defacements which are attacks most used for what Downs and Rocke (1987) called “tacit bargaining”. Tacit bargaining is when a state wants to influence policies of another state by behaviour and not with formal or informal diplomacy. A DDoS attack can therefore signal pressure for conflict escalation and website defacements with propaganda can lead to the public loosing trust in existing policies. Espionage is used for gaining information from the enemy to achieve a strategic advantage, it is also the most used means of cyber operations. Espionage can also entail corrupting information of the adversary, so it loses trust in its information systems. As for degradation, it looks similar to disruption and espionage however it is purposefully made to disrupt as specific system of the enemy. It is therefore more expensive as the development of such an attack is more complex (Jensen, Valeriano and Maness, 2020).

Regarding the Russia cyber doctrine, the study of Jensen, Valeriano and Maness (2020) also found that Russia it uses cyber-attacks do destabilize their targets and to make them adhere to the political ideals of Moscow. Russia does this by not only obtaining information via espionage but also using that information for propaganda purposes to change the opinion of the public. An example of such espionage activity was the 2013 operation called Armageddon which used spear phishing to target security services in Ukraine. In general Russia uses two tactics in its cyber operations. First, it prepares the target environment by infiltrating its networks, systems, and steal information

for future exploitation. A similar way the military does. This also leaves the target with questions on what other systems were compromised and information was stolen when the attack is discovered. Second, they use the attacks to cheaply change the opinion of the public. By releasing information about their successful cyber-attack, they show the public of that country its government is lousy and prone to Russian rule (Jensen, Valeriano and Maness, 2020).

Furthermore, when Jensen, Valeriano and Maness (2020) analysed the Russian cyber-attack doctrine with the conflict in Ukraine in 2014 as a case study, it also found that Russia seeks domination rather than manipulation. As it dominated most of the cyber space of Ukraine its cyber operations supported its propaganda machine and military efforts. Russia also showed another side to its cyber strategy by executing false flag operations. These are operations where an attacker performs an attacker under the flag of another country thus deceiving the target the attack was carried out by a different state. Such operations are also similar to those performed during the Soviet era. The researchers conclude that Russian cyber operations innovative and not yet seen in other superpowers but question if the strategy has exhibited "(…) any novel utility." (Jensen, Valeriano and Maness, 2020: 17).

Early analyses of the doctrine have been published since 2008 which was shortly after the first Russian backed cyber-attack on western countries such as Estonia and Georgia. The first of these studies comes from (Giles, 2011) which analysed the threat of Russian "Information Troops" which duties are that of, as he defined it, similar to cyber operations. Its goal is to improve the cyber capabilities of the Russian troops in case of a cyber war. A master thesis published in 2015 from a student at the Naval Postgraduate School California analysed the capabilities of the troops of Russia and found that although Russia likes to make it look it aims to defend its cyber space and sovereignty,

analyses from both public sources and interviews shows that there has been an increase in Russian cyber weapons, suggesting it rather seeks an offensive approach (Medvedev, 2015).

A similar finding was also found in a more recent study by Lilly and Cheravitch (2020). In their article explores the importance of cyber and information operations in the cyber doctrine enforced by Russia. Their analysis of the doctrine shows that it has shifted from practicing warfare with only violence to violence and non-military measures. These measures being information warfare. To have this insight is very important for the west as it explains the foreign policy and signals of Russia towards the rest and helps develop long-term strategic goal that addresses this. On the one hand, the view of Russia in cyber space resembles that of the same view it had during its Soviet era. It views Russia as "(…) a besieged fortress defending itself against constant internal and external threats, (…)" (Lilly and Cheravitch, 2020: 134). This has also been found in the study of Kari and Pynnöniemi (2023) who analysed the Russian threat perception with the theory of strategic culture. The strategy of Russia therefore suggests expressing a posture towards this cyber space that is defensive and cooperative. This can be seen in official documents where external threats are contained with legal frameworks and partners. On the other hand, Russian military scholars write about usefulness of cyber weapons in modern warfare. As they are not expensive and cause less physical harm than their physical counterparts, they are an effective tool to inflict damage on the adversary without causing outright war. Especially in cyber space it is always unclear when warfare commences and when it ceases. Moreover, Russian officials and scholars have argued that such weapons can also gain Russia information supremacy without the physical labour that is needed. More significant for Russia is that an offensive strategy in cyber sphere is a cheaper alternative to defending in a state that is already less economically and technologically well off than its adversaries.

In 2015 a technical report published by the Center for Naval Analyses explains how Russia develops and deploys this offensive cyber strategy and found that Russia employs cyber criminals, Advanced Persistent Threats (APTs) and hacktivists as part of their cyber operations (Connel and Vogler, 2016). APTs are, according to the U.S. National Institute of Standards and Technology, "An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives (…)." (*Guide for Conducting Risk Assessments*, 2012). These objectives are repeated and are typically to infiltrate an information infrastructure of an organization. The reasons for using APTs is that they provide anonymity and can be mobilized easily. It is also cheap to employ these groups compared to setting up and maintaining APTs for military use. There is little technical support needed as these groups only need a target. Compared to maintaining your own staff these groups work on a freelance basis so can be retired quickly as soon as the job is done. Some groups even offer their services for free if it aligns with their political view. More importantly, such groups always work in precaution to protect their anonymity, as their practices in their own country are illegal. This gives the Kremlin a bonus as first, the cyber-attacks they carry out are hard for investigators to attribute to an APT and secondly, these APTs act as proxies for the offensive strategy of the Kremlin (Connel and Vogler, 2016).

However, Russia does not only focus on technical cyber-attacks. According to a study by Akimenko and Giles (2020) the Russian cyber doctrine also includes the use of information as a soft power. This also known as information operations. Although this is not part of the scope of this dissertation, cyber-attacks are part of executing this part of the doctrine. Information as soft power incorporates means such as publishing fake news to

achieve disinformation campaigns, executing trolling campaigns and subversion to for example, achieve a change of regimes in their adversaries (Akimenko and Giles, 2020). In the previous discussed study of Connel and Vogler (2016) its findings show that Russia uses this soft power in three categories. The first is the use of pro-Russian news media and sites (e.g., Sputnik and RT). Second, it tries to paint a bad picture of adversarial governments and their officials by obtaining and publishing confidential and/or private information via cyber-attacks and publishing these files on websites such as WikiLeaks or news media websites. These operations are often done by APT groups such as APT 28 (also known as Fancy Bear) and APT 29 (also known as Cozy Bear) which will be further analysed in section 6.1. Lastly, it employs "trolls" (these are individuals who spread misleading and pro-Russian information via blogs and news forums) to spread a better reputation of Russia to foreign adversaries. They also aim to discredit anti-Russian information. This practice was discovered after members of the hacker group Anonymous posted documents on WikiLeaks exposing the Russian government to evidence of paying "troll farms" which are groups of hundreds of trolls (Connel and Vogler, 2016).

These practices have led to a new cold war between the U.S. and Russia which the study of Shuya (2018) has analysed in depth. The direct causes of these are part of the information war Putin has started against the west. This first started with the cyber-attacks against Estonia in 2007. These were DDoS attacks against government and news websites after Estonia had moved a statue dating back to the Soviet era to a different location. This attack lasted days resulting in the halt of the digital functioning of Estonia. Russia quickly moved on to new targets with first attacking Georgia with a similar cyber-attack during the Five Days War. As Russia controlled the internet access of Georgia it could hide its blame and disrupt military communications. Seven years later, in 2015 and 2016 Ukraine was victim to advanced cyber-attacks against critical

national infrastructure. The Ukrainian power company Prykarpattyaoblenergo was victim to a cyber-attack targeting its Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) in a control centre, an attack that was only seen once before in the STUXNET attack on the Natanz nuclear facility in Iran (Shuya, 2018).

This showed the world Russia had greatly improved its offensive cyber capabilities. This was seen a few years later again when evidence was found that Russia had meddled with the 2016 U.S. elections. This attack was a result of the sanctions the U.S. put in place on Russia after it annexed the Crimea in Ukraine. In 2016 Putin recognized that then President Barack Obama could not hold his position for another term and saw that its republican opponent, Donald Trump, was less hard on its relations with Russia. To prevent the democratic candidate, Hilary Clinton, to win and resume the sanctions Putin worked to influence the operations of the democratic party and the minds of the voters. Russia thus hacked into the Democratic National Committee and leaked sensitive information, preventing the party from retaking the presidency. To influence the voters, Russia employed troll factories to spread propaganda by turning the discussion to the leaked documents and Hillary Clinton. This tactic stems from Stalin who made sure people were joining the discussion thereby forcing them to listen. This manipulation became a success as it divided the American public greatly on many topics. Russia has therefore shown that its greatest asset is its cyber capability as with it, it can attack any country without dire consequences (Shuya, 2018).

A study by Shackelford *et al.* (2017) analysed the threat Russia posed to the U.S. critical national infrastructure. It found that the advanced attacks that Russia has developed against the power grid in Ukraine and their effects did not only remain in eastern Europe. The APT that executed this attack, attributed to Sandworm Team, has also attacked the North Atlantic Treaty

Organization (NATO) and governmental institutions in Europe. This has raised the concern of the researcher on whether other western countries are able to withstand against such attacks. This concern is based on three observations. First, energy grids in western countries often use outdated ICS which are unable to prevent an adversary from penetrating. Although these countries try to update with newer systems, this leads to a multiplication of vulnerabilities according to a report about smart grids by the Congressional Research Service. Second, there seems to be an increase in such types of attacks which has increased the perception of Russia as a threat and other nations performing similar attacks. This is strengthened by the results of some evaluations of the ICS of the Ukraine energy grid that tell that it was more secure than similar systems in the U.S. Lastly, as the sophistication of these APTs has risen, governments try to keep up implementing security strategies. This is especially important as an attack on a power grid can influence much more in terms of retribution, monetary gain, or a social or political cause to another country than a simple DDoS attack on a government website (Shackelford *et al.*, 2017).

Regarding the recent increase in cyber-attacks against Ukraine since the war in 2022 there seems to be no new academic analyses covering this new doctrine. This is a gap that dissertation aims to fill in. As for the other studies, despite providing valuable knowledge on Russia's cyber capabilities and strategy, it seems that no comprehensive framework has been created to cover the majority of the targets and methods used for comparing NCSSs.

2.2. Comparison of NCSSs

As for comparing NCSSs of the U.S., France, Germany, and Ukraine, only the first three have been compared. The results of the studies of these comparisons have been varied, however. The first study comparing these has been done by Luiijf *et al.* (2013) which compared the NCSSs on nine different aspects such

as perceived threats and identified strategies and stakeholders. The NCSSs used in this study were published between 2009 and 2011. What was remarkable is that none of the Strategies specifically named Russia as a threat actor. In the same year Luiijf, Besseling and Graaf (2013) also published a study comparing 19 different NCSSs with mostly the same countries. The NCSSs where mostly compared on the same questions as the previous study and no country specified Russia as being a cyber threat.

A year later another study was published by Tatar *et al.* (2014) who compared the same NCSSs of Germany, France, Turkey, the Netherlands, the U.S., and the United Kingdom. The method of comparison differs from the previous studies as they used a framework developed by Luiijf and Healey (2012) which uses five national cyber security mandates. These being: military cyber operations, counter cybercrime, intelligence, and counterintelligence, cyber security crisis management and critical infrastructure protection, and internet governance and cyber diplomacy. The results showed that the NCSSs focussed on the situation in their own country, such as the economic effects of cyber-attacks and their fight with cybercrime while other countries focused on using cyber as a tool to enhance military capabilities, others prioritize preventing cyber-attacks against critical national information infrastructures and key resources in order to maintain the functioning of society.

In 2016 a study was published by Shafqat and Masood (2016) that compared twenty countries including the U.S., France, and Germany and included the revised NCSSs of the Department of Defence (DoD) of the U.S. published in 2015. Four years later in 2020 the U.S. and France were once again compared as they both ranked in the top five of the Global Cybersecurity Index in 2018. This study, published by Tvaronavičienė *et al.* (2020), compared their NCSSs, of which the most recent were published in 2018, but only focussed on their focus national infrastructure. Russia was not mentioned in any NCSSs as a

threat. The results of the study were rather shocking as although the U.S. scored well on all categories (which consisted of legal regulation, governance, risk management, security culture, technology management and incident management), France scored nought in the categories of risk management, security culture and technology management and very low (lower than the U.S.) on the other categories. The U.S. scored the highest in all three countries.

The crux of these studies in relation to this dissertation is that there has not been a full in-depth comparison made with the NCSSs of Germany, France, U.S. and Ukraine and their evolution. Hence, there appears to be a gap in comparing recent cyber defence tactics and strategies used by Ukraine to defend against Russian attacks to tactics and strategies of other western countries. Furthermore, there also appears to be a gap in comparing any NCSS with framework focussed specifically on the Russian cyber threat. This research aims to develop such framework.

2.3. Analysis of the NCSS of Ukraine

Although Ukraine did not have a NCSS when these comparisons were made, there also appears to be a gap in the academic literature of comparisons done with NCSS after 2018. This means that neither more recent NCSSs of the same countries have been compared but also the NCSS of Ukraine has not been compared to any. The Ukraine NCSS has however been analysed by a few studies since the Russian cyber doctrine took affected Ukraine in 2014. One of such studies was done by Nataliya (2016). The findings showed that the NCSS focussed on combating the hybrid threat coming from Russia, but it still had to solve problems. The study provided several recommendations. First, to build political will, to understand, measure and protect the cyber security of the state. Second is to raise awareness of cyber hygiene for all civil servants, military personnel, and critical national infrastructure operators and

sanctions put in place when these are not met. Third is to increase the capabilities of human resources by training and hiring IT-professionals. Furthermore, the author recommends creating a Multi-Stakeholder Cybersecurity Platform between the government, business, and international donors. This platform should aim to provide free services to each other in raising, for example, cyber security awareness and recommendations for policy making. Moreover, a register of all national information objects should be adopted together with a legal framework for protecting critical cyber infrastructure by formulating the owners and their responsibilities. The author also recommends that to improve the prevention and investigation of cybercrime and promote international collaboration in this field, the cybersecurity policy of Ukraine should incorporate steps such as increasing penalties for cybercrime and enforcing the Budapest Convention's requirements for service providers to retain, protect, and partially disclose computer data upon request from authorized entities. This study recommends focussing on governmental and private sector cooperation and transparent policy (Nataliya, 2016).

A similar recommendation to establishing cooperation between the government and private sector was also made in a different study published a year later by Vakulyk *et al.* (2020). It analysed the Ukraine NCSS based on its legal, organizational, and technological methods. The results showed that in Ukraine, countering and preventing cyber threats is based on a legal basis that consists of legal documents. This legal basis is in addition to the NCSS of Ukraine. As for the organizational method The Cyberpolice Department of Ukraine is given a central place in the system which is different from France and Germany where the National Cybersecurity Agency (ANSSI) and the Cyberdefence Center (Cyber-AZ) respectively are at the centre. The study concluded however, that Ukraine has not yet established cooperation between the public and private sector for improving the cyber security of the country. It

thus recommends establishing such cooperation and communication but also to create a legal and institutional framework to support.

A more recent study analysing information security of the Ukrainian Defence Forces also came to the same conclusion. According to Zolotar *et al.* (2022) the information resources of the Defence Forces are interrelated to each other which makes pointing out one key resource difficult without taking into account the rest. One issue the study showed is that the legislation of Ukraine distinguishes between cyber security and information security. The author stresses the importance of enhancing the information security of Ukraine as a nation and its Defence Forces, which can be achieved by optimizing the system responsible for safeguarding the information space, fostering collaboration between the public and private sector similarly to Germany, and ensuring that these entities have competent IT-professionals working to protect the information systems.

3. Methodology

Different methodologies were needed to achieve the three research questions to answer the main research question. To answer the research question 1, first hand sources were consulted as much as possible such as reports from government agencies like the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the SSSCIP of Ukraine, and from private organizations such as Google and Microsoft. This was needed to get information as close as possible from the organizations that have experienced and analysed the Russian cyber doctrine.

Moreover, as the war has started a year ago there is limited insight into the cyber doctrine since. Hence, interviews were conducted with cyber security experts who study the Russian cyber threat experienced by Ukraine or support organizations defending against it. It was therefore chosen to use the grounded

theory as its ontologically assumes that theory can be discovered from subjects who experienced a similar process. This methodology therefore helps to find theories regarding the Russian cyber doctrine (Creswell, 2007). It is important however to mention the bias and limited sample size when using this method (Bogdan and Biklen, 1998) (see section 5 for limitations).

Experts were contacted via the network of the researcher and LinkedIn. The age and gender of these experts were not specified; selecting experts was only based on their knowledge and background on the subject of the Ukraine cyber war. In total six interviewees were conducted of which three were Ukrainians based in Ukraine consulting organizations on cyber security, two other experts (not Ukrainian) were working in the Netherlands analysing the cyber threat of Russia and the other expert was an independent researcher on the cyber war. The importance of ethics was taken into account as the identities of these experts and organizations they work for are made anonymous to protect them from any harm caused by information they have shared. All interviewees gave consent to be interviewed and their audio recorded for transcription analysis.

To identify similar themes a semi-structured interviews were taken (see appendix 1 for interview outline), and grounded theory analysis was done on the transcriptions. Grounded theory was chosen as it is a qualitative research method that makes it possible to develop concepts, categories, and theories that emerge from the data itself (Strauss and Corbin, 1994). After six interviews repetition of themes could be observed from the data hence no more interviews were taken. Interviews were held on online platforms Zoom and Microsoft Teams and only audio was recorded to protect the anonymity of the participants as much as possible.

For the second research question NCSS of the case study countries had to be analysed on whether they mentioned targets and TTPs and strategies to protect

(against) them. This was done by searching the NCSS for the sector and TTP names and words related to them. For this research question the case study method was used as it makes it possible to analyse multiple sources (NCSSs, laws and interviews) to find and understand, in this case, if and how a country formulates strategies to protect itself from attacks used by the Russian cyber doctrine. The researcher is therefore often led by the data (Fidel, 1984; Creswell, 2007: 73).

For the last research question, recommendations were made based on differences between the score of and strategies formulated in the NCSS or initiated by the countries. Experts were also asked in interviews to provide recommendations for states and organizations to protect themselves. Hence, grounded theory was also used to find common recommendations.

4. Case study selection

This dissertation compares the NCSSs of the U.S., France, Germany, and Ukraine. These countries have been chosen as they all have experienced an increase in frequency of Russian cyber-attacks after 2014. This is around the same the annexation of Crimea in Ukraine started. Although there are many other countries that could have been chosen (who also have mature NCSS such as Estonia and the United Kingdom) as case studies for comparison with Ukraine. The chosen countries all started to experience an increase of Russian cyber-attacks around the same time which makes their situation comparable. This is something that other potential countries lack. These countries had therefore the same amount of time to update and revise their NCSS according to the Russian cyber threat since their first attack. In this section the reasons for choosing each of these countries will be elaborated on.

The U.S. has always had an unstable connection with Russia ever since the fall of the Soviet Union. As these relations are very critical for strategic safety

between the west and east, more important than the cases of France and Germany, the Unites states is therefore an outlier among the chosen countries. Consequently, it has received a few cyber-attacks from Russia before 2014. One of these being the 1999 investigation called “Moonlight Maze” into a breach of confidential information from different government organizations such as the U.S. National Aeronautics and Space Administration and the Pentagon. The investigation concluded that the threat actor (person or group inflicting a cyber-attack) was “Turla” which is a Russian APT group (Pankov, 2017). In 2008 the DoD was also hit by a cyber-attack. A pentagon official said it was “the most significant breach of U.S. military computers ever” (Knowlton, 2010). Although it has not officially been attributed to Russia, investigators were suspicious as the code was used by a Russian APT before (Shachtman, 2010). The next Russian attack the U.S. experienced was however after 2014. In 2015, the State Department and the White House were both victims of sophisticated cyber-attacks. The State Department experienced malicious activity in its email system, which although unclassified, contained information valuable for foreign intelligence agencies. It was suspected hackers working for the Russian government were behind this (Perez and Prokupecz, 2015b). The attack targeted to the White House was an unclassified system that holds the itinerary of the president which was protected by the State Department. Although it is not confirmed, also in this investigation were traces left that pointed to the Russian government (Perez and Prokupecz, 2015a). Following these attacks officials of the Unites States government began to grow concerned about the Russian cyber threat as they were more advanced and persistent than expected. These cyber-attacks came around the same time when the U.S. and Russia conflicted over issues regarding the annexation of Ukraine and military operations in Syria (Perez and Prokupecz, 2015a).

As for France, it did not experience Russian cyber-attacks before 2015. In April in 2015 its international broadcasting service TV5Monde was taken out of the air by a group called the Cyber Caliphate. This group took the first responsibility and linked themselves to the Islamic State. Later investigation suggested however that it was carried out by a Russian APT group which is generally known as APT 28 and linked to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (also known as the GRU). The motive for the attack remains unclear to this day (Corera, 2016).

The case study of Germany was chosen as it also experienced its first cyber-attack in early 2015. In this cyber-attack 2,420 important files were stolen from a parliament inquiry. According to the German newspaper Frankfurter Allgemeine Sonntagszeitung, a senior security official said that it is "highly plausible" that the cyber theft of files from a German parliamentary inquiry was conducted by Russian hackers (Wehner and Lohse, 2016). The files that were stolen were published a year later by WikiLeaks. The date of the files suggests they came from the hack in 2015. The files were originally stored electronically at parliament for an inquiry into the National Security Agency's interactions with Germany's BND foreign intelligence service. Security sources believe that there are parallels between the German attack and the theft of messages from the server of the U.S. Democratic Party (Wehner and Lohse, 2016).

5. Limitations

As this research covers the topic of the Russian cyber doctrine which will continue to develop for the foreseeable future, there are a few limitations to the findings. First, data gathered to analyse the Russian cyber aggression against Ukraine has been collected between March 1st and July 1st of 2023. Furthermore, the threat groups covered in the analysis are only ones those that have been significantly active to be covered by multiple distinguished sources

such as Google and CISA. However, the typology of Russian cyber threat groups and their targets and TTPs analysed in this research is only indicative of the time of writing. Some groups may disappear, and new groups appear. It is therefore important to mention that although the Russian war against Ukraine is an important context in which this research takes place, it is not the primary focus. Instead, it aims to get a broader understanding of Russian cyber threat groups in the current state of affairs.

Interviews taken with cyber security experts were not focussed on discussing technical remedies to defend against Russian cyber aggression as such information is confidential and could compromise the security of the organization or individual when shared in this research. Instead, the interviews focussed on general strategic initiatives taken by the Ukraine government and organizations and providing general strategic recommendations. Notwithstanding, the interviewees are prone to have bias in their answers. This can be due to their stance in the conflict or their experience of Russian cyber aggression. This bias could also explain the limited interested in participating in an interview, hence the sample size of six.

6. Research question 1: Analysis of the Russian cyber doctrine for developing the framework

In this section the Russian cyber doctrine is analysed to develop the framework for comparing NCSSs. As Russian APTs attack many different targets and uses many different techniques we cannot describe each attack individually. To give a better overview of this threat, an overview of the most common targets and TTPs for each Russian APT (per Russian intelligence agency), hacktivist and cybercrime groups, and private companies. This followed by a quantitative summary of the history of the Russian cyber doctrine and recent insights gathered from interviews and reports.

For an indexed overview of the groups covered please see table 1.

Table 1: overview of Russian hacker groups covered in this section.

The Russian Federal Security Service (FSB)	1. Dragonfly 2. Dragonfly 2.0 3. Gamaredon Group
Russian Foreign Intelligence Service (SVR)	4. APT 29 5. InvisiMole
Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS)	6. APT28
Main Center for Special Technologies (GTsST)	7. Sandworm Team
Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)	8. Temp.Veles
APTs aligning with the Russian cyber doctrine	9. Turla
Hacktivist groups aligning with the Russian cyber doctrine	10. Killnet 11. XakNet Team 12. Zarya
Cybercrime groups aligning with the Russian cyber doctrine	13. The CoomingProject 14. MUMMY SPIDER 15. SALTY SPIDER 16. SCULLY SPIDER 17. SMOKEY SPIDER 18. WIZARD SPIDER
Other espionage groups	19. ALLANITE

	20. Ember Bear 21. Nomadic Octopus
Private companies supporting Russian intelligence agencies	22. NTC Vulkan 23. ERA Technopolis 24. Pasit, OA 25. SVA 26. Neobit, OOO 27. Advanced System Technology, AO 28. Pozitiv Teknolodzhiz, AO

6.1. APT groups linked to Russian intelligence agencies

First APT groups proved to be connected to Russian intelligence agencies are covered. For a tree map overview of which APT group is connected to which group please see figure 1.

Figure 1: APT groups connected to Russian intelligence agencies

6.1.1. The Russian Federal Security Service (FSB)

This also includes the FSB Center 16 and Center 18 or Military Unit 71330. This research has found three APTs that are employed by the FSB: Dragonfly, Dragonfly 2.0 and Zarya.

6.1.1.1. Dragonfly

According to Secureworks, activity of this APT has been going on since at least 2010 (*Resurgent Iron Liberty Targeting Energy Sector*, 2019). Dragonfly is an espionage group as most of its activity involves stealing information from its victims. It is also known by multiple names among different cyber security organizations, these names being TG-4192, Crouching Yeti, IRON LIBERTY and Energetic Bear (*Dragonfly*, 2021). Targets of Dragonfly have thus far been organizations related to state, local, territorial, and tribal (SLTT) government systems in Western Europe and North (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). Furthermore, transportation systems and defence industrial base organizations have also been victim of Dragonfly. This has also included the energy sector since 2013 with watering hole attacks which exploit the browser when a targets visits the compromised website (*Dragonfly*, 2021). Finally, the APT has also target critical national infrastructure such as the water and wastewater systems sector. The TTPs of Dragonfly consist of scanning for internet connected IT-systems and network infrastructure for vulnerabilities and brute forcing publicly accessible web applications. It is also known to exploit these found vulnerabilities to cause destruction (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.1.1.2. Dragonfly 2.0

Although there are arguments that the capabilities of Dragonfly overlap with Dragonfly 2.0 and thus could be the same APT, there is enough proof that these are separated entities according to the MITRE corporation. Dragonfly 2.0 has been active since at least 2015 and is also known by the following names: IRON LIBERTY, DYMALLOY, Berserk Bear (*Dragonfly 2.0*, 2021). Like Dragonfly, Dragonfly 2.0 aims to gather intelligence from its victims. Victims of Dragonfly 2.0 include mostly the oil and gas organizations in the energy sector of Turkey, Europe, and North America. The transport sector has

also been reported to be attacked. Its TTPs are also similar to that for Dragonfly but also include malicious emails, watering hole attacks, custom malware and trojans to infiltrate the network of a target ('Dragonfly: Western energy sector targeted by sophisticated attack group', 2017; *DYMALLOY Threat Group*, 2020).

6.1.1.3. Gamaredon Group

According to the SSSCIP report, Gamaredon Group is a Russian cyber espionage group that has been active since at least 2013 (*Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine*, 2023). It is also known as IRON TILDEN, PRIMITIVE BEAR, ACTINIUM, Armageddon, Shuckworm, DEV-015 and UAC-0010. Ukrainian National Security and Defense Council (NSDC) has stated that it attributes the group to Center 18 of the FSB (*Gamaredon Group*, 2017). According to IronNet, a cyber defence company, recent evidence suggests Gameradon Group is a hacking group that other than executing attacks themselves, also sells its services to other APTs. It is therefore seen as second tier APT as it provides information to top-tier APTs. It therefore lies in between being an APT and a cyber-crime group. Although its TTPs would suggest it being a cyber-crime group, those being phishing emails with malware and trojans, its targets are mainly those residing in Ukraine making it politically motivated (Demoboski, Fitzpatrick and Rydzynski, 2021). Such targets have been the Ukraine government, military, journalists, NGO, and law enforcement organizations (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). As of recently, it has carried out the most cyber-attacks of all actors SSSCIP has tracked (*Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine*, 2023).

6.1.2. Russian Foreign Intelligence Service (SVR)

The SVR is known to be behind APT 29 and InvisiMole (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.1.2.1. APT29

This group known by many names such as IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm and Blue Kitsune (*APT29*, 2023). The operations of this group have been going on since at least 2018 (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). APT29 mostly focuses on targets related to critical nation infrastructure. It has for example been attributed to the SolarWinds supply chain cyber-attack which affected governments and private sector organizations part of national critical infrastructure in Europe, Asia, and the Middle East ('Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor', 2022). In general, it targets governments that are NATO members, institutions for research and think tanks. It is believed that they can be attributed to the 2015 hack of networks at the he White House, Department of State, Pentagon, and the Joint Chiefs of Staff ('The 7 Dukes: 7 years of Russian cyberespionage', 2015). Their TTPs also vary in sophistication as they can both be simple initial exploits that are publicly known or infiltrating networks in a stealthy manner (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). They use custom made malware send via spear phishing emails and use lateral movement (Demoboski, Fitzpatrick and Rydzynski, 2021).

6.1.2.2. InvisiMole

This APT group, also known as UAC-0035 is a cyber espionage group linked to the SVR according to SSSCIP. Their attacks are slow but persistent and target mainly individual Ukrainian diplomats that are deployed outside of Ukraine as well as the Ministry of Foreign affairs. This APT is makes use of

spyware name InvisiMole with the RC2 backdoor to record webcam footage, audio, geolocation, and file access. Infrastructure of the Gamaredon Group has also been used to spread this spyware (*InvisiMole*, 2021; *Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine*, 2023).

6.1.3. Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS)

This military unit also known as military unit 26165 are known to be behind the threat group APT28 (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.1.3.1. APT28

APT28 also known by the names of SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127 (*APT28*, 2021). This espionage group mostly targets public sector and military organizations, organizations in the travel and hospitality sector, research institutions, non-governmental organizations (NGOs) and organizations operating in critical national infrastructure such as energy, financial, telecom, news, shipping, and rail organizations (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022; 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape', 2023). The group has been attributed to many high-profile cases such as the hack of the Hilary Clinton campaign and Democratic National Committee in 2016 to disrupt the U.S. presidential elections ('Our Work with the DNC: Setting the record straight', 2020). It has also been involved with cyber operations against the World Anti-Doping Agency, the U.S. antidoping agency, a nuclear facility in the U.S. and the Organization for the Prohibition of Chemical Weapons (*U.S. Charges Russian GRU Officers with International Hacking and Disinformation Operations*, 2018). According to the MITRE corporation some of these have also been

done together with Sandworm Team (*APT28*, 2021). The main TTPs of this threat group include harvesting credentials via spear phishing and registering domain names for websites that gathers credentials that are similar to tourism and sport organizations, social media platforms and streaming platforms (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). It has also recently been reported to spread a malicious custom version of a Microsoft Windows update (Burt, 2023). The TTPs of APT28 can be very diverse as MITRE reported 85 different techniques (*APT28*, 2021).

6.1.4. Main Center for Special Technologies (GTsST) of the GRU

The GTsST, which falls under the GRU, is also known as Unit 74455 and has shown activity since at least 2009. Industry reports show that GTsST has a long track record of spying on and attacking NATO countries, their governments, militaries, and organizations related to national infrastructure, especially in the energy sector (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.1.4.1. Sandworm Team

This is group is known by the names of ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear and IRIDIUM (*Sandworm Team*, 2023). Sandworm Team is known to cause as much harm as possible with their attacks as they disregard the consequences of the effects it causes. Examples of such an attack was in December 2015 when it got access to passwords of users with Black Energy malware to activate wiper malware KillDisk that wipes and disables infected computer (*Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*, 2021). This led to energy outages across the country. Sandworm is also known to have caused the cyber-attack against the Ukraine energy grid in 2016 using the Industroyer malware (also known as CRASHOVERRIDE) to manipulate the processes of ICS of substations (*Industroyer*, 2022). It has also been attributed to the NotPetya

wiper malware attacks in 2017 which, according to the White House caused 10 billion dollars in damages worldwide (Greenberg, 2018). This attack affected radiation monitoring systems at the Chernobyl Nuclear Power Plant as well as banks, ministries, and public transport sector in Ukraine as well as critical infrastructure organizations in western Europe, U.S., Australia and India (Griffin, 2017; Perlroth, Scott and Frenkel, 2017). Generally, Sandworm Team targets the same organizations as APT28 according to Google ('Fog of war: how the Ukraine conflict transformed the cyber threat landscape', 2023). The Sandworm Team is one of only few APT groups that employ disruptive attacks to ICS. According to the MITRE corporation it has used 15 different ICS TTPs (*Sandworm Team*, 2023). It also uses mainly DDoS attacks and wiper malware which is malware that deletes or overwrites data and programs of computer systems thus making them inoperable (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). It also uses spear phishing where malware is delivered in Microsoft Office documents and is known to control SCADA systems remotely (Demoboski, Fitzpatrick and Rydzynski, 2021).

6.1.5. Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)

The TsNIIKhM is a research branch under the Russian ministry of defense and is associated with the Temp.Veles group and the TRITON malware framework. (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). This malware framework was used on energy facilities resulting in U.S. sanctions and indictements on TsNIIKhM (*UK exposes Russian spy agency behind cyber incidents*, 2022; *Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide*, 2022).

6.1.5.1. Temp.Veles

In general Temp.Veles targets the energy sector such as oil, gas and electricity organizations in the Middle East, U.S., Europe, and the Asia-Pacific

(Demoboski, Fitzpatrick and Rydzynski, 2021). As for its TTPs, it uses its TRITON malware framework, but it is also known to have the capabilities of harvesting credentials, infiltrate networks and use easy to obtain tools (*XENOTIME Threat Group*, 2020).

6.2. APTs aligning with the Russian cyber doctrine

Apart from APT groups being directly linked to a Russian governmental agency, a Joint Cyber Security Advisory (JCSA) also identified APTs aligning with the Russian cyber doctrine (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). These two are known as Gamaredon Group (covered in 6.1.1.3.), and Turla.

6.2.1. Turla

This APT is based in Russia and has been active since at least 2004 with a spike in activity in 2015. Turla is an espionage group and is also known as Group 88, Belugasturgeon, Waterbug, WhiteBear, VENOMOUS BEAR, Snake, UNC4210 and Krypton (*Turla*, 2021; 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape', 2023). One of the high-profile cases Turla was attributed to a major espionage campaign lasting six years of which the victims where governments, military, educational sector, research sector, pharmaceutical, companies, aerospace, and media sector of 45 countries, with a focus on former soviet countries (*Turla Enterprise Evaluation 2023*, no date). Their main TTP was the use of their own made malware called Uroboros, which is a sophisticated malware which can be used against Windows, Mac and Linux machines, with spear phishing (Brewster, 2014). It is also known for hijacking satellite internet connections and infrastructure of other Russian APTs (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). Turla is, according to researchers, also connected to the Moonlight Maze investigation in the 1990s which was mentioned in the case study section (Demoboski, Fitzpatrick and Rydzynski, 2021).

6.3. Hacktivist groups aligning with the Russian cyber doctrine

Recent phenomenon has shown that hacktivist groups have picked up the slack of APT groups who have limited resources according to SSSCIP. The following groups have been identified as hacktivist groups by SSSCIP. (*Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine*, 2023).

6.3.1. KillNet

Apart from having attacked U.S. airports, it has also targeted the U.S. healthcare sector, NATO websites, Lithuania government websites with DDoS attacks as well (*Lithuania Says Hit by Cyberattack, Russia 'Probably' to Blame*, 2022; 'Pro-Russian Hacktivist Group "KillNet" Threat to HPH Sector', 2023; Dahan and Pasha, 2023). In generally, KillNet is known to use DDoS attacks and bruteforce attacks against publicly available services as their TTP (*KillNet Group*, no date). However, it has recently also attacked the American defense contractor, Lockheed Martin, in a more sophisticated attack where according to KillNet, employee data was stolen (Townsend, 2022). As for Ukraine, it has also targeted the Ukrainian government, Ministry of Foreign affairs, and Ministry of Economics. According to SSSCIP it is the most active Russian hacktivist group (*Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine*, 2023).

6.3.2. XakNet Team

This hacktivist group has been established since the start of the Ukraine war in 2022. Just like most other hacktivist groups, the XakNet Team has been established to target Ukrainian organization in retaliation of perceived cyber-attacks against Russia (Vail, 2022). It is believed in the security industry that the XakNet Team also works with Killnet although this was denied by Killnet in a Wired article (Burgess, 2022). According to the cyber security company

Mandiant, the XakNet team also has close ties with the GRU. XakNet has used DDoS, information compromises, and website defacements against Ukraine. Targets so far have been the Ukrainian officials, Ukraine news media and Ukraine energy sector (Gillum, 2022). As for the energy sector, its victim was the largest Ukrainian energy organization DTEK Group although ICS were not compromised (Lyngaas, 2022).

6.3.3. Zarya

The 2023 Pentagon leak by airman Jack Teixeira revealed that an APT group named Zarya has damaged the infrastructure of a Canadian gas pipeline company early in 2023. According to one of leaked intelligence report if the hack succeeded "it would mark the first time" the intelligence services of the U.S. have "observed a pro-Russia-hacking group execute a disruptive attack against Western industrial control systems." (Schmitt and Crowley, 2023). Evidence for the connection to the FSB was found in the fact that a member of the group sent screenshots of the intrusion to the security services though it remains known as a hacktivist group according to SSSCIP (*Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine*, 2023). Zarya is not a well-known group, so it is unclear what its main targets are. According to Allan Liska, a senior security architect at Recorded Future, the group only has caused nuisances. He also said that the group has connections with Cyber Spetsnaz which uses the same TTPs as KillNet (Starks, Nakashima and Coletta, 2023).

6.4. Cybercrime groups aligning with the Russian cyber doctrine

Since the Ukraine war in 2022 Russian cybercrime groups have sided with Russia and stated to attack critical infrastructure sectors. The following are Russian cybercrime groups identified by in the JCSA report (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.4.1. The CoomingProject

This group showed support for the Russian government in a tweet in response to cyber-attacks against Russia. The CoomingProject has also launched a site where they publish leaked data. As of November 2021, they have made data breaches from over 36 companies for sale including those of Orange and Vimeo (*Ain't No Actor Trustworthy Enough: The importance of validating sources*, 2021). They are known as a ransomware group and call themselves similar to the cyber-crime group ShinyHunters on their website (Simpson, 2021).

6.4.2. MUMMY SPIDER

MUMMY SPIDER is a cyber-crime group that is also known as Gold Crestwood, TA542, TEMP.Mixmaster and UNC3443 and is responsible for creating the Emotet malware (also known as Geodo). This malware is used to download other malware such as TrickBot and IceID, which is used to target the banking sector to steal information. MUMMY SPIDER is also known to target the e-commerce, healthcare, academic, government, and technology sector (*Emotet*, 2020; *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.4.3. SALTY SPIDER

This cyber-crime group is famous for operating and developing the Sality botnet first discovered in 2003 which is now also known as KuKu, SalLoad, Kookoo, SaliCode and Kukucka. The most recent version of this botnet is still operating and effective. It appears that the group does not target specific countries or sectors as its activity can be found all over the world. Its Sality botnet is designed to infect machines and download and execute malware (Meyers, 2019). SALTY SPIDER has also been attributed to DDoS attacks against a Ukrainian forum discussing Russian troops infiltrating Kharkiv (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.4.4. SCULLY SPIDER

SCULLY SPIDER, also known as Gold Opera, and is a cyber-crime group that gains money by selling their malware as a service. It does this by operating and developing the DanaBot botnet which is used to infiltrate command and control infrastructure and selling access to its malware where buyers will be able to allocate their own malware. It operates in therefore in the same way as Emotet. The botnet was initially used to infiltrate the banking sector via a trojan but is has been more recently used to give access to other malware such as TrickBot, DoppelDridex, and Zloader. Industry reports indicate that the recent attacks on Ukrainian government organizations where DanaBot is used as a DDoS tool would suggest that SCULLY SPIDER is helping Russia in its offensive against Ukraine (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022).

6.4.5. SMOKEY SPIDER

This cyber-crime group develops the malicious Smoke Loader malware, which is also known as Smoke Bot and Dofoil. The malware is used to load other malware such as DanaBot, TrickBot, and Qakbot on infected systems and has been active since at least 2011 (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). It is famous for being deceptive and self-protective (*Smoke Loader*, 2020). What makes this cyber-crime group aligned with the Russian cyber doctrine is that its malware was found spreading DanaBot in a campaign to launch a DDoS attack against the Ministry of Defence in Ukraine (Schwarz and Stone-Gross, 2022).

6.4.6. WIZARD SPIDER

WIZARD SPIDER, which is also known as UNC2727 and Gold Ulrick, is behind the development of the TrickBot malware and the ransomware-as-a-service named Conti. This cyber-crime earns money by paying for ransomware deployers such as SMOKEY SPIDER for initial access and

earning a share of the profits. When WIZARD SPIDER has obtained access, its members use openly available tools before using Conti. It has also used Emotet, Cobalt Strike, phishing and stolen credentials to get its own initial access (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). Recently the cyber-crime group has said to support the Russian doctrine and threatened to attack critical infrastructure organizations in retaliation to cyber-attacks against Russia and its people (Culafi, 2022). In general, the victims of the Conti malware are organizations in industries such as construction, engineering, legal, professional services, manufacturing, and retail. According to the FBI cyber division, the healthcare sector and first responder networks have also been a victim to Conti ransomware ('FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks', 2021).

6.5. Other espionage groups

This research has also found other Russian cyber groups that are suspected to be espionage groups which actions are in line with the Russian cyber doctrine and suspected to be sponsored by the Russian federation.

6.5.1. ALLANITE

ALLANITE is the only the of the APT groups that has solely targeted industrial control systems. It first activity has been seen since at least 2017 and could also be linked or associated to the groups Palmetto Fusion and Dymalloy (*ALLANITE Threat Group*, 2020; *ALLANITE*, 2022). Its TTPs do also overlap with those of Dragonfly, however ALLANITE has shown to be less destructive and tends to resemble that more of espionage related activity, especially in the ICS domain (*Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, 2022). The overlap might suggest this APT is Russian sponsored or are at least in line with the Russian cyber doctrine (*Allanite*, no date). This is not however corroborated by Dragos (*ALLANITE*

Threat Group, 2020). The group has targeted energy companies and tts TTPs are known to be spear phishing and watering hole attacks (Kovacs, 2018).

6.5.2. Ember Bear

Activity of Ember Bear has started more recently since at least 2021. Ember Bear is also known as Saint Bear, UNC2589, UAC-0056, Lorec53, Lorec Bear, Saint Bear and Bleeding Bear and is likely interested in gaining intelligence from networks of targets (*EMBER BEAR: Threat Actor Profile*, 2022; *Ember Bear*, 2023). This collected intelligence appears to be used for information operations. Their TTPs also show that the actions of Ember Bear are aligned with the Russian cyber doctrine and are partially state sponsored according to Mandiant (Sadowski and Hall, 2022). The main target nations of this group are Ukraine and Georgia, although ministries, pharmaceutical organizations, and financial sector organizations of countries in Western Europe and North America have also been a victim. Ember Bear has also used different wiper malware known as WARYLOOK, GOOSECHASE, and FINTIDE which is made to imitate ransomware, to destroy Ukrainian networks in 2022 (Sadowski and Hall, 2022). In early attacks it also used spear phishing with malicious Word documents ('Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot', 2022).

6.5.3. Nomadic Octopus

Nomadic Octopus which is also known as DustSquad. Its activity has been active since at least 2014. The main targets of Nomadic Octopus have been local governments, diplomatic entities, and civilians of countries in Central Asia (*Nomadic Octopus*, 2022). Such political targets make Nomadic Octopus suspicious as they are similar to what the Russian cyber doctrine targets. Moreover, one of the trojans that Nomadic Octopus developed as their TTP was a Windows version of the Telegram app disguised as used by the Democratic Choice (DVK) opposition party of Kazakhstan. This trojan was

written in the Delphi programming language which makes it unique as there is only one other Russian APT that has used this before, APT28. However, cyber security company Kaspersky does not find a direct link between code written by these groups (*Octopus-infested seas of Central Asia*, 2018).

6.6. Private companies supporting the Russian cyber doctrine

Russian technology companies have also been observed helping the Russian cyber doctrine as recent leaks and U.S. sanctions and would suggest.

6.6.1. NTC Vulkan

Russian cyber security consultancy company NTC Vulkan had its documents leaked in February 2023 to the German press revealing its operations supporting the Russian cyber doctrine. The leak, which consisted of roughly 1000 pages of internal documents which were dated between 2016 and 2021, unveiled that Vulkan had Russian agencies connected to GRU, SVR and FSB as their clients. Even APT groups APT29 and Sandworm Team were among these clients. The documents reveal classified tools Vulkan developed for these clients:

- A scanning tool called Scan-V, which scans the internet for vulnerabilities in systems that can be exploited for future cyber-attacks.
- A monitoring tool Amezit and is used to monitor and control access of internet usage and spread disinformation in Russian controlled regions. Usage of this system in the Ukraine war in 2022 has also been observed in the form of social media accounts linked to Vulkan by reporters of news organizations analysing the leaked documents. Russia is also known to shut down internet access in occupied parts of Ukraine.
- A training tool called Crystal-2V which is used to train agents on attacking critical infrastructure such as transportation systems for sea, air and rail and vital systems for water and energy supply systems.

Among the leaked documents was also a U.S. map with marked targets for potential cyber-attacks. All in all, this leak shows the advanced capabilities of the Russian cyber power and its cooperation with the private sector and the impact it can create (Antoniadis *et al.*, 2023; Harding, Ganguly and Sabbagh, 2023).

6.6.2. Private companies on U.S. sanction list

The U.S. Department of the Treasury had already set sanctions before the war on the 15th of April 2021 on Russian technology companies that support Russian intelligence services (*Treasury Sanctions Russia with Sweeping New Sanctions Authority*, 2023). For an overview of the companies and their clients please see figure 2.

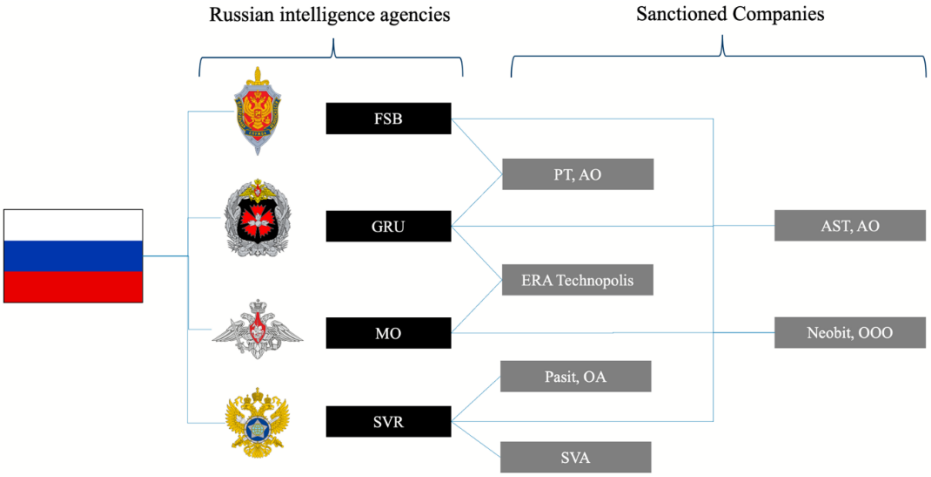

Figure 2: Sanctioned companies who offer services to Russian intelligence agencies (*Treasury Sanctions Russia with Sweeping New Sanctions Authority*, 2023).

The reason why these companies cooperate with Russian intelligence agencies is because the power dynamic between these two is skewed. According to a former U.S. intelligence official who was interviewed by MIT Technology Review, this relationship is complex and abusive as the pay is lower than with

other clients and the demands are one-sided. These companies also feel threatened if they do not cooperate (O'Neill, 2021).

6.7. Quantitative history of targets and TTPs used by Russian threat groups

To translate the threat of the above groups in a quantitative historic overview, an analysis was done on all the groups mentioned on the MITRE ATT&CK website, as it provides unique TTPs used for each group (*Groups*, no date). Groups not covered are 10, 12, 13, 14 and 15 (see table 1). The analysis showed that the TTP used most often was the abuse of commands and scripts of Microsoft PowerShell (ID T1059.001) (*Command and Scripting Interpreter: PowerShell*, 2023). It is often used in the execution phase of a cyber-attack after a malicious actor has gained initial access to a system. This TTP was used by nine cyber threat groups (see figure 3), one of which is Sandworm Team in the 2016 attack on the energy grid of Ukraine (*2016 Ukraine Electric Power Attack*, 2023). This occurrence does not indicate a high likelihood as there have been 273 other unique techniques reported of which this one accounts for only 3.3%.

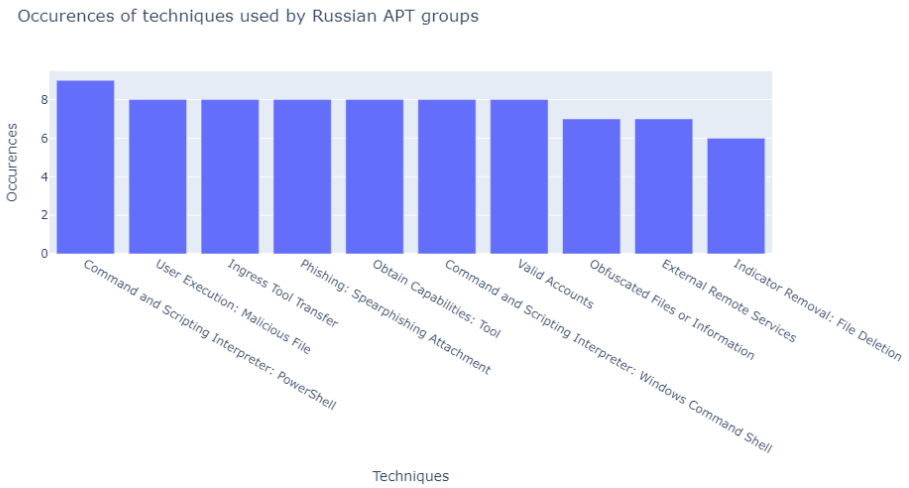

Figure 3: Top 10 occurrences of techniques used by Russian APT groups (*Groups*, no date).

Furthermore, TTPs could either target systems in the enterprise domain or the ICS domain. By counting the number of different techniques used against each target, the analysis showed that 4.75% of unique attacks were used on ICS with 95.2% unique TTPs on enterprise (see figure 4). This could suggest that ICS systems are more vulnerable and do not need many sophisticated attacks or ICS are less monitored.

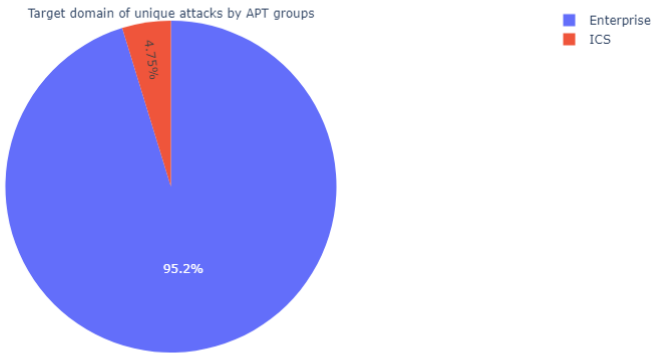

Figure 4: Target domain of unique attacks used by APT groups (*Groups*, no date).

Other sources have also quantitatively analysed the Russian cyber doctrine on a more recent time frame. For example, the U.S. Treasury Financial Crimes Enforcement Network published an analysis of financial trends between Jul7 2021 and December 2021. Their analysis has found that malware connected to Russia has been the most prominent in ransomware incidents (‘Ransomware Trends in Bank Secrecy Act Data between July 2021 and December 2021’, 2022).

At the same time Google noted a spike of phishing campaigns against Ukrainian targets and 14 thousand emails internationally around April and October of 2021. It was during this period that Russia started preparing troops

at the border with Ukraine. During this time Russia targeted over 150 domains of the Ukraine military and government as well with the domain of the Ministry of Defence being targeted the most. Furthermore, according to the report Google saw an increase of 300% of phishing attacks in the same period to NATO countries from Russia. APT28 was the main culprit here as it has been responsible for more than three quarters of phishing attacks against NATO countries (‘Fog of war: how the Ukraine conflict transformed the cyber threat landscape’, 2023).

6.8. The Russian cyber doctrine since the Ukraine war in 2022

Since the start of the war in February 2022, the Russian cyber doctrine has evolved in multiple fazes which has been tracked by private sector and public sector cyber security teams. Those of Microsoft have found a huge influx of attacks in February using malware named FoxBlade, which makes the infected system carry out DDoS attacks (*DoS:Win32/FoxBlade.A!dha threat description*, 2022). This attack was recorded 20 times which is the highest type of attack recorded in a single month in the year of 2022. These attacks were recorded targeting government systems in Ukraine (‘A year of Russian hybrid warfare in Ukraine’, 2023).

Microsoft also recorded nine different types of wiper malware which had not been discovered earlier and two types of ransomware used against a hundred different Ukrainian organizations. According to the same report, the top three sectors targeted most in Ukraine were the public sector (with 46 organizations), IT and communication sector (18 organizations) and energy sector (16 organizations) (‘A year of Russian hybrid warfare in Ukraine’, 2023).

As for outside the Ukraine, the top three most targeted sectors were government (with a hundred attacks, or 49% of all attacks), IT and

communication (51 attacks or around 20% of attacks) and think tanks and NGOs (31 attacks) (*Defending Ukraine: Early Lessons from the Cyber War*, 2022).

Moreover, both Google and Microsoft have seen new trends in the Russian cyber doctrine that are likely to continue as the war continues. Microsoft has first noted that apart from the destructive use of wiper malware, ransomware is also for destruction. They have also seen a rapid improvement of ransomware. Second, Russian APTs have become more diverse with using backdoors, spear phishing, spreading pirated and weaponized versions of common software, use of public exploits and trust relationships between clients and IT companies to get initial access. Thirdly, Microsoft observed an increase in hacktivist groups and links between these groups and Russian military intelligence agencies. These groups have been established to increase the projection of power of the Russian cyber doctrine (‘A year of Russian hybrid warfare in Ukraine’, 2023).

Furthermore, according to SSSCIP, the second half of 2022 showed that about one third of all attacks were focused on destruction and the other two thirds were spear phishing attacks with the objective of stealing information. The APT groups Gamaredon Group and Sandworm Team were especially active in this second half of the year with conducting cyber espionage and destructive cyber-attacks respectively. The targets of the phishing attacks have also moved from their primary target to organizations connected to the primary target via their supply chain. The FSB, GRU and SVR were focussed on collecting intelligence. Their main targets were government, energy, private organizations, logistics, and defence organizations. As for communication infrastructure, IT companies connected to supply chains for providing services to the government were targeted primarily. Although the media sector was targeted in the first half of 2022 with the goal to exert psychological manipulation, the second half saw more disruptive attacks with wiper and

ransomware being used primarily by Sandworm Team. Another trend that has appeared is that Russian APT groups have experienced a lack of resources as their teams usually consists of 20 people and cannot recruit new talent as such people are in the private sector and are not in favour of the actions of the Russian government and in many cases have left the country. As a result, it is observed that these APT groups have outscored their work to criminal and hacktivists organizations (*Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine*, 2023). The TTPs of hacktivist groups have also become more novel and to a similar level to those of state sponsored APT groups ('Fog of war: how the Ukraine conflict transformed the cyber threat landscape', 2023).

All in all, the Russian cyber doctrine has focussed on espionage and destructive attacks with phishing, wiper malware, ransomware, and DDoS attacks. The targets have not changed much with government, communication infrastructure, NGO, energy, financial and defence sector being targeted the most.

6.9. Insights of Russian cyber threat since the start of the war gathered from interviews with cyber experts on Ukraine

From the grounded theory analysis on the transcription of the interviews, a number of themes came up relating to the Russian cyber doctrine and the recent trends thereof. These themes will be explored in this section.

The first theme identified was that of threat groups. These being: hacktivists, cybercrime groups, APT (state-actors) and private companies (see figure 5). According to figure 1, interviewees talked the most about hacktivists (an occurrence of 23) and this was also reflected in the codes reflecting trends (see figure 6). This is mostly because Russia experiences a 'brain drain' according to some interviewees, meaning that skilled cyber practitioners are leaving the country or do not work in support of the Russian doctrine anymore.

Interviewee 3 (2023) said that the increase of hacktivism could be a result of this: “I would say that in order to expand their capacity, currently we see a bit of a different trend, which is usage of hacktivism” (Interviewee 3, 2023). The same interviewee also went on to say that “ (…) we are a bit of under the impression that they don't solely operate on their own, you know, but there is some kind of a relationship between the state and those groups itself” (Interviewee 3, 2023) . The interviewee could not provide any evidence, however.

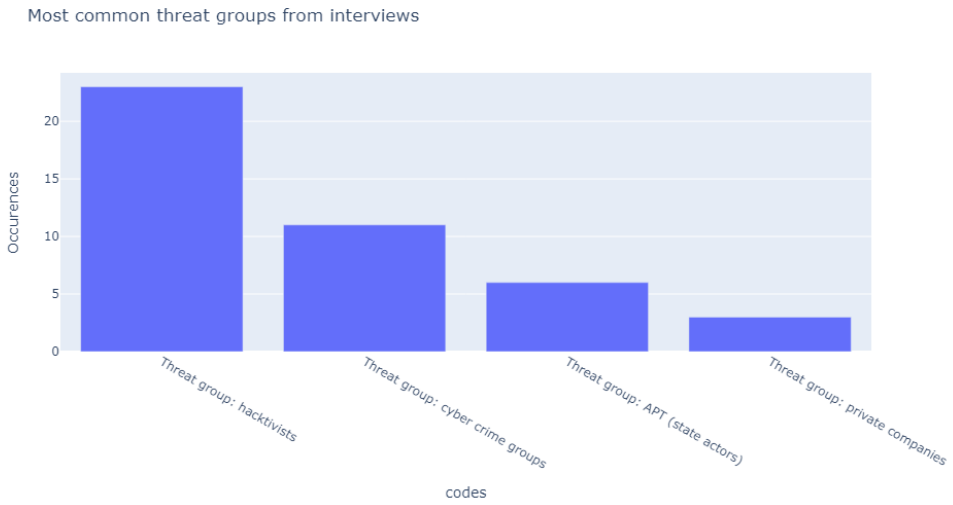

Figure 5: Most common threat groups from interviews (Interviewee 1, 2023; Interviewee 2, 2023; Interviewee 3, 2023; Interviewee 4, 2023; Interviewee 5, 2023; Interviewee 6, 2023).

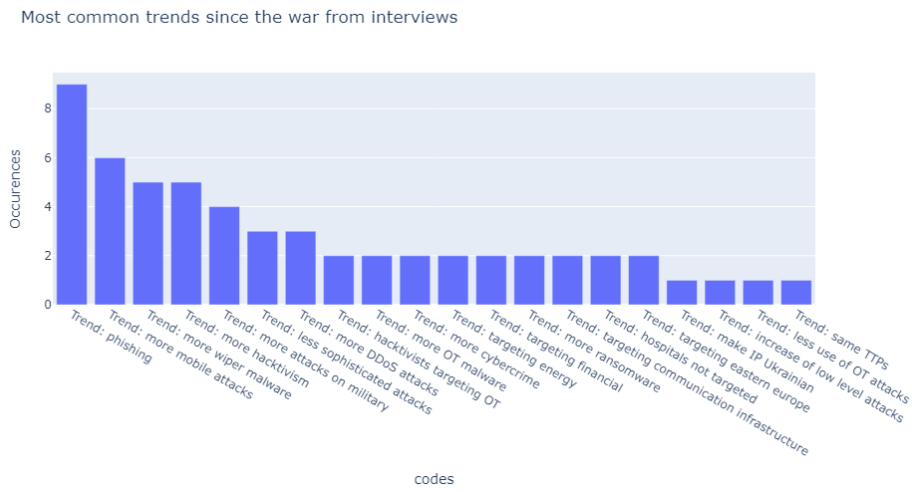

Figure 6: Most common trends since the war from interviews (Interviewee 1, 2023; Interviewee 2, 2023; Interviewee 3, 2023; Interviewee 4, 2023; Interviewee 5, 2023; Interviewee 6, 2023).

As for TTPs, the most common TTP mentioned in the interviews were DDoS attacks followed by phishing and wiper malware (see figure 7). The most mentioned trend regarding TTPs was phishing followed by wiper malware attacks and mobile attacks (see figure 2). This would suggest that the most common attacks used since the war are DDoS attacks phishing attacks, mobile attacks, and wiper malware. This was also confirmed by interviewee 5 (2023): “the main focus of attacks is usually DDoS attacks, phishing, trying to steal data”. As for mobile attacks, according to interviewee 3 one third of all attacks related to propaganda are based on Android: “So one third of their attacks, which is looking from a very broad view, tend to be mobile, phone, and Android specifics” (Interviewee 3, 2023). This is because Android smartphones are used more by Ukrainians. An example of such an attack is an Android application made by the Turla APT that pretended it was made by the Ukrainian Azov Regiment and tricked the user into thinking it could help with DDoS attacks against Russian websites but, helped Russia track pro-Ukrainian activists (Leonard, 2022). Interviewee 6 (2023) also mentioned that the

Ukraine military has experienced attacks on their drones and artillery that are controlled by the Android operating system.

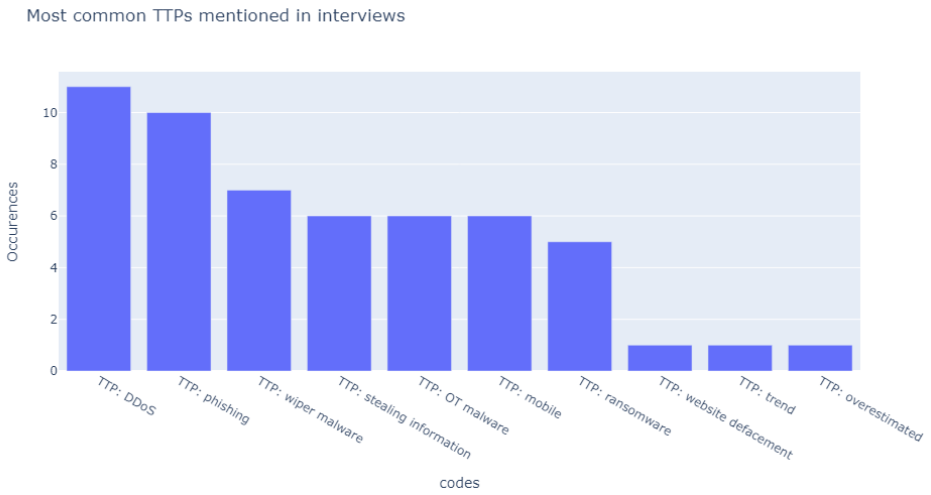

Figure 7: Most common TTPs mentioned in interviews (Interviewee 1, 2023; Interviewee 2, 2023; Interviewee 3, 2023; Interviewee 4, 2023; Interviewee 5, 2023; Interviewee 6, 2023).

As for targets, Operational Technology (OT) systems was mentioned the most followed by the energy sector, government, military, and financial sector (see figure 8). What was interesting is that interviewee 3 (2023) mentioned that a lot of attacks are focussed on eastern European targets and targets in countries that support Ukraine in the war. Furthermore, communication infrastructure was also ranked high with interviewee 6 (2023) mentioning the recent increase in research on developing attacks against the SpaceX Starlink system which Ukrainians use to get internet access in case of a shutdown or blackout. Also, Small and Medium-sized Enterprises (SMEs) were also targeted as their cyber defence was not mature enough. These trends have also been confirmed by codes in figure 6. There is an increase in attacks on military targets since the start of the war, hacktivists targeting OT infrastructure, more attacks on energy, communication, and financial sector. Hospitals were targeted less

since the start of the war. This is because they have shown to be very resilient as they can quickly change to a paper-based system. Lastly, there have been attacks on media companies both before and during the war to spread propaganda.

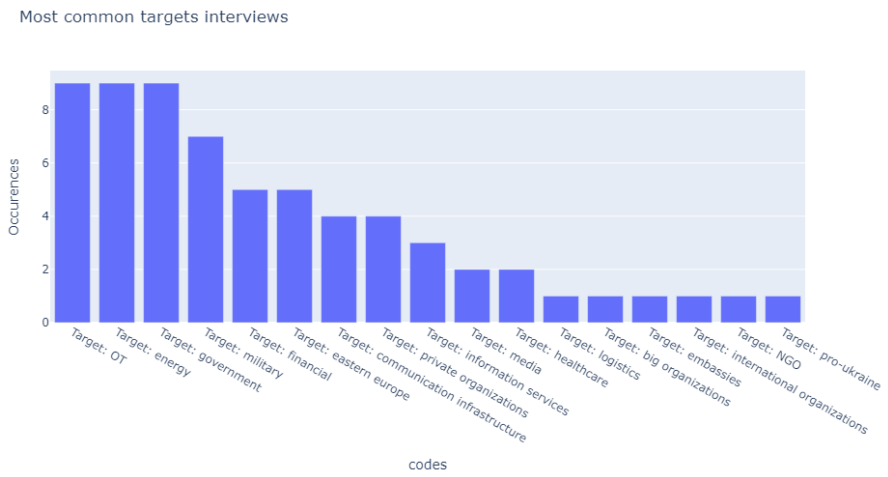

Figure 8: Most common targets in interviews (Interviewee 1, 2023; Interviewee 2, 2023; Interviewee 3, 2023; Interviewee 4, 2023; Interviewee 5, 2023; Interviewee 6, 2023).

During the interviews also the theme of the motivations or ideas behind the cyber-attacks of Russia were discussed (see figure 9). The main motivation seems to be psychological influence. They aim to achieve by “not just to steal the data, but also to demonstrate the capabilities and assert the psychological pressure on Ukrainian citizens” according to interviewee 1 (2023). This is also reflected in the second most common motivation which is to destroy its targets which leads to the third, disrupt the way of living.

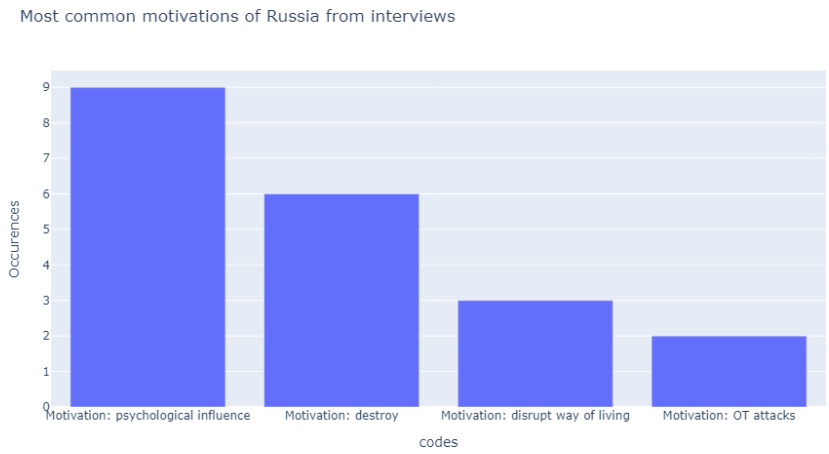

Figure 9: Most common motivations of Russia from interviews (Interviewee 1, 2023; Interviewee 2, 2023; Interviewee 3, 2023; Interviewee 4, 2023; Interviewee 5, 2023; Interviewee 6, 2023).

6.10. Final framework

By taking all the common targets and TTPs used by Russian APT groups and cyber-crime groups into account, a framework can be formed with which the different NCSSs of Ukraine, U.S., Germany, and France can be compared and evaluated with. To do this in a transparent way a table was created (see Table A in appendix) containing the most common targets and TTPs per group taken from the above analysis. From this table bar charts were made counting the most common targets and TTPs (see Figure A and B in appendix). For targets all counts above 3 were chosen to be significant and for TTPs all above 2. For each target and TTP important sub targets are mentioned and its trend since the start of the war.

To compare the NCSS in a quantitative way a score is given based on three parameters. These scores and parameters are the following:

- For not mentioning a TTP or Target a 0 is given to the NCSS.
- For mentioning a TTP or Target but no strategy is given to protect (against) it, a 1 is given to the NCSS.

- For mentioning a TTP or Target and formulating a strategy to protect (against) it a 2 is given to the NCSS.

To more easily compare the separate NCSS, a score can be calculated for each country by summing all scores which will yield an overall score that reflects how well the NCSS of these countries are protect against the Russian cyber doctrine. This total score can be found in the last row of the framework (table 2) under 'Total score Russian cyber doctrine'. Also, a score per target and TTP can be calculated for each NCSS of the countries, this total score can be found in the framework (table 2) under 'Total score targets' and 'Total score TTPs' respectively. This framework should be used with caution in the future as the Russian cyber doctrine may evolve.

Table 2: framework for comparing NCSSs based on incorporating strategies protecting themselves against the Russian cyber doctrine.

		Ukraine	**United States**	**Germany**	**France**
Targets:					
Before the war	**Since the war**				
Government: - Officials - Diplomats - SLTTs	Government: - Increased attacks since war - Espionage - Diplomats - Organizations part of communication infrastructure supply chains for government				
Energy: - Utility companies	Energy: - Increased attacks on OT				

- Companies and organizations managing energy supply	infrastructure - Disruptive attacks - To disrupt communication infrastructure				
Defence: - Military organizations - Defence contractors	Defence: - Attacks on artillery systems				
Financial: - Banks	Financial: - Financial data				
Transportation: - Rail - Air - Ships	Transportation: - No trend observed				
Healthcare: - Hospitals - Pharmaceutical organizations	Healthcare: - Has been targeted less. - Data still valuable.				
Non-governments: - Such as, think tanks and agencies like the OPCW	Non-governments: - Has been victim of on fifth of all attacks.				
Research and education: - Research Institutes - Universities - Schools	Research and education: - No trend observed				

- Target of espionage					
Communication infrastructure	Communication infrastructure: - On satellite communication Organizations providing communication technology				
	Small to medium sized business - Targeted for poor cyber security maturity.				
Total score targets:					
TTPs					
Before the war	**Since the war**				
Custom malware: - Developed by some APT and cyber-crime groups	Custom malware: - No trend observed				
Phishing: - Obtaining information and credentials	Phishing: - Huge increase of use				
DDoS: - Disrupting services and access to important sites	DDoS: - Huge increase of use for disruptive effect				
Trojans:	Trojans: - No trend observed				

- To gain a foothold in the system					
Watering hole (also known as drive-by compromise): - To gain a foothold in the network	Watering hole: - No trend observed				
Ransomware: - To gain money by cyber-crime groups	Ransomware: - Used for destruction				
Botnets: - For executing DDoS attacks or phishing	Botnets: - No trend observed				
Scanning: - For vulnerabilities of software open on the network.	Scanning: - Large tool developed for Russian intelligence agencies				
	Mobile malware: - E.g., used for tracking activists				
Total score TTPs:					
Total score Russian cyber doctrine resilience:					

7. Research question 2: NCSSs compared with Russian cyber threat comparison framework.

With the framework developed in the previous section in this section it will be used to compare the NCSS of Ukraine, the U.S., Germany, and France. First the NCSS of each country will be analysed and assessed where the framework will be filled in.

The results of this analysis are shown in table 3. In short, the Ukraine NCSS mentioned and formulated strategies for all targets in the framework except for NGOs, thus these receive a 2. The financial sector and government get a 2 as well as well as initiatives have been put in place to protect these since the war. A 0 is given to all TTPs as they were not mentioned. However, since the start of the war strategies have been put in place to mitigate DDoS, phishing, ransomware, and custom malware attacks so these will be given a 2.

The U.S. NCSS gets a 1 for defence and healthcare sector and 2 for government, energy, research and education, communication infrastructure and SMEs. It mentioned the TTPs of custom malware, ransomware and botnets earning it a 1, but only formulated strategies to protect against the latter two. Earning them a 2.

The German NCSS mentions all targets in the framework except for transportation. Therefore, a 1 is given to all targets except transportation in the framework. As for strategies, a 2 is given for formulating strategies for government, energy, defence, and SMEs. A 1 is given for mentioning the TTP of malware, DDoS, ransomware, phishing, and botnet attacks. No strategies against TTPs were formulated.

As for France, government, defence, financial, communication infrastructure, research and education and healthcare get a 1 in the framework. A 2 was only

given to government, defence, healthcare, and SMEs for mentioning strategy. The NCSS only mentioned ransomware, phishing, trojans and mobile malware and will therefore receive a 1. The TTP of ransomware, phishing and mobile malware will receive a 2 on the framework for formulating strategies to protect against them.

7.1. Ukraine

The latest NCSS of Ukraine was updated and approved by President Zelensky on the 26th of August 2021, a bit more than 4 months before the start of the invasion. This recent version of the NCSS of Ukraine mentions the main cyber threat of Ukraine is Russia. It states that Russia wages information warfare by using a combination of destructive cyber-attacks on cyberspace and information and psychological operations, which are both actively used in the hybrid war against Ukraine (*УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021*, 2021). Although Ukraine already had a strong strategy (already ranking 25th in the NCSI (*Ukraine*, no date)) the rapid increase in cyber-attacks meant that Ukraine had to implement new strategies which are not mentioned in the NCSS which is also covered in this section.

7.1.1. Targets

7.1.1.1. NCSS

According to the NCSS, Russia is seen posing a threat of cyber terrorism and espionage against Ukrainian information infrastructure and information and communication systems of state bodies (Government per framework). Furthermore, it has also identified the main targets of global cyber terrorism in general, these being nuclear energy facilities, electricity (which falls under energy per framework) and water supply, the spheres of electronic communications (communication infrastructure as per framework), the financial and banking spheres (Financial as per framework), air and railway transport (Transportation as per framework), warehouses of strategic types of

raw materials and chemical and biological facilities. It also identified objects of critical infrastructure as targets but did not give a definition or examples of such objects (*УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021*, 2021). This definition can however be found in chapter 3, article 9.4 of the law of Ukraine "Про критичну інфраструктуру"[1] which definition includes all sectors of the framework except for NGOs and SMEs (*Про критичну інфраструктуру*, 2022).

To protect the government the NCSS mentions legislation which states that the government should foresee costs to protect cyber security (this legislation also applies to enterprises, institutions, and organizations but the NCSS does not specify for which sectors. The NCSS goes further by formulating strategies to protect critical national infrastructure with three priorities: deterrence potential, cyber resilience, and improve interaction (*УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021*, 2021). This universal approach to protecting targets could however form an issue as each sector uses information systems differently.

7.1.1.2. Strategic initiatives of Ukraine to protect targets gathered from interviews

From the grounded theory analysis done on the interviews several themes came up regarding strategic initiatives have put in place to protect common targets in Ukraine from the Russian cyber doctrine. These themes are discussed in this section.

The most common code that came up regarding the theme of defence was "Defence strategy: external cooperation" (see figure 10) with an occurrence of 12. This code reflects the theme of working together with other parties such as nations and private companies to protect the IT systems of Ukraine against

[1] Translation: About critical infrastructure

Russian cyber-attacks. Examples of cooperation that interviewees mentioned was a 37-million-dollar investment by the U.S. into protecting the IT systems of critical infrastructure and networks (‘Proceedings of the 2023 U.S.-Ukraine Cyber Dialogue’, 2023). Furthermore, big corporations such as Microsoft and Google are also helping Ukraine by giving licenses of software and free cloud storage according to interviewee 1 (2023): “Microsoft permits several months of free access and use of cloud, which was very helpful for companies creating a sense of recorded future gives certain intelligence data”. They have also been helping with maintaining internet access and securing governmental services. Although this does highly benefit Ukraine, these corporations also do this to monitor the types of cyber threats posed by Russia and gather intelligence according to interviewee 3 (2023). To support the sharing of threat intelligence with NATO, Ukraine has also taken the strategic initiative to connect to the MSIP open-source threat intelligence sharing platform told interviewee 2 (Interviewee 2, 2023; *SSU and NATO step up cooperation in cybersecurity: threat monitoring systems integrated*, 2022).

Just as common was the code of “Defence strategy: IT army”. As mentioned in the introduction, this army is made from volunteers who want to defend the IT systems of Ukraine and also support the military in offensive operations for gathering intelligence and disrupting the Russian threat. The view on this IT army was mixed among the interviewees with interviewee 2 (2023) calling it a “genius move” and interviewee 3 (2023) “symbolic”. The interviewee went on to say that having many volunteers helps with the reconnaissance part of preparing for a cyber-attack. The attack on a vital Russian vodka distribution portal (Toulas, 2022a) was also mentioned as an example and interviewee 2 (2023) told that such understanding of culture to psychologically effect your opponent has not been seen from Russia on Ukraine.

Second most common code was “Defence strategy: prepared”. This code means that targets in Ukraine were already prepared for the coming cyber-attacks before the war. These targets were mostly large banks, military IT systems and large government-controlled institutions “were able to survive in a good way” according to interviewee 1.

Furthermore, another common code was that of “Defence strategy: backup different location” (see figure 10). This strategic initiative was put forward by Ukraine to move its databases to the cloud. This was especially important to protect the critical data of the financial sector and the government. The reason for this was not only for cyber threats but also the physical damage that could occur from missile attacks as the chance of such an attack in a western NATO country is far lower. Firewalls and Web Application Firewalls (WAF) were also put in place to protect old Operational Equipment of critical infrastructure and services of the government according to Interviewee 4 (2023) and Interviewee 6 (2023). Finally, to be more resilient, Starlink satellite dishes were spread out quickly among organizations and citizens as an alternative when communication infrastructure is targeted, and banks have started to work 24 hours to ensure the payment systems work.

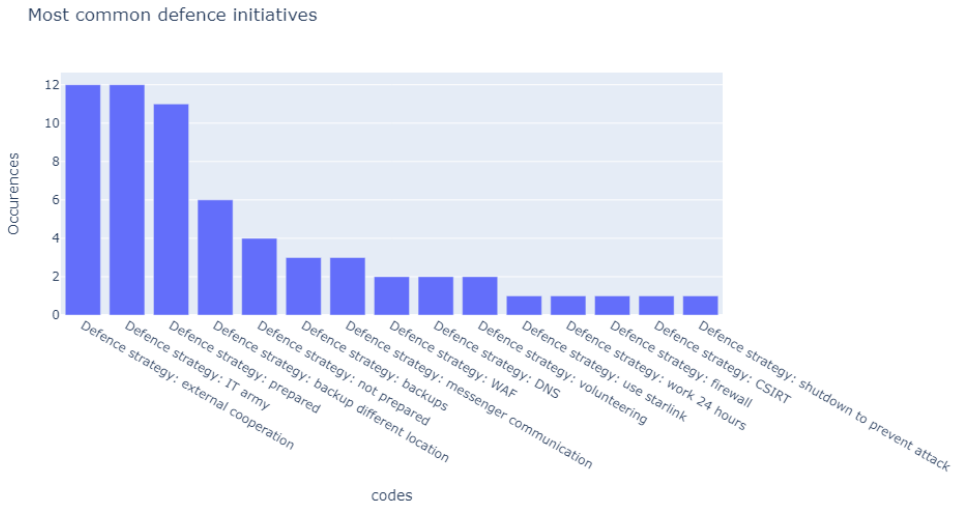

Figure 10: Most common defence initiatives (Interviewee 1, 2023; Interviewee 2, 2023; Interviewee 3, 2023; Interviewee 4, 2023; Interviewee 5, 2023; Interviewee 6, 2023).

7.1.2. TTPs

7.1.2.1. NCSS

The NCSS does not discuss any other cyber-attacks found in the analysis of the Russian cyber doctrine, nor does it articulate any specific cyber threat. Instead, it talks about cyber threats on a higher level, calling them cyber weapons in the militarization of cyberspace used to covertly extract information from Ukraine. It also mentions Russian cyber weapons are made to be destructive, to obtain access control, and to carry out intelligence and intelligence-subversive activities. The NCSS also identifies cybercrime as a motivation for cyber-attacks to occur. It also notes that cyber-attacks are getting more technically advanced. The NCSS does not however formulate goals or tasks to strategically defend against such attacks specifically. As for mobile malware, although it does not mention this being a threat, it does state one of the objectives of the key strategies to ensure mobile devices are secure.

8.1.2.2. Strategic initiatives of Ukraine to protect against TTPs gathered from interviews

The most common code found regarding defence strategies was "Defence strategy: prepared", in this code the there was a theme among interviewees that some smaller organizations implemented security standards that repelled ransomware, DDoS and phishing attacks. The code of "Defence strategy: backups" (see figure 10). According to Interviewee 5 (2023), organizations have started to implement more backups to restore after a ransomware attack. Another code was based on the initiative of setting up a national Domain Name System (DNS). Although this was already written in the most recent NCSS, interviewees mentioned that is initiative, though important to mitigate attacks, has not yet been fully implemented. Finally, with the code "Strategic initiative: MISP" interviewee 2 (2023) mentioned that Ukraine has started to cooperate with NATO and joined the Malware Information Sharing Platform (MISP) (*SSU and NATO step up cooperation in cybersecurity: threat monitoring systems integrated*, 2022). This means that both parties can share new threats more quickly with each other. All in all, it looks like recent strategic initiatives are focussed on defending against DDoS, phishing, and ransomware attacks with a national DNS and MISP cooperation for custom malware attacks.

7.2. United States

On March 1st, 2023, President Joe Biden signed the most recent NCSS of the U.S., a year after the start of the Ukraine war ('National Cyber Security Strategy', 2023). The last NCSS was approved and signed by former President Donald J. Trump on September 2018 ('National Cyber Strategy of the United States of America', 2018). Back then the U.S. ranked 29th on the NCSI index but now ranks 44th at the time of writing (*United States*, no date). It identifies, among others, Russia as a cyber threat which aggressively uses advanced cyber capabilities which go against international and U.S. norms and security and economic prosperity ('National Cyber Security Strategy', 2023).

7.2.1. Targets

The NCSS states that state and local governments partly carry the responsibility of protecting the cyber security of the country. This responsibility is shared with individuals, SMEs, and infrastructure operators. It also mentions energy as a target of criminal syndicates in the form of ransomware attacks on energy pipelines as well as food companies, schools, and hospitals (stated as research and education and healthcare as per framework). It also states that SMEs have limited resources and are thus vulnerable to attacks ('National Cyber Security Strategy', 2023).

The government gets the role of protecting their own systems and make sure those of private organizations part of critical infrastructure protect theirs as well. This falls under "Pillar one | Defend critical infrastructure" ('National Cyber Security Strategy', 2023: 7). The NCSS aims with strategic objectives 2.5 and 3.5 to make the government work with government agencies and private organizations to ensure the cyber security of the country. With strategic objective 4.3 the NCSS aims to improve the security of government networks by making them quantum cryptographically resistant and develop strategies to mitigate future risks to the encryption of these networks and protect the privacy of citizens according to objective 4.5.

The NCSS also states strategies to protect energy infrastructure by integrating the Sector Risk Management Agencies for sharing information with each other and with the private sector as stated in strategic objective 1.3.

As for research and education and healthcare strategic objective 2.5 aims to protect this target by countering the threat of ransomware attacks.

Furthermore, strategic objective 3.1 will indirectly aim to protect personal data hold by the healthcare industry by imposing limits and set standards on the ability of these organizations to collect and handle such information.

As for communication infrastructure, strategic objective 5.5 aims to develop 5G supply chains and networks with domestic and trusted, allied suppliers so its infrastructure is not depended on foreign untrusted suppliers.

Lastly, strategic objective 2.1 talks about securing the target of defence. This will be done by the DoD who will develop a new strategy which will define how the DoD will integrate with the U.S. Cyber Command and other elements of the DoD to protect itself against state, hacktivists, and criminal actors.

Finally, SMEs will be protected in the NCSS by working with cloud providers to prevent espionage, develop secure IoT devices, shift liability of insecure software to vendors and prevent fraud of funds for these business with digital identities (‘National Cyber Security Strategy’, 2023).

7.2.2. TTPs

The NCSS states that the DoD will focus on identifying the development of custom malware. Ransomware is also mentioned in the NCSS as a new trend in attacks to undermine the trust of the public and to disrupt critical services. Furthermore, botnets are also mentioned and the success of the U.S. in taking these down and the threat they pose to IoT devices (‘National Cyber Security Strategy’, 2023).

According to strategic objective 2.5, ransomware will be fought with international cooperation, separating from those countries harbouring cyber criminals that use ransomware, investigating ransomware attacks and cracking down on actors and their infrastructure behind those attacks, improving resilience of target infrastructure, and preventing the exploitation of digital currency in ransomware attacks. The Joint Ransomware Task Force (JRTF) will also work to integrate governmental agencies to stop ransomware operations and help the private sector defend against ransomware. Finally, the U.S. will also crack down on cryptocurrency exchanges on which

cybercriminal rely on. Lastly, government agencies and private sector will work together to identify and trace ransomware payments.

As for botnets, the NCSS identified this as a threat to IoT devices ranging from consumer devices to ICS. It states that such IoT devices have many vulnerabilities and therefore a favourable target for constructing botnets to use for espionage. The Biden administration aims to improve the security of these devices by investing into Research and Development (R&D), risk management and enforce cyber security labels for such devices to create a competitive on the market (‘National Cyber Security Strategy’, 2023).

7.3. Germany

Germany has last updated its NCSS in August of 2021 (*Cyber Security Strategy for Germany*, 2021), before that it was updated in November of 2016 from the 2011 version. Germany has also steadily been on the fifth place in the world when it comes to the NCSI since 2019, making it a mature cyber country (*Germany*, no date). Although it does mention in 5.2.2 that there is a cyber threat from nation-states, it does not mention Russia, nor any other state (*Cyber Security Strategy for Germany*, 2021).

7.3.1. Targets

The NCSS mentions in 5.2.1 and 5.2.2 that the government, private sector, and individual users can be a target to cyber-crime with blackmail and ransomware and nation-state cyber-attacks with cyber espionage and cyber sabotage. It also states in 5.3 that the growing use of digital technology in government administration brings risks to sensitive data from espionage and cyber-attacks on government institutions.

As for energy, section 8.2.10 mentions it to be vulnerable to the fast innovation in IT products which have not yet been tested for basic security.

According to 8.3.13. the Bundeswehr, which task is also defending national cyber security is vulnerable to cyber threats as it is deployed all around the world and uses advanced systems.

Financial systems are also mentioned in the NCSS as a target under the term of critical infrastructure in 5.3. Under this term also falls electricity, telecommunication network and networks of hospitals (energy, communication infrastructure, and healthcare as per framework). What is remarkable is that under critical infrastructure transportation is not mentioned.

The research community is also mentioned in 7.1 as a potential target for cyber-attacks and cybercrime. Non-governments are also mentioned as a target for state sponsored cyber-attacks in 5.2.2.

Lastly, a big focus was also put on businesses in 8.4.2. where it states that these face a constant evolving risk of cyber-attacks (*Cyber Security Strategy for Germany*, 2021).

To protect the government, according to 6.4.1, the Chief Information Officer (CIO) Council and its working group on information security are made responsible for the IT security management of the Federal government and implementing information security guidelines into the public administration systems. Furthermore, according to 6.4.2, the Federal Office for Information Security (BSI) is also responsible for keeping the networks and IT safe and secure. The role of the BSI is also important in the digital transition of the government by offering testing, standardization, certification, authorization, and general advice to the government. Moreover, the Federal Office for the Protection of the Constitution (BfV) is responsible for internal security and evaluating the threat of cyber-attacks from state actors and terrorist organizations. The federal states are also responsible for preventing threats in their own cyberspace though no strategy is given in how this is achieved. The NCSS also mentions the importance of actors, both federal and private, in maintaining the security of the federal IT infrastructure. As the NCSS describes in point 7.1 that cyber-attacks and cybercrime can affect the government, private sector, research community and the public it strategizes

that these actors should work together to not only protect themselves but also each other.

According to 8.2.5, targeted measures will be taken to strengthen the security of systems used in sectors and supply chains of the energy sector. The NCSS also states that the energy sector can become vulnerable to the fast introduction of new untested IT products. The NCSS therefore states that such products should be tested, approved, and certified (see 8.2.10).

According to 8.3.13, the Military Counterintelligence Service (MAD) should review and adjust structures and capabilities to mitigate risks in the cyberspace of the defence sector. Furthermore, IT systems, including command systems and weapon/operating systems, will be identified, and bolstered for increased security and resilience. Also, these systems will be replaced by systems from trustworthy contractors.

Under 8.2.13 strategies for securing the telecommunication of are formulated with the main aim to continuously monitor and secure the networks, in particular 5G and 6G networks. The German government will also promote standards for securing these telecommunication networks.

As for SMEs, focus will be put on protecting those, particularly in the craft sector, with much support to eventually protect themselves (*Cyber Security Strategy for Germany*, 2021).

Strategies for protecting the financial sector, research community and non-government institutions, previously mentioned as targets were not formulated in the NCSS. Financial and transportation sectors do recur in the definition of critical infrastructure in the Law on the Federal Office for Information Security (BSI Law – BSIG)[2] but not in the definition of critical infrastructures in the NCSS (*BSIG - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, 2009; *Cyber Security Strategy for Germany*, 2021).

[2] In German: “Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)”

7.3.2. TTPs

The NCSS mentions custom malware as one of the techniques that has started to be more developed by actors that are extremely specialized. 8.2 of the NCSS mentions that new types of malware are also being discovered at an increasing rate.

Not only did the NCSS mention DDoS attacks it also explained how they work with botnets and why they are used. 5.2.1. explains that DDoS are used to overload IT systems with network traffic and to blackmail victims. It has also provided a definition of the attack in the glossary.

Interestingly, the NCSS mentions phishing as a crime in the threat section (5.2) but does not focus its cyber security strategy on such acts. Instead, it states that it focusses on those cyber-attacks "(…) that directly and substantially compromise the availability, integrity and confidentiality of IT systems." (*Cyber Security Strategy for Germany*, 2021: 15).

Furthermore, ransomware is also mentioned elaborately in the cyber-crime section (5.2.1). It states that ransomware is one of the biggest threats and are mostly non-targeted, meaning that criminals attack any system regardless of which individual or organization if it has the unprotected vulnerability. It goes further on to explain that it has developed to the point where it can be destructive as the victim machines are part of a global network and can thus takeout infrastructures and divisions of big organizations which tend as a result to be targeted more often.

As for botnet attacks, it states that the malware for creating botnets has become more advanced as well such that they, besides DDoS attacks, can also be used to obtain personal information from the machine of the victim which has become a typical technique of obtaining access data (*Cyber Security Strategy for Germany*, 2021).

Strategies to defend against these TTPs are not formulated (*Cyber Security Strategy for Germany*, 2021).

7.4. France

The last time the prime minister of France approved the NCSS of France was in 2015 (‘French National Digital Security Strategy’, 2015). Since then, president Macron has announced a NCSS on the 18th of February 2021 (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021), though this strategy does not seem to be a full replacement of the NCSS from 2015 as the document is not registered in the European Union Agency for Cyber Security (ENISA) under NCSS of France (*National Cyber Security Strategies - Interactive Map: France*, no date) and the website of the NCSI (*France*, no date). Nonetheless, this latest document will be analysed as an update to the NCSS of 2015. Regarding the NCSI, France has dropped in ranking from fourth place in the world in 2019 to 15th in 2023 (*France*, no date). Both the NCSS of 2015 and the updated version do not mention Russia as a threat.

7.4.1. Targets

The 2015 NCSS mentions in the introduction that local authorities were subject to website defacements in a cyber-attack in January 2015, thus stating the government can be a target. It also mentions under strategic objective number one, that attackers could target the state and stay within the information system to obtain confidential information. (‘French National Digital Security Strategy’, 2015). As for the updated strategy, it does mention that cyber espionage is a big risk for government agencies and refers to the SolarWinds cyber-attack. It also states that cyber-crime is a big threat for public bodies and local authorities and that these are also vulnerable to them (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

The NCSS of 2015 also mentions military (defence) and economic (finance) information as a target “(…) when an attacker targets the State, operators of vital importance or strategic businesses” (‘French National Digital Security Strategy’, 2015: 14). The updated strategy does not mention military

and financial sector as a target (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

Although the 2015 NCSS does not mention the healthcare sector as a target for cyber-attacks, the updated strategy mentions that the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) was seeing one attempted cyber-attack per week on hospitals at the time of writing. The strategy also includes two case studies of cyber-attacks targeting French hospitals (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

The 2015 NCSS also mentions communication as a target which are not designed and developed in France. It goes on by saying that sections of this infrastructure will become inaccessible in an international cyber crisis (‘French National Digital Security Strategy’, 2015). The updated NCSS only mentions telecommunications in a graph depicting the share of total ransomware attacks experienced. In this graph telecommunications received 9% of all attacks and education 6% (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

As for SMEs, the 2015 NCSS mentions protecting their security is vital (‘French National Digital Security Strategy’, 2015). The updated version however, does mention SMEs are targeted and ensuring the cyber security of small businesses is essential and one of the key objectives (‘French National Digital Security Strategy’, 2015).

Strategies to protect the security of the government can be found in both versions of the NCSS. In the 2015 version of the NCSS the government will be secured by providing a State Information Systems Security Policy (PSSIE) that consists of a new communication network between ministries and secure mobile terminals to keep the information of the government more sovereign. It also states under the first strategic objective that the ANSSI will inform territorial authorities of cyber threats. (‘French National Digital Security Strategy’, 2015). The updated version of the NCSS formulates a strategy

where government departments will be assisted in case they are hit with a cyber-attack. This is done via a government website called cybermalveillance.gouv.fr which creates awareness about cyber threats and assists governments, businesses and individuals with recovering from cyber-attacks. Moreover, 176 million euros will be invested in supporting the adoption of cyber solutions for local authorities and the state. Another 136 million will be invested in a recovery plan for all, but not limited to, territorial local authorities and public bodies. A guide will also be made by ANSSI, the Direction Générale des Entreprises (DGE) and the cybermalveillance.gouv.fr on how to protect themselves against cyber risks with a limited budget. Also, accredited ExpertCyber professionals will help local authorities in securing their information systems. Finally, the Gendarmerie Nationale and the operational sections for combating cyber threats (SOLC) will support, monitor, and provide advice for security systems of local authorities (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

The military (defence) will also be provided with the PSSIE according to the 2015 NCSS (‘French National Digital Security Strategy’, 2015) and the healthcare sector will also benefit from the 136-million-euro investment in the recovery plan according to the updated NCSS (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

To protect SMEs, although the 2015 strategy does not state a strategy to protect SMEs, the updated strategy did state producing a guide that gives SMEs advice and solutions to protect their cyber security (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

7.4.2. TTPs

The TTP of custom malware is only mentioned once in the 2015 version of the NCSS. However, the context in which it is mentioned could suggest it is ransomware. It states that businesses in France are often hit with malware that makes their files inaccessible until they pay a ransom of which the transaction is difficult to trace (‘French National Digital Security Strategy’, 2015).

As for ransomware, the 2015 NCSS does not mention it directly but states in the second objective that cyber-attacks are often done for financial gain, this would suggest the use of ransomware (‘French National Digital Security Strategy’, 2015). The updated strategy states that the number of ransomware attacks observed by ANSSI has increased by four times between 2019 and 2020. Moreover, in 2020, 20% of victims who reported a ransomware attack to ANSSI were local authorities. Healthcare establishments are accounted for 11% of report ransomware attacks. Finally, the updates strategy also mentions ransomware in the case studies of the Dax-Côte d'Argent and Villefranche-sur-Saône Hospital where RYUK ransomware compromised their data (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

Phishing is also mentioned in the updated NCSS but only as a topic in the awareness kit provided by the cybermalveillance.gouv.fr. Phishing was not mentioned in the 2015 version of the NCSS (‘French National Digital Security Strategy’, 2015).

Another difference is that the updated strategy did mention trojans. The context wherein it was mentioned was in how France has acted against cybercrime. It has, together with a coalition of France, U.S., Netherlands, United Kingdom, Lithuania, Canada, and Ukraine (coordinated by Europol) dismantled the spreading of the Emotet Trojan via infected emails (‘Cybersécurité, faire face à la menace: la stratégie française’, 2021).

Regarding strategies to defend against ransomware, the 2015 strategy aims to universalise the principles of the Budapest Convention on Cybercrime and cooperate with other European states by sharing information (‘French National Digital Security Strategy’, 2015). The updated strategy states that the website cybermalveillance.gouv.fr will provide a free awareness kit that covers topics of including, but not limited to, ransomware and phishing. It also states that the Gendarmerie Nationale and the Centre de lutte contre les criminalités

numériques (C3N) will work on fighting ransomware attacks but does not elaborate how this will practically be achieved.

Although the updated NCSS did not mention mobile malware as a threat, the 2015 strategy stated that an initiative of the previous NCSS of 2013 proposed for better mobile security ('French National Digital Security Strategy', 2015).

7.5. Overview of comparison of the case study countries

For an overview of the comparison please see the filled in framework (table 3) according to the analysis of each country. The following are points that stood out from this comparison:

- First, when considering the strategic initiatives Ukraine has taken to protect itself, its total score Russian cyber doctrine becomes the highest with at least 10 points. When this is not taken into the calculation it falls with 8 points, bringing it closer to the score of the other NCSSs. This is mostly because no TTPs were mentioned in the NCSS which could suggest it does not have good intelligence on this matter. This would also explain why it chose to connect to the MISP as one of the strategic initiatives. The rest of the score would come from mentioning targets and formulating strategies to protect them but this was only given because these fall into the definition of critical national infrastructure. There is still a lack of specific strategies to protect each target in the NCSS.

- Second, only Germany mentioned non-governmental organisations as a potential target of cyber-attacks but failed to provide a strategy to protect it. A potential reason for this is that countries do not see this target as a vital part of the functioning of the state. Other targets such as government, energy, finance, and businesses were mentioned more

and protected more. One would also argue that transportation is also a vital part, but it was also only mentioned indirectly by Ukraine in their NCSS.

- Thirdly, both Germany and the U.S. scored low in the section of TTPs. This is also peculiar as especially the U.S. is well known for its excellent intelligence and Germany being a member of NATO should have at least the score of France as it is also a member.

Table 3: framework filled in according to the analysis of each country (0 = not mentioned, 1 = mentioned, 2 = mentioned and strategy to defend (against) it formulated). * = this score was given because Ukraine has improved its cyber security strategy on this part according to interviews.

		Ukraine	**United States**	**Germany**	**France**
Targets:					
Before the war	**Since the war**				
Government: - Officials - Diplomats - SLTTs	Government: - Increased attacks since war - Espionage - Diplomats - Organizations part of communication infrastructure supply chains for government	(2)-2*	2	2	2
Energy: - Utility companies - Companies and organizatio	Energy: - Increased attacks on OT infrastructure	2	2	2	0

ns managing energy supply	- Disruptive attacks - To disrupt communication infrastructure				
Defence: - Military organizations - Defence contractors	Defence: - Attacks on artillery systems	2	1	2	2
Financial: - Banks	Financial: - Financial data	(2)-2*	0	1	1
Transportation: - Rail - Air - Ships	Transportation: - No trend observed	2	0	0	0
Healthcare: - Hospitals - Pharmaceutical organizations	Healthcare: - Has been targeted less. - Data still valuable.	2	1	1	2
Non-governments: - Such as, think tanks and agencies like the OPCW	Non-governments: - Has been victim of on fifth of all attacks.	0	0	1	0
Research and education: - Research Institutes - Universities - Schools - Target of espionage	Research and education: - No trend observed	2	2	1	1

Communication infrastructure	Communication infrastructure: - On satellite communication Organizations providing communication technology	2	2	1	1
	Small to medium sized business - Targeted for poor cyber security maturity.	2	2	2	2
Total score targets:		**(18)-18***	**12**	**13**	**11**
TTPs					
Before the war	**Since the war**				
Custom malware: - Developed by some APT and cyber-crime groups	Custom malware: - No trend observed	(0)-2*	1	1	0
Phishing: - Obtaining information and credentials	Phishing: - Huge increase of use	(0)-2*	0	1	2
DDoS: - Disrupting services and access to important sites	DDoS: - Huge increase of use for disruptive effect	(0)-2*	0	1	0
Trojans: - To gain a foothold in the system	Trojans: - No trend observed	0	0	0	1

Watering hole (also known as drive-by compromise): - To gain a foothold in the network	Watering hole: - No trend observed	0	0	0	0
Ransomware: - To gain money by cyber-crime groups	Ransomware: - Used for destruction	(0)-2*	2	1	2
Botnets: - For executing DDoS attacks or phishing	Botnets: - No trend observed	0	2	1	0
Scanning: - For vulnerabilities of software open on the network.	Scanning: - Large tool developed for Russian intelligence agencies	0	0	0	0
	Mobile malware: - E.g., used for tracking activists	2	0	0	2
Total score TTPs:		**(2)-10***	**5**	**5**	**7**
Total score Russian cyber doctrine resilience:		**(20)-28***	**17**	**18**	**18**

8. Research question 3: Recommendations

From the gaps found in the comparison among NCSS and the grounded theory analysis of interviews taken with cyber security experts and practitioners

helping Ukraine recommendations can be formed both for states currently drafting a new NCSS and organizations wanting to know where to improve their cyber strategy.

8.1. Recommendations from the comparison of NCSS

1. The government of Ukraine should improve their perceived threat section by adding common TTPs of Russia into the NCSS. It should also add strategies to protect its targets from these TTPs. Intelligence gathered from SSSCIP, MISP and reports from Microsoft and Google can be used to achieve this.
2. Germany and the U.S. should state more common targets and TTPs of Russia. It can also use information from the MISP network as a NATO member and perform more threat intelligence on their own systems to achieve this.
3. The TTP of DDoS, scanning, watering hole and phishing is not mentioned in NCSS as much as expected. These are one of the main TTPs of Russia. Watering hole should be mentioned more often as it has been used often by Russia in the past although there is no clear trend of this being used more since the war. Also scanning is used often in the reconnaissance part of the cyber kill chain, not just by Russia.
4. The NCSS of every country should be clearer about the use of the concept ‘critical national infrastructure’. It is not often defined in the NCSS, and it should be clear whish sectors and organizations are part of this. Even better would be to formulate strategies specific to each sector that full under the definition as each sector might need a tailored focus and approach to cyber security.

8.2. Recommendations from interviews with cyber security experts

1. The most common recommendation given by experts was to implement a universal approach to cyber security under the code ‘Recommendations: universal defence’. Experts were asked whether it is better to focus on most common targets and TTPs or have a more universal approach. The overall majority said it was better to focus on a universal defence as organizations can expect “attacks from multiple levels” according to interviewee 1 (2023). He goes on that especially during war something that was not a risk in the past could be a risk now.
2. The second most common recommendation given is that countries need to build national resilience by building redundancies in organizations. This could mean that there is a backup system that can be used in case the main system is made inoperable. Interviewee 3 (2023) said there needs to be national mind shift that in a war you need to have redundancies as the stake are high.
3. Another recommendation given by interviewee 3 (2023) is to prohibit the use of applications from foreign countries that have an offensive cyber program against your state. Such applications could send personal data to servers in their own jurisdictions which allows them to do anything with them. The interviewee stated that such advise would be radical a few years ago but is becoming more serious. An example of this is the banning of the use TikTok by government officials in the U.S. and the Netherlands.
4. Lastly, interviewee 3 (2023) and interviewee 2 (2023) also recommended to share cyber threat intelligence to achieve collective resilience. Fortunately, such initiative was already taken by Ukraine by connecting to the NATO MISP network.

9. Conclusion

This dissertation identified a gap in academic research where there is no recent view of the cyber doctrine of Russia since the war and where the recent NCSS of Ukraine has not been compared against any country or analysed for resilience against the Russian cyber doctrine. The reason to compare the NCSS of the US, Germany, and France with the NCSS of Ukraine is that these countries have all experienced an increase in cyber-attacks since 2014. To fill in this gap it set out to answer the research question: what can states and organisations learn from the National Cyber Security Strategy of Ukraine, compared to those of the United States, Germany and France on the Russian cyber doctrine since 2014? Three objectives were set out to answer this question.

9.1. Conclusion research question 1

The first research question was: what are the most common targets and TTPs used of the Russian cyber doctrine since 2014? To answer it, first the Russian cyber doctrine was analysed to distil the most common targets and TTPs. The results of this analysis are formed into a framework where the NCSS of the case study countries can be compared against each other. In total 28 Russian cyber threat groups and companies were analysed. These ranged from APT groups linked to specific ministries and centres of the Russian government, hacktivist groups, cyber-crime groups, espionage groups, and organizations supporting the Russian state and its APT groups with offensive cyber operations. The results of this analysis showed that the most common targets the Russian cyber doctrine attacks are sectors of government, energy, defence, financial, transportation, healthcare, NGOs, research and education, communication infrastructure and SMEs. To obtain recent insight on attacks since the war, 6 interviews were held with cyber experts on the Ukraine cyber war. This showed that targets of the government, energy, research and education and SMEs were targeted more often, and healthcare targeted less.

As for TTPs, custom malware, phishing, DDoS, trojans, watering hole, ransomware, botnets, scanning, and mobile malware were used. Since the war there has been increase of use of phishing, DDoS, ransomware and wiper malware and mobile malware attacks. Advanced attacks were less common as Russian APT groups experience lack in skilled resources as such people are hard to find as they have either left the country or are not in support of the war. Instead, there has been an increase of hacktivists who have started to perform more advanced attacks in support of the Russian state. These results have been put into a framework where a score between 0 and 2 is given per target or TTP for each country based on whether their NCSS mentions the target or TTP or has formulated a strategy to protect the target or against the TTP (see table 2).

9.2. Conclusion research question 2

The second research question was: which NCSS of Ukraine, U.S., Germany, and France scores the highest on the Russian cyber doctrine framework? To answer it each NCSS was first analysed based on the framework and a score was given based on this analysis. The NCSS of Ukraine identifies Russia as an aggressive actor that uses destructive means and psychological manipulation to assert dominance. The document did not state specific targets directly but mentioned them indirectly with the term critical national infrastructure. Some strategies to protect these targets consisted of covert inspections and developing open-source software. From interviews with cyber security experts, other strategic initiatives came to light implemented since the war such as the IT army and connecting to the MISP NATO network. An interesting observation was that no TTPs were mentioned in the NCSS though recent initiatives implemented protect against ransomware and wiper malware by backing up data and implementing security standards to further protect against phishing and DDoS. As for the US, it has the most recent updated NCSS and mentioned Russia as an aggressive cyber actor. The U.S. failed

however to mention financial, transportation, and NGOs as targets. It also only mentioned custom malware, ransomware, and botnets with only providing strategies for the latter two. Germany mentioned all targets except for transportation and its main strategic goal is to improve cyber security by making it a shared task among all sectors. Although it mentioned half of the TTPs it failed to provide any strategies. Finally, France has the oldest strategy. Although it published an update, it is not a full replacement. Nevertheless, the two versions were taken as one which resulted in mentioning every target except energy, transportation, and NGOs. Although the 2015 strategy mentions mobile malware, the updated version does mention trojans, phishing and ransomware with strategies to protect against them for the latter two. All in all, considering the recent strategic initiatives Ukraine took since the war, it scored the highest in the framework with 28 points. If it is not considered it still scores the highest followed by a tie between France and Germany at 18 points and the U.S. at 17 points.

9.3. Conclusion research question 3

The third research question was: what recommendations can be given to governments and organizations based on the resiliency of their NCSS compared to other NCSSs? Out of the comparison of the second research question, three interesting observations were made. First, Ukraine scored the lowest on TTPs in the framework compared to other countries which could mean it lacks intelligence on this matter. This could also explain the strategic imitative to connect to the NATO MISP network to share cyber threat intelligence more quickly. Second, the only country to mention NGOs was Germany which could mean countries do not consider this sector a vital part of the state which is worthy to protect. Other sectors such as government, SMEs and defence were considered in all NCSS. Lastly, the U.S. and Germany scored the second lowest on TTPs which is surprising as both these countries are known to have good intelligence agencies.

The third objective was to give recommendations. Four recommendations were made based on the differences found in the comparison of the NCSS and four recommendations based on interviews with cyber experts. Recommendations based on the comparison were first that Ukraine should mention common TTPs of Russia in their NCSS. Second, Germany and the U.S. should state more common targets and TTPs of Russia. Third, the TTPs of DDoS, scanning, watering hole and phishing is not mentioned in NCSS as much as expected and Last but not least, the NCSS of every country should define the concept 'critical national infrastructure' or not use it at all. Recommendations based on interviews were first, to focus on a holistic approach to cyber defence and not on specific TTPs. Second, build redundancies so organizations can keep on operating. Third, prohibit the use of application developed by cyber adversarial states and lastly, share threat intelligence to achieve collective intelligence.

9.4. Answer to the main research question

By having answered these three research questions, the answer to the main research question is as follows: states can learn from this research that Russia is an aggressive cyber actor who mainly targets sectors of critical national infrastructure often with low cost TTPs such as DDoS, phishing, and ransomware attacks. Since the start of the war, they have experienced a lack of resources and have thus not shown more advanced attacks. By comparing the NCSS of Ukraine, US, Germany, and France with a framework based on the Russian cyber doctrine recommendations can be made for future NCSS of these and other states. It is important for states to learn that they should mention common TTPs of Russia but also implement a holistic approach to cyber security.

9.5. Implications and future research

The framework developed in this research can be used in future research to assess and compare other NCSSs. However, as the Ukraine war is continuing at the moment of writing, new TTPs could be developed that could strengthen the Russian cyber doctrine and the framework developed in this research needs to be updated. It is therefore recommended to update the framework before using it to compare the NCSS of states. By maintaining this framework, using it to analyse and compare the NCSS of states and implementing recommendations for improvement, states and organizations can become more resilient to the Russian cyber doctrine. To improve this framework, future research should aim to assess whether (improved) cyber strategies have been implemented as a big difference can be found in the total score of Ukraine in this research due to strategies implemented that have not been stated in the NCSS.

As Russia is not the only foreign cyber power with an aggressive cyber doctrine against the west, the methodology used in this research could also be used to develop frameworks encompassing the cyber doctrine of China and North Korea for example. As cyber-attacks are used more as tensions rise internationally, a framework to compare cyber strategies and improve them becomes increasingly more important.

10. Bibliography

2007 cyber attacks on Estonia (no date). NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf (Accessed: 13 July 2023).

2016 Ukraine Electric Power Attack (2023) *MITRE*. Available at: https://attack.mitre.org/campaigns/C0025/ (Accessed: 13 July 2023).

'A year of Russian hybrid warfare in Ukraine' (2023) *Microsoft Threat Intelligence*, 15 March. Available at: https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (Accessed: 13 July 2023).

Ain't No Actor Trustworthy Enough: The importance of validating sources (2021) *KELA*. Available at: https://www.kelacyber.com/aint-no-actor-trustworthy-enough-the-importance-of-validating-sources/ (Accessed: 13 July 2023).

Akimenko, V. and Giles, K. (2020) 'Russia's Cyber and Information Warfare', *Asia Policy*, 27(2), pp. 67–75. Available at: https://doi.org/10.1353/asp.2020.0014.

ALLANITE (2022) *MITRE*. Available at: https://attack.mitre.org/groups/G1000/ (Accessed: 13 July 2023).

Allanite (no date) *Council on Foreign Relations*. Available at: https://www.cfr.org/cyber-operations/allanite (Accessed: 13 July 2023).

ALLANITE Threat Group (2020) *Dragos*. Available at: https://www.dragos.com/threat/allanite/ (Accessed: 13 July 2023).

Antoniadis, N. *et al.* (2023) *The 'Vulkan Files': A Look Inside Putin's Secret Plans for Cyber-Warfare*, *Spiegel International*. Available at: https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236 (Accessed: 13 July 2023).

APT28 (2021) *MITRE*. Available at: https://attack.mitre.org/versions/v10/groups/G0007/ (Accessed: 11 July 2023).

APT29 (2023) *MITRE*. Available at: https://attack.mitre.org/groups/G0016/ (Accessed: 11 July 2023).

Bogdan, R. and Biklen, S.K. (1998) *Qualitative research for education*. 3rd ed. Boston: Allyn and Bacon. Chapter 1, pp. 1-48.

Brewster, T. (2014) 'Sophisticated "Turla" hackers spying on European governments, say researchers', *The Guardian*, 7 August. Available at: https://www.theguardian.com/technology/2014/aug/07/turla-hackers-spying-governments-researcher-kaspersky-symantec (Accessed: 12 July 2023).

BSIG - Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (2009). Available at: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (Accessed: 23 July 2023).

Burgess, M. (2022) 'Russian "Hacktivists" Are Causing Trouble Far Beyond Ukraine', *Wired UK*, 11 July. Available at: https://www.wired.co.uk/article/russia-hacking-xaknet-killnet (Accessed: 13

July 2023).

Burt, J. (2023) *Russia's APT28 targets Ukraine with bogus Windows updates*, *The Register*. Available at: https://www.theregister.com/2023/05/02/russia_apt28_ukraine_phishing/ (Accessed: 12 July 2023).

Command and Scripting Interpreter: PowerShell (2023) *MITRE*. Available at: https://attack.mitre.org/techniques/T1059/001/ (Accessed: 13 July 2023).

Connel, M. and Vogler, S. (2016) *Russia's Approach to Cyber Warfare*. Available at: https://apps.dtic.mil/sti/citations/AD1019062 (Accessed: 18 June 2023).

Corera, G. (2016) 'How France's TV5 was almost destroyed by "Russian hackers"', *BBC News*, 10 October. Available at: https://www.bbc.com/news/technology-37590375 (Accessed: 11 July 2023).

Creswell, J.W. (2007) *Qualitative inquiry & research design: choosing among five approaches*. 2nd ed. Thousand Oaks: Sage Publications.

Culafi, A. (2022) *Conti ransomware gang backs Russia, threatens U.S.*, *TechTarget*. Available at: https://www.techtarget.com/searchsecurity/news/252513982/Conti-ransomware-gang-backs-Russia-threatens-US (Accessed: 13 July 2023).

Cyber Security Strategy for Germany (2021) *Federal Ministry of the Interior and Community*. Available at: https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-artikel.html;jsessionid=6A290294A24D616B1DAFFAE524CA419B.1_cid37

3?nn=16825398 (Accessed: 13 July 2023).

‘Cybersécurité, faire face à la menace: la stratégie française’ [‘Cybersecurity, facing the threat: the French strategy’] (2021). Agence nationale de la sécurité des systèmes d’information. Available at: https://www.ssi.gouv.fr/uploads/2021/02/anssi-dossier_presse-strategie_nationale_cyber.pdf (Accessed: 14 July 2023).

Dahan, A. and Pasha, S. (2023) ‘KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks’, *Microsoft Security Blog*, 17 March. Available at: https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/ (Accessed: 13 July 2023).

Defending Ukraine: Early Lessons from the Cyber War (2022). Microsoft. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK (Accessed: 13 July 2023).

Demoboski, M., Fitzpatrick, J. and Rydzynski, P. (2021) ‘Russian cyber attack campaigns and actors’, *Ironnet*, 25 October. Available at: https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors (Accessed: 11 July 2023).

DoS:Win32/FoxBlade.A!dha threat description (2022) *Microsoft Security Intelligence*. Available at: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=DoS:Win32/FoxBlade.A!dha&ThreatID=2147813512 (Accessed: 13 July 2023).

Downs, G.W. and Rocke, D.M. (1987) ‘Tacit Bargaining and Arms Control’, *World Politics*, 39(3), pp. 297–325. Available at: https://doi.org/10.2307/2010222.

Dragonfly (2021) *MITRE*. Available at: https://attack.mitre.org/versions/v10/groups/G0035/ (Accessed: 11 July 2023).

Dragonfly 2.0 (2021) *MITRE*. Available at: https://attack.mitre.org/versions/v10/groups/G0074/ (Accessed: 11 July 2023).

‘Dragonfly: Western energy sector targeted by sophisticated attack group’ (2017) *Symantec*, 20 October. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks (Accessed: 11 July 2023).

DYMALLOY Threat Group (2020) *Dragos*. Available at: https://www.dragos.com/threat/dymalloy/ (Accessed: 11 July 2023).

Ember Bear (2023) *MITRE*. Available at: https://attack.mitre.org/groups/G1003/ (Accessed: 13 July 2023).

EMBER BEAR: Threat Actor Profile (2022) *crowdstrike.com*. Available at: https://www.crowdstrike.com/blog/who-is-ember-bear/ (Accessed: 13 July 2023).

Emotet (2020) *MITRE*. Available at: https://attack.mitre.org/versions/v10/software/S0367/ (Accessed: 13 July 2023).

‘FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks’ (2021). FBI. Available at:

https://www.ic3.gov/Media/News/2021/210521.pdf (Accessed: 13 July 2023).

Fidel, R. (1984) 'The Case Study Method: A Case Study', *Library and Information Science Research, An International Journal*, 6(3), pp. 273–88.

'Fog of war: how the Ukraine conflict transformed the cyber threat landscape' (2023) *Google*, 16 February. Available at: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/ (Accessed: 12 July 2023).

France (no date) *National Cyber Security Index*. Available at: https://ncsi.ega.ee/country/fr/ (Accessed: 14 July 2023).

'French National Digital Security Strategy' (2015). Premiere Ministre. Available at: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf (Accessed: 11 July 2023).

Gamaredon Group (2017) *MITRE*. Available at: https://attack.mitre.org/groups/G0047/ (Accessed: 11 July 2023).

Germany (no date) *National Cyber Security Index*. Available at: https://ncsi.ega.ee/country/de/ (Accessed: 13 July 2023).

Giles, K. (2011) '"Information Troops" - A Russian Cyber Command?', in *2011 3rd International Conference on Cyber Conflict*. *2011 3rd International Conference on Cyber Conflict*, pp. 1–16.

Gillum, J. (2022) 'Mandiant Finds Possible Link Between Kremlin, Pro-Russian "Hacktivists"', *Bloomberg.com*, 29 June. Available at:

https://www.bloomberg.com/news/articles/2022-06-29/mandiant-finds-possible-link-between-kremlin-pro-russian-hacktivists (Accessed: 13 July 2023).

Greenberg, A. (2018) 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Accessed: 12 July 2023).

Griffin, A. (2017) *Chernobyl's radiation monitoring system has been hit by the worldwide cyber attack*, *The Independent*. Available at: https://www.independent.co.uk/tech/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html (Accessed: 12 July 2023).

Groups (no date) *MITRE*. Available at: https://attack.mitre.org/groups/ (Accessed: 13 July 2023).

Guide for Conducting Risk Assessments (2012). NIST Special Publication (SP) 800-30 Rev. 1. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-30r1.

Harding, L., Ganguly, M. and Sabbagh, D. (2023) '"Vulkan files" leak reveals Putin's global and domestic cyberwarfare tactics', *The Guardian*, 30 March. Available at: https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics (Accessed: 13 July 2023).

'Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor' (2022)

Mandiant, 10 May. Available at: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor (Accessed: 11 July 2023).

Industroyer (2022) *MITRE*. Available at: https://attack.mitre.org/software/S0604/ (Accessed: 12 July 2023).

InvisiMole (2021) *MITRE*. Available at: https://attack.mitre.org/software/S0260/ (Accessed: 11 July 2023).

Interviewee 1 (2023) 'Interview regarding experience of the Russian cyber doctrine'. Interview by Frans Sebastiaan Berting [Microsoft Teams], 17 May.

Interviewee 2 (2023) 'Interview regarding experience of the Russian cyber doctrine'. Interview by Frans Sebastiaan Berting [Zoom], 17 May.

Interviewee 3 (2023) 'Interview regarding experience of the Russian cyber doctrine'. Interview by Frans Sebastiaan Berting [Zoom], 26 May.

Interviewee 4 (2023) 'Interview regarding experience of the Russian cyber doctrine'. Interview by Frans Sebastiaan Berting [Zoom], 2 June.

Interviewee 5 (2023) 'Interview regarding experience of the Russian cyber doctrine'. Interview by Frans Sebastiaan Berting [Zoom], 8 June.

Interviewee 6 (2023) 'Interview regarding experience of the Russian cyber doctrine'. Interview by Frans Sebastiaan Berting [Zoom], 9 June.

Jensen, B., Valeriano, B. and Maness, R. (2020) ‘Fancy bears and digital

trolls: Cyber strategy with a Russian twist', in, pp. 58–80. Available at: https://doi.org/10.4324/9781003009207-4.

Kari, M.J. and Pynnöniemi, K. (2023) 'Theory of strategic culture: An analytical framework for Russian cyber threat perception', *Journal of Strategic Studies*, 46(1), pp. 56–84. Available at: https://doi.org/10.1080/01402390.2019.1663411.

KillNet Group (no date) *Blackberry*. Available at: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/killnet (Accessed: 13 July 2023).

Knowlton, B. (2010) 'Military Computer Attack Confirmed', *The New York Times*, 25 August. Available at: https://www.nytimes.com/2010/08/26/technology/26cyber.html (Accessed: 11 July 2023).

Kovacs, E. (2018) *'Allanite' Group Targets ICS Networks at Electric Utilities in US, UK*, *SecurityWeek*. Available at: https://www.securityweek.com/allanite-group-targets-ics-networks-electric-utilities-us-uk/ (Accessed: 13 July 2023).

Leonard, B. (2022) *Continued cyber activity in Eastern Europe observed by TAG*, *Google*. Available at: https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/ (Accessed: 13 July 2023).

Lilly, B. and Cheravitch, J. (2020) 'The Past, Present, and Future of Russia's Cyber Strategy and Forces', in. *2020 12th International Conference on Cyber Conflict (CyCon)*, pp. 129–155. Available at: https://doi.org/DOI:

10.23919/CyCon49761.2020.9131723.

Lithuania Says Hit by Cyberattack, Russia 'Probably' to Blame (2022) *SecurityWeek*. Available at: https://www.securityweek.com/lithuania-says-hit-cyberattack-russia-probably-blame/ (Accessed: 13 July 2023).

Luiijf, E. *et al.* (2013) *Ten National Cyber Security Strategies: a Comparison: Critical Information Infrastructure Security*, p. 17. Available at: https://doi.org/10.1007/978-3-642-41476-3_1.

Luiijf, E., Besseling, K. and Graaf, P. (2013) 'Nineteen National Cyber Security Strategies', *International Journal of Critical Infrastructure Protection*, 9, pp. 3–31. Available at: https://doi.org/10.1504/IJCIS.2013.051608.

Luiijf, E. and Healey, J. (2012) 'Organisational Structures & Considerations', in, pp. 108–145.

Lyngaas, S. (2022) *Russian hackers allegedly target Ukraine's biggest private energy firm*, *CNN*. Available at: https://www.cnn.com/2022/07/01/politics/russia-ukraine-dtek-hack/index.html (Accessed: 13 July 2023).

Medvedev, S.A. (2015) 'Offense-Defense Theory Analysis of Russian Cyber Capability'. Available at: https://apps.dtic.mil/sti/citations/ADA620663 (Accessed: 13 July 2023).

Meyers, A. (2019) 'Who is SALTY SPIDER (Sality)?', *crowdstrike.com*, 6 September. Available at: https://www.crowdstrike.com/blog/who-is-salty-spider/ (Accessed: 13 July 2023).

Nataliya, T. (2016) ‘National cyber security system of Ukraine: perspectives of policy development and capacity building’, *International scientific journal ‘Internauka’. Series: ‘Juridical Sciences’*, (7(21)), pp. 15–36. Available at: https://doi.org/10.25313/2520-2308-2019-7-5340.

National Cyber Security Strategies - Interactive Map: France (no date) *ENISA*. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (Accessed: 14 July 2023).

‘National Cyber Security Strategy’ (2023). The White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (Accessed: 13 July 2023).

‘National Cyber Strategy of the United States of America’ (2018). The White House. Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Accessed: 13 July 2023).

National Cybersecurity Strategies Guidelines & tools (no date) *ENISA*. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools (Accessed: 18 June 2023).

Nomadic Octopus (2022). Available at: https://attack.mitre.org/groups/G0133/ (Accessed: 13 July 2023).

Octopus-infested seas of Central Asia (2018). Available at: https://securelist.com/octopus-infested-seas-of-central-asia/88200/ (Accessed:

13 July 2023).

O'Neill, P.H. (2021) *The $1 billion Russian cyber company that the US says hacks for Moscow*, *MIT Technology Review*. Available at: https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/ (Accessed: 13 July 2023).

Ongoing Sophisticated Malware Campaign Compromising ICS (Update E) (2021) *Cybersecurity and Infrastructure Security Agency*. Available at: https://www.cisa.gov/news-events/ics-alerts/ics-alert-14-281-01e (Accessed: 12 July 2023).

'Our Work with the DNC: Setting the record straight' (2020) *crowdstrike.com*, 5 June. Available at: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (Accessed: 12 July 2023).

Pankov, N. (2017) *Moonlight Maze: Lessons from history*, *Kaspersky*. Available at: https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/ (Accessed: 11 July 2023).

Paul, K. (2022) '"We are not ready": a cyber expert on US vulnerability to a Russian attack', *The Guardian*, 11 March. Available at: https://www.theguardian.com/technology/2022/mar/10/us-russia-cyber-attack-prepared (Accessed: 18 June 2023).

Perez, E. and Prokupecz, S. (2015a) *How the U.S. thinks Russians hacked the White House*, *CNN*. Available at: https://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.html (Accessed: 11 July 2023).

Perez, E. and Prokupecz, S. (2015b) *Sources: State Dept. hack the 'worst ever'*, *CNN*. Available at: https://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html (Accessed: 11 July 2023).

Perlroth, N., Scott, M. and Frenkel, S. (2017) 'Cyberattack Hits Ukraine Then Spreads Internationally', *The New York Times*, 27 June. Available at: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html (Accessed: 12 July 2023).

'Proceedings of the 2023 U.S.-Ukraine Cyber Dialogue' (2023) *United States Department of State*, 5 June. Available at: https://www.state.gov/proceedings-of-the-2023-u-s-ukraine-cyber-dialogue/ (Accessed: 13 July 2023).

'Pro-Russian Hacktivist Group "KillNet" Threat to HPH Sector' (2023). U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3). Available at: https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf (Accessed: 13 July 2023).

Przetacznik, J. (2022) *Russia's war on Ukraine: Timeline of cyber-attacks*. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549 (Accessed: 16 November 2022).

'Ransomware Trends in Bank Secrecy Act Data between July 2021 and December 2021' (2022). U.S. Treasury Financial Crimes Enforcement Network. Available at: https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf (Accessed: 13 July 2023).

Resurgent Iron Liberty Targeting Energy Sector (2019) *Secureworks*. Available at: https://www.secureworks.com/research/resurgent-iron-liberty-targeting-energy-sector (Accessed: 11 July 2023).

Romo, V. (2022) 'Pro-Russian hackers claim responsibility for knocking U.S. airport websites offline', *NPR*, 10 October. Available at: https://www.npr.org/2022/10/10/1127902795/airport-killnet-cyberattack-hacker-russia (Accessed: 18 June 2023).

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (2022) *Cybersecurity and Infrastructure Security Agency*. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a (Accessed: 11 July 2023).

Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine (2023) *State Special Communications Service of Ukraine*. Available at: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine (Accessed: 11 July 2023).

Sabbagh, D. (2023) 'Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency', *The Guardian*, 19 January. Available at: https://www.theguardian.com/world/2023/jan/19/cyber-attacks-have-tripled-in-past-year-says-ukraine-cybersecurity-agency (Accessed: 18 June 2023).

Sadowski, J. and Hall, R. (2022) 'Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation', *Mandiant*, 25 November. Available at: https://www.mandiant.com/resources/blog/russia-invasion-ukraine-retaliation (Accessed: 13 July 2023).

Sandworm Team (2023) *MITRE*. Available at: https://attack.mitre.org/groups/G0034/ (Accessed: 12 July 2023).

Schectman, J. and Bing, C. (2022) 'EXCLUSIVE Ukraine calls on hacker underground to defend against Russia', *Reuters*, 24 February. Available at: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/ (Accessed: 4 November 2022).

Schmitt, E. and Crowley, M. (2023) 'Leaked Pentagon Documents Reveal Secrets About Friends and Foes', *The New York Times*, 8 April. Available at: https://www.nytimes.com/explain/2023/russia-ukraine-war-documents-leak (Accessed: 13 July 2023).

Schwarz, D. and Stone-Gross, B. (2022) *Using DDoS, DanaBot targets Ukrainian Ministry of Defense*, *Zscaler*. Available at: https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense (Accessed: 13 July 2023).

Several state websites disrupted by Killnet DDoS attacks (2022) *SC Media*. Available at: https://www.scmagazine.com/brief/malware/several-state-websites-disrupted-by-killnet-ddos-attacks (Accessed: 18 June 2023).

Shachtman, N. (2010) 'Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated)', *Wired*, 25 August. Available at: https://www.wired.com/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/ (Accessed: 11 July 2023).

Shackelford, S.J. *et al.* (2017) 'From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It',

Nebraska Law Review, 96, pp. 320–338. Available at: https://heinonline.org/HOL/Page?handle=hein.journals/nebklr96&id=338&div=&collection= (Accessed: 13 July 2023).

Shafqat, N. and Masood, A. (2016) 'Comparative Analysis of Various National Cyber Security Strategies', *International Journal of Computer Science and Information Security*, 14(1), pp. 129–136.

Shuya, M. (2018) 'Russian Cyber Aggression and the New Cold War', *Journal of Strategic Security*, 11(1), pp. 1–18. Available at: https://www.jstor.org/stable/26466903 (Accessed: 18 June 2023).

Simpson, S. (2021) *SANSA breach: International hacker group claims responsibility for Space Agency leak*, *The South African*. Available at: https://www.thesouthafrican.com/technology/sansa-breach-international-hacker-group-claims-responsibility-for-space-agency-leak-9-september-2021/ (Accessed: 13 July 2023).

Smoke Loader (2020) *MITRE*. Available at: https://attack.mitre.org/software/S0226/ (Accessed: 13 July 2023).

'Spear Phishing Attacks Target Organizations in Ukraine, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot' (2022) *Unit 42*, 26 February. Available at: https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/ (Accessed: 13 July 2023).

SSU and NATO step up cooperation in cybersecurity: threat monitoring systems integrated (2022) *SSU*. Available at: https://ssu.gov.ua/en/novyny/sbu-ta-nato-posylyly-spivpratsiu-u-sferi-kiberbezpeky-vidbulasia-vzaiemna-intehratsiia-system-monitorynhu-zahroz

(Accessed: 13 July 2023).

Starks, T., Nakashima, E. and Coletta, A. (2023) ‘Leaked Pentagon documents claim that hackers breached a Canadian gas network. Here’s what to know.’, *Washington Post*, 11 April. Available at: https://www.washingtonpost.com/politics/2023/04/11/leaked-pentagon-documents-claim-that-hackers-breached-canadian-gas-network-heres-what-know/ (Accessed: 13 July 2023).

Strauss, A. and Corbin, J. (1994) ‘Grounded theory methodology: An overview’, in *Handbook of qualitative research*. Thousand Oaks, CA, US: Sage Publications, Inc, pp. 273–285.

Tatar, Ü. *et al.* (2014) ‘A Comparative Analysis of the National Cyber Security Strategies of Leading Nations’, in *International Conference on Cyber Warfare and Security*. Reading, United Kingdom: Academic Conferences International Limited, pp. 211–218. Available at: https://www.proquest.com/docview/1779459625/abstract/4ED79F37AF624868PQ/1 (Accessed: 18 October 2022).

‘The 7 Dukes: 7 years of Russian cyberespionage’ (2015). F-Secure. Available at: https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf (Accessed: 11 June 2023).

Toulas, B. (2022a) *Ukraine’s IT Army is disrupting Russia’s alcohol distribution*, *BleepingComputer*. Available at: https://www.bleepingcomputer.com/news/security/ukraine-s-it-army-is-disrupting-russias-alcohol-distribution/ (Accessed: 13 July 2023).

Toulas, B. (2022b) *US airports’ sites taken down in DDoS attacks by pro-*

Russian hackers, *BleepingComputer*. Available at: https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/ (Accessed: 18 June 2023).

Townsend, K. (2022) 'Killnet Releases "Proof" of Its Attack Against Lockheed Martin', *SecurityWeek*, 12 August. Available at: https://www.securityweek.com/killnet-releases-proof-its-attack-against-lockheed-martin/ (Accessed: 13 July 2023).

Treasury Sanctions Russia with Sweeping New Sanctions Authority (2023) *U.S. Department of the Treasury*. Available at: https://home.treasury.gov/news/press-releases/jy0127 (Accessed: 13 July 2023).

Turla (2021) *MITRE*. Available at: https://attack.mitre.org/versions/v10/groups/G0010/ (Accessed: 12 July 2023).

Turla Enterprise Evaluation 2023 (no date) *MITRE ENGENUITY ATT&CK EVALUATIONS*. Available at: https://attackevals.mitre-engenuity.org/enterprise/turla/ (Accessed: 12 July 2023).

Tvaronavičienė, M. *et al.* (2020) 'Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania', *Insights into Regional Development*, 2(4), pp. 802–813. Available at: https://doi.org/10.9770/ird.2020.2.4(6).

UK exposes Russian spy agency behind cyber incidents (2022) *GOV.UK*. Available at: https://www.gov.uk/government/news/uk-exposes-russian-spy-agency-behind-cyber-incidents (Accessed: 12 July 2023).

Ukraine (no date) *National Cyber Security Index*. Available at: https://ncsi.ega.ee/country/ua/ (Accessed: 18 June 2023).

United States (no date) *National Cyber Security Index*. Available at: https://ncsi.ega.ee/country/us/ (Accessed: 13 July 2023).

U.S. Charges Russian GRU Officers with International Hacking and Disinformation Operations (2018) *U.S. Embassy and Consulate in the Netherlands*. Available at: https://nl.usembassy.gov/u-s-charges-russian-gru-officers-with-international-hacking-and-related-influence-and-disinformation-operations/ (Accessed: 12 July 2023).

Vail, E. (2022) *Russia or Ukraine: Hacking groups take sides*, *The Record*. Available at: https://therecord.media/russia-or-ukraine-hacking-groups-take-sides (Accessed: 13 July 2023).

Vakulyk, O. *et al.* (2020) 'CYBERSECURITY AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE', *Journal of Security and Sustainability Issues*, 9, pp. 775–784. Available at: https://doi.org/10.9770/jssi.2020.9.3(4).

Wehner, M. and Lohse, E. (2016) 'Wikileaks: Sicherheitskreise: Russland hackte geheime Bundestagsakten', *FAZ.NET*, 11 December. Available at: https://www.faz.net/aktuell/politik/inland/wikileaks-sicherheitskreise-russland-hackte-geheime-bundestagsakten-14568558.html (Accessed: 11 July 2023).

XENOTIME Threat Group (2020) *Dragos*. Available at: https://www.dragos.com/threat/xenotime/ (Accessed: 12 July 2023).

Zolotar, O.O. *et al.* (2022) ‘Prospects and Current Status of Defence Information Security in Ukraine’, *Hasanuddin Law Review*, 8(1), pp. 18–29. Available at: https://doi.org/10.20956/halrev.v8i1.3582.

Про критичну інфраструктуру [About critical infrastructure] (2022). Available at: https://zakon.rada.gov.ua/go/1882-20 (Accessed: 23 July 2023).

УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 [DECREE OF THE PRESIDENT OF UKRAINE No. 447/2021] (2021) *Офіційне інтернет-представництво Президента України*. Available at: https://www.president.gov.ua/documents/4472021-40013 (Accessed: 13 July 2023).

11. Appendix

Appendix 1: interview outline for semi-structured interviews.

- What is your experience with Russian cyber-attacks?
    - What do they target most often?
    - What attack techniques do they use?
    - What types of attackers are these?

- Do you know of any strategic initiatives Ukraine has put in place on a national level to protect its IT systems?

- What have you learned are general best practices to protect IT-systems against these attacks?
    - What have been essential parts of crisis management plan?
        - E.g. leadership
    - What have been the most important parts of cyber operations?
        - E.g. having many backups
    - What can you recommend to governments and organizations to protect their cyber security?

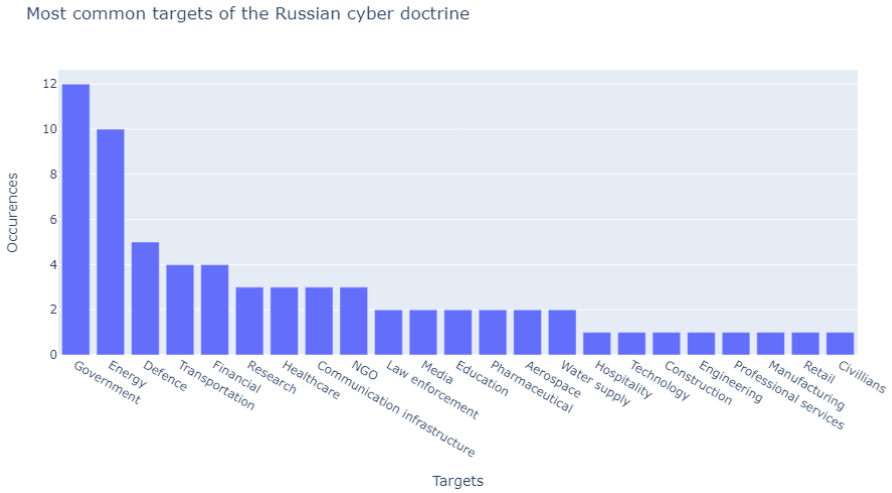

Figure A: most common targets of the Russian cyber doctrine.

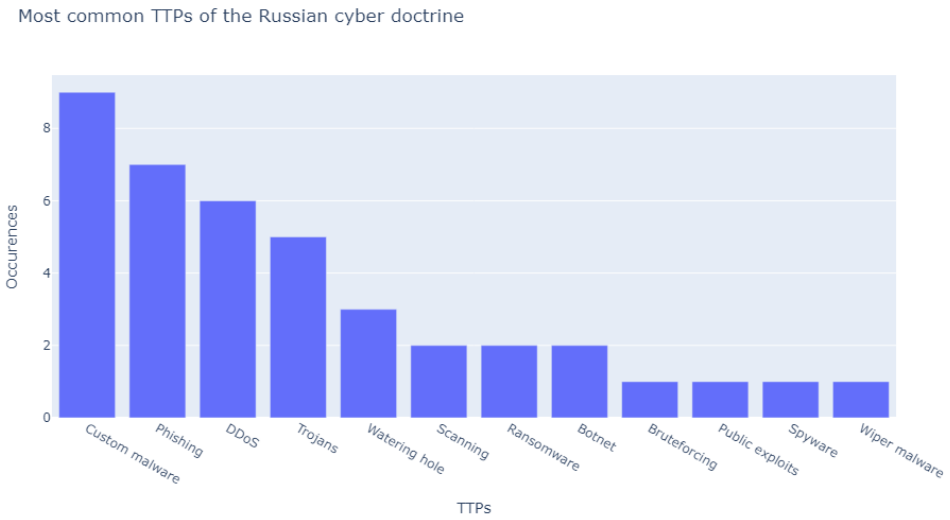

Figure B: most common TTPs of the Russian cyber doctrine.

Table A: Most common targets and TTPs per Russian threat group and private companies.

Russian threat groups and private companies	Targets	TTPs
Dragonfly	Government	Scanning
Dragonfly	Transportation	Bruteforcing
Dragonfly	Defence	Watering hole
Dragonfly	Energy	
Dragonfly	Water supply	
Dragonfly 2.0	Energy	Phishing
Dragonfly 2.0	Transportation	Watering hole
Dragonfly 2.0		Trojans
Dragonfly 2.0		Custom malware
Gamaredon	Government	Trojans
Gamaredon	Defence	Phishing
Gamaredon	Media	
Gamaredon	NGO	
Gamaredon	Law enforcement	
APT29	Government	Custom malware
APT29	NGO	Phishing
APT29	Research and education	Public exploits
InvisiMole	Government	Spyware
APT28	Government	Phishing
APT28	Defence	Custom Malware
APT28	Hospitality	
APT28	Research and education	
APT28	NGO	
APT28	Energy	
APT28	Financial	
APT28	Communication infrastructure	
APT28	Transportation	
APT28	Energy	
Sandworm	Energy	DDoS
Sandworm		Custom Malware
Sandworm		Phishing

Temp.Veles	Energy	Custom Malware
Turla	Government	Custom Malware
Turla	Defence	
Turla	Research and education	
Turla	Pharmaceutical	
Turla	Aerospace	
Killnet	Government	DDoS
Killnet	Healthcare	
Killnet	Defence	
XakNet	Government	
XakNet	Media	
XakNet	Energy	
Zarya	Energy	DDoS
The Coomingroject	Communication infrastructure	Ransomware
The CoomingProject		
MUMMY SPIDER	Financial	Custom malware
MUMMY SPIDER	Healthcare	Trojans
MUMMY SPIDER	Research and education	
MUMMY SPIDER	Government	
MUMMY SPIDER	Technology	
SALTY SPIDER		Botnet
SALTY SPIDER		DDoS
SCULLY SPIDER	Financial	Botnet
SCULLY SPIDER	Government	Custom malware
SCULLY SPIDER		Trojans
SCULLY SPIDER		DDoS
SMOKEY SPIDER		Custom malware
SMOKEY SPIDER		DDoS

WIZARD SPIDER	Construction	Ransomware
WIZARD SPIDER	Engineering	
WIZARD SPIDER	Law enforcement	
WIZARD SPIDER	Professional services	
WIZARD SPIDER	Manufacturing	
WIZARD SPIDER	Retail	
WIZARD SPIDER	Healthcare	
ALLANITE	Energy	Phishing
ALLANITE		Watering hole
Ember Bear	Government	Wiper malware
Ember Bear	Pharmaceutical	Phishing
Ember Bear	Financial	
Nomadic octopus	Government	Trojans
Nomadic octopus	Civilians	
NTC Vulkan	Energy	Scanning
NTC Vulkan	Water supply	
NTC Vulkan	Transportation	
NTC Vulkan	Communication infrastructure	