Cyber Warfare: A Part of the Russo-Ukrainian War in 2022

Jari Juutilainen

Master’s thesis
September 2022
Master’s Degree Programme in Information Technology

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Description

Juutilainen, Jari

Cyber Warfare: A Part of the Russo-Ukrainian War in 2022

Jyväskylä: JAMK University of Applied Sciences, September 2022, 111 + 39 pages.

Technology, Information and Communications. Degree Programme in Information and Communications Technology. Master’s thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

On 24th of February, 2022, the Russian Federation launched an invasion of Ukraine. This is the first-time cyber warfare capabilities are used as part of modern warfare. During this war around 800 cyber-attacks have been witnessed targeting to Ukraine alone. This created a possibility to research cyber warfare and its different methods used along-side with traditional warfare in armed conflict.

The research’s focus was in finding what kind of data regarding the monitored cyber-attacks and cyber operations can be discovered and what kind of impacts those attacks can be analyzed to have while depending solely on public sources. To achieve this, qualitative research methods were used to analyze multiple different sources ranging from online news articles to government reports. To create a summarized baseline for understanding the events witnessed, an extensive literature review was made to collect information. These data were used to achieve understanding of what is counted as cyber warfare in different nations interpretations.

The concepts and terminology of cyber warfare are analyzed and presented as a part of the literature review. These also include analyses of subjects identified to cause bias to the different studied topics of the Russo-Ukrainian cyber war.

The main finding of the research was cyber warfare being limited warfare during the Russo-Ukrainian war. No strategically meaningful outcomes for the Russian war effort have not been conducted by the means of cyber warfare. The finding was in-line with recently published reports by private security vendors and government organizations and research institutes. With known bias created by dependency to public sources, the longer analysis period is required for a more in-depth analysis for the root causes. While the war is still ongoing it allows the possibility to continue monitoring of the situation for the more detailed observations.

Keywords/tags (subjects)

Cyber Warfare, Cyber Operations, Cyber Weapons, Cyber-attacks, Cyber Incidents, Russia, Ukraine

Miscellaneous (Confidential information)

No confidential information in this thesis.

Contents

Figures

Tables

Acronyms

ACINT	Acoustic Intelligence
APT	Advanced Persistent Threat
CA	Cyber Actions
CCDR	Combatant Commander
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CISR	Cyber Intelligence, Surveillance, Reconnaissance
CPT	Cyber Protection Team
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CO	Cyber Operations
CS	Cyber Security
CTI	Cyber Threat Intelligence
CW	Cyber Warfare
DCO	Defensive Cyber Operations
DCO-IDM	Defensive Cyber Operations – Internal Defensive Measures
DCO-RA	Defensive Cyber Operations – Responsive Action
DDoS	Distributed Denial of Service
DNI	Digital Network Intelligence
DoD	Department of Defence
DODIN	Department of Defence Information Networks
DoS	Denial of Service
EMS	Electromagnetic spectrum
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FSB	Federal Security Service of the Russian Federation
GEOINT	Geospatial Intelligence
GRU	Main Intelligence Directorate of the Russian Federation
GU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
HUMINT	Human Intelligence
IIoT	Industrial Internet of Things
ICT	Information and Communications Technologies
ICS	Industrial Control Systems
IHL	International Humanitarian Laws
IMINT	Imagery Intelligence
IO	Information Operations
IOC	Indication of Compromise
IoMT	Internet of Medical Things
IoT	Internet of Things

ISR	Intelligence, Surveillance and Reconnaissance
IW	Information Warfare
JCS	Joint Chiefs of Staff
LOAC	Laws of Armed Conflict
MASINT	Measurement and Signature Intelligence
MEDINT	Medical Intelligence
MILDEC	Military Deception
MRRT	Mission Rapid Response Team
SIGINT	Signals Intelligence
SSSCIP	State Service of Special Communication and Information Protection of Ukraine
SSU	Security Service of Ukraine
StratCom	Strategic Communication
SVR	Foreign Intelligence Service of the Russian Federation
TECHINT	Technical Intelligence
TTPs	Tactics, Techniques, and Procedures
OCO	Offensive Cyber Operations
OPE	Operational Preparation of Environment
OPSEC	Operations Security
OSINT	Open Sources Intelligence
PLC	Programmable Logic Controller
PSYOPS	Psychological Operations
ROE	Rules of Engagement

1 Introduction

“After land, sea, air and space, warfare has entered the fifth domain: cyberspace” (Murphy, 2010).

On February 24th, 2022, armed forces of the Russian Federation launched invasion of Ukraine. One day earlier massive cyber-attacks began targeting different organizations of the Ukrainian government, financial sector, energy sector, and several others. This is not the first cyber war we are witnessing as cyber warfare operations have also been continuously targeting Ukraine over the past decade, but this is the very first time when we can observe cyber warfare being used to support traditional and modern warfare.

The Ukrainian cyber theatre is academically intriguing as we see two strong cyberspace actors going head-to-head. Russian hacker units have traditionally been recognized to be among the best in the world. Ukrainian cyber defence is one of the strongest if not even the strongest in the Europe (Connell &Vogler, 2016; Voo et al., 2020). This creates a unique opportunity to monitor how these cyber capabilities are used during an armed conflict and how well suitable cyber warfare is for supporting traditional warfare. Also, this allows us to understand how efficiently a strong cyber resilience and cyber defence can help to counter these cyber-attacks.

During the first days of Russo-Ukrainian war we also witnessed a huge increase of hacktivism. Ukraine called for international mobilization of volunteers for “IT Army of Ukraine” (Burgess, 2022a). Soon after, hacktivist collective Anonymous “declared war” against Russia and many more new hacktivist groups were born to both sides of the conflict (Pitrelli, 2022). This is also the first time when we are seeing volunteering civilians from other countries participating in offensive actions in this scale without actually joining to the armed forces (Delcker, 2022). This creates new challenges for the interpreting of international laws and treaties of armed conflict.

A short history review of the evolution of cyber warfare is made to understand the nature of these cyber-attacks. The review includes what kind of international laws and treaties are setting the rules for armed conflicts and how those are currently interpreted for acts done in cyberspace. The characteristics of cyberspace are discussed as there is no consensus of what actually is this digital realm called cyberspace. So, for this it is necessary to understand how different nations are treating it as a warfare capability. This is followed by introducing what kind of military cyber operations are executed in cyberspace.

2 Research methodology

2.1 Research Question

The main research question for this thesis was defined as what kind of cyber operations (CO) have been observed during the Russo-Ukrainian war and how does the cyber warfare (CW) aspect of the war reflect to the academic concept of use of cyber capabilities as part of conventional warfare?

Secondary research question was defined to analyze effectivity of impact of these observed cyber operations for military and civilian targets.

This thesis is delineated to include only cyber operations where cyber weapons, hacking tools or similar technical methods are being utilized. Even when some of the military doctrines include information operations performed in the cyber domain as cyber operations, those are covered only superficially as a part of this thesis and their effects are not studied in detail.

2.2 Research Methodology and Data Collection

This thesis is aiming to provide a baseline for understanding what kind of cyber operations have been monitored in Ukraine during the Russo-Ukrainian war in 2022. To achieve this object, this thesis relays on qualitative research methods. As such, data collection for this thesis is done only from the public sources. The data regarding cyber-attacks has been collected from January to end of July. These sources include public websites, reports published by different organizations and companies, military doctrines, technical analyses published by security researchers, white papers, books/ebooks, news articles from the media, Facebook posts, Twitter posts, and Telegram channels. The data were collected on daily basis from CERT-UA and from various websites utilizing different search engines. Articles translated from Ukrainian or Russian were compared with different sources to be reasonably confident of the correctness of the translation. The collected data from these sources were summarized and used as a dataset for the research. The dataset is included in the appendixes.

Usually only one source is cited for the observed cyber-attacks, but their content has been verified by the author from multiple sources or they have been cross-referenced with other sources for verification of translation. In those rare occasions, when the contents have not been possible to verify from multiple sources, it is mentioned in the text. The cyber-attacks listed by some of the used sources that the author was not able to verify have been left out from this thesis.

2.3 Research Ethics

On writing this thesis, including its data collection, the author has followed Jyväskylä University of Applied Science's ethical principles (JAMK, 2018) as well the ethical recommendations for thesis writing at universities of applied sciences (Arene, 2019) during this thesis project.

The author has not participated in any of the illegal or malicious acts presented in this thesis. Also, leaked data dumps published by the hacktivists groups or any other actors mentioned on this thesis were not collected nor analyzed during the research by the author. In all information and analyses of their content the author is dependent from the third parties cited as their sources instead of the primary sources typically used in the academic research.

It is also important to note that the author did not have perfect visibility into all the relevant events and cyber-attacks done in Ukraine during the research period. Reasons for these are e.g., different languages and information sharing strategies. The author is not seeking to take sides on the monitored cyber operations, but to research them as technical observations to understand current state of the cyber warfare and its legality in the eyes of the international law and treaties.

3 Cyber Warfare

3.1 Evolution of Battlefield

The roots of cyber warfare can be placed, as suggested by Bosquet (2009), roughly in the beginning of the twentieth century (Figure 1). The communication warfare started to make its way to the battlefield as the troop movements started to become much faster with the development of steam engines and later of combustion engines. This led to the need for developing better and faster communication methods to create a more accurate situational awareness.

After the Second World War, militaries started to adopt electronic warfare (EW) as a part of their activities. Electronic signals were used for communications and encryption algorithms were used to prevent intelligence activities. Bosquet (2009) proposes, that this created a need to be able to affect transfer of electronic signals. Modification, or prevention, of them all together was used to reduce the reliability of command-and-control and fire control. Need for the computers and their calculation power became much more critical to battle with the increasing information needs, the uncertainty on the battlefield and to support the decision-making process, according Bosquet.

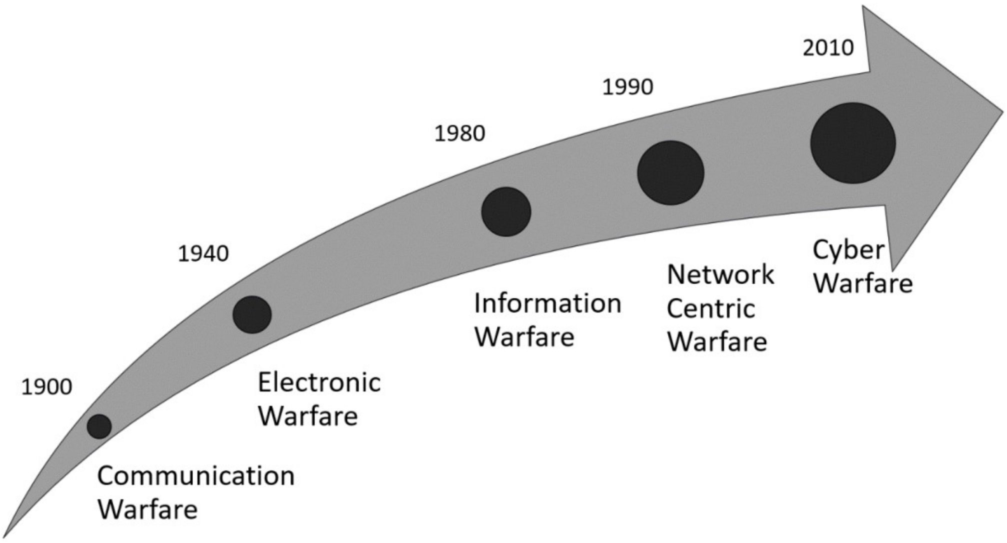


Figure 1. Evolution from Communication Warfare to Cyber Warfare (Lehto, 2014, modified)

Information demands of the battlefield kept growing and it made armed forces dependent from the information, electronic data transfer and energy distribution. To clarify these newly introduced needs Libicki (1995) presented a concept of information warfare (IW) as the main category with sub-categories:

- Command-and-control warfare
- Intelligence-based warfare
- Electronic warfare
- Psychological operations

- Hackerwar
- Information economic warfare
- Cyberwar

This new information warfare definition must not be confused with “war of minds,” (Toffler & Toffler, 1993) the modern definition of IW, where information operations are used to affect the psychological aspect of the target. Information warfare has a part in a today’s CW, at least according to some doctrines, and this will be discussed in the next chapter.

The US Naval Institute introduced in 1998 a concept of network to parallel with information. As introduced by Alberts et al. (2000), this created a concept of network centric warfare where the idea was to move from the calculation intensive model to network intensive model. It began to create joint situational-awareness from the battlefield for the first time for the military commanders which made it possible to have an advance in military operations with new kind of tactics and methods.

This evolution led to the birth of current concept of CW as the role of critical infrastructure was increased with the role of command-and-control as centric part of this new warfare method. One of the main new reasons to differentiate the CW from its predecessors was the new concept of Total War where the participants of the warfare were not only the military forces, but the society as a whole. The effects to society will be studied in more detail in later chapter. Another reason to differentiate the CW from the IW was because cyber threats were considered to be the continuous new normal, when IW was considered to be a part of crisis and war-time (Lehto, 2014). The term “Cyber” as a new method of warfare was introduced around the same time period with the concept of network centric warfare, but the term started to reach more popularity during the early 2000’s.

Electronic warfare, information warfare and cyber warfare as modern concepts still share several similarities and their definitions are somewhat overlapping. These will be analyzed in a more detail later.

3.2 The Birth of Cyberspace

To understand what cyber warfare actually is and how it is interpreted by different nations, we must examine how the cyberspace itself is understood. The definition of cyberspace has evolved during the last three decades and still is constantly changing as technological progress proceeds. Limnéll et al. (2014) discusses how complexity of defining the nature of cyberspace can be seen in the inability to form a consensus for its exact definition. The definition of cyberspace differs in military doctrines and national strategies created by different nations. It is usually also a bit different from cyberspace definition in non-military context as stated by Limnéll et al.

The word “cyber” originates from the Greek word “kybereo”, which means “to steer, to guide, to control”. The word began to appear in military publications at the end of the 1990’s when it started to replace terms information warfare and information operations in context of network security, computer security and information security as introduced in the previous chapter (Limnéll et al., 2014).

Origins of the interconnected networked computers and current internet can be backtracked to the era of Cold War, when the United States build the advanced research projects agency network, or more commonly known by its acronym, the ARPANET (Bolt, Beranek & Newman Inc., 1981). It took a few years before militaries started to wake up to networked computers as a new threat vector. Kaplan (2016) claims that this began in 1983 when the United States’ President Ronald Reagan saw the movie WarGames. The movie is about a young teenage hacker getting access to the North American Aerospace Defense Command’s main computer leading eventually to a nuclear war. Questions raised by the movie resulted about a year later in a directive of National Policy on Telecommunications and Automated Information Systems Security (NSDD-145) which descripted means of unauthorized electronics access being already widely done by foreign intelligence services. According to Kaplan, this would be the starting point of cyber warfare.

To understand cyberspace in a military context, and what kind of attributes are commonly attached to its description, we can look for definitions used in military doctrines.

Military doctrine

A military doctrine and its purpose could be shortly generalized as it being a document that presents the best practices to operate armed forces capabilities to accomplish different national military objectives and goals (U.S. Air Force, 2020). It should not be confused with national or military policies and strategies. A policy is a document to give national or military directive of what must be accomplished. It may include rules of the engagement (ROE) of what can or can not be retaliated with kinetic and non-kinetic actions. A strategy explains how military operations are used to achieve objectives set by the national policy (U.S. Air Force, 2020). Sometimes these three document types can be merged as a single document where a nation describes, how it is going to defend its own existence by retaliating by different means during different circumstances (Colarik & Janczewski, 2012). One example of this kind of doctrine is from the Russian Federation (Sinovets & Renz, 2015).

The author suggests that noticing cyber threats and own cyber capabilities in a military doctrine is important as we are speaking from such a new and different kind of threat vector for a nation. It is important to specify how cyber-attacks will be retaliated and what kind of military cyber operations can be performed. Then the doctrine will also provide a clear guide line for the decision makers when these tasks need to be performed.

3.3 Cyberspace and Cyber Domain

As stated before, there is no consensus of what is considered to be cyberspace because complexity of the whole concept and its definitions vary by source and used context. Laari (2019) suggests that in the Finnish Defence Forces' context cyberspace is commonly understood as a domain formed by digital information systems, which also includes physical communications infrastructure and all the end users or entities. Typical characterization is the use of electronics and the electromagnetic spectrum (EMS) for transferring, modifying and storing data (Laari, 2019).

Military doctrines of the United States used to define cyberspace similarly to be an environment where "electronics and the electromagnetic spectrum are used to store, modify, and exchange data via networked systems" (Joint Chiefs of Staff, 2010, p. 60), but the definition was later on modified by JCS to “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Joint Chiefs of Staff, 2014, p. 100).

The United Kingdom’s doctrine broadens the definition describing it as “an operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains” (Ministry of Defence, 2016, p. 1). From this we can gather that the United Kingdom includes information operations, or at least, those done in or through cyberspace as a part of cyber warfare.

The Russian Federation does not acknowledge cyberspace as a part of their doctrine since they use a broader definition of information warfare. The Russian Federation’s 2010 military doctrine stated “the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force” (Russian Federation presidential edict, 2010, p. 6). As claimed by Connell and Vogler (2016), this allows Russia to use cyber capabilities during peacetime. It is notable that Russia does not acknowledge using these kind of methods as use of military force, as the Western World do. The part specifying the use of information warfare for achieving political goals was removed from the Russian doctrine in 2014 (The Embassy of the Russian Federation to United Kingdom of Great Britain and Northern Ireland, 2015).

Characteristics of Cyberspace

Cyberspace has some special and unique characteristics that distinguish it from the other battlefields. As Collier (2017) states, the deniability is one of the most typical characteristics of cyber warfare and the amount of deniability can be increased by using proxy warfare. In a proxy warfare the use of violence is outsourced from the armed forces to the technologies or other human participants. In cyber warfare a common example of using proxies along-side with the nation-state groups, are multiple organized-crime groups, known to be at least partially controlled and financed by the nation-state actors. These are the cyber counterparts of terrorist satellites and “little green men” used in the kinetic warfare (Collier, 2017). Using this kind of plausible deniability has become a crucial part of Russia’s cyber warfare actions, as claimed by Connell and Vogler (2016), even when the Russian Federation officially denies such allegations. Using proxies in cyberspace is not unique for the Russia and other nation-state actors are known to do the same (China, North Korea, Iran, etc.) as noted by Connell and Vogler.

The second unique characteristic for cyberspace is its global reach. In the other battlespaces (land, sea, air, space) physical troop movements are required and military operations can be predicted from military build-ups. In cyberspace a cyber-attack can be launched instantly to the other side of the globe without advance warning (Welch, 2011).

Another often raised suggestion regarding to cyberspace, as claimed by Springer (2015), is it being a battlefield where cyber warrior doesn’t require similar physical strength and other physical qualities as soldiers fighting traditional wars do. This remark is usually raised with concern of difficulties to get technically oriented and skilled persons for armed services and not to push these “keyboard warriors” away. While this might be true for casual hacking, we probably need to separate it from military service and could compare military cyber operations to be more similar to e-sports. Both of these are stressful and demanding environments causing a strain to the body and mind. To help counterbalance these effects good physical fitness is a must as suggested by studies (Ketelhut et al., 2021). The stressful and cognitive demanding environment of cyber operations was also studied by the U.S. Department of Defense which found that even five hours long cyber operations caused a significant frustration and fatigue to the cyber operators (Dykstra & Paul, 2018).

A Warfare Domain or Not?

Domains are used in military terms to define where the action and operations occurs. The term “domain” was firstly introduced in US Joint Chiefs of Staff’s publication, Joint Vision 2020, where domains replaced earlier concept of dimensions (Kreuzer, 2021). A principal difference between cyber domain and other four domains is that cyberspace is fully man-made while the rest are physical and natural domains. Warfare began from the land, extended to the sea, extended again three millennia later to the air and finally is reaching into the space (Springer, 2015). This shows how good humans have been to adapt any new inventions for their use in warfare and cyberspace is no different.

Classically there are own specialized armed forces branches of service for the different domains (army, navy, air force and in some countries separate space force), but usually there is no cyber force. Cyber units have been merged inside of the organizational structures of each branch which could indicate how interconnected and inseparable cyber domain is from these other domains (Welch, 2011). Though there has been calls for founding own service branch for the cyber force, for example in the United States (Barno & Bensahel, 2021).

To understand the properties of this man-made domain, Springer (2015) remarks cyberspace to be relied upon the hardware devices where the protocols and code are run which makes it possible to affect operationality of the domain through architectural and/or software changes while we cannot affect the same way the unchangeable laws of physical domains, like gravity.

For the last decade, as Kreuzer (2021) comments, there has been ongoing discussion if cyberspace really should be classified as a separate domain or something else. Kreuzer suggests that in a modern warfare context thinking cyberspace as a domain is too restrictive definition and not fitting to the definitions of other four domains. Problem with cyberspace as a domain is its lack of fixed boundaries and its rapidly evolving nature. As claimed by Patella-Rey (2012), cyberspace does not exist. It is an analogy or metaphor to simplify this complex network of interconnected devices and users. For this Kreuzer (2021) proposes that cyberspace should be considered as “a multi-domain operational construct” rather than a single domain. This would make it more similar to special operations or intelligence operations which are also multi-domain operations.

According to Connell and Vogler (2016), Russia has its own approach to the subject and it has not separated cyberspace as the fifth domain. In Russian military theory there are no cyber warfare or cyber operations at all. Instead, they have classified, as claimed by Connell and Vogler, the information landscape as a separate warfighting domain. For the Russian military, what the Western World call as cyber operations, are computer network operations subcategory of information warfare along with information operations, psychological operations (PSYOPS) and electronic warfare.

Cyberspace as a domain

Even though the discussion about cyberspace's combability to domain model is ongoing, it is currently understood as a domain. Cyberspace's relationship to other traditional warfare domains (land, sea, air and space) is complex. Cyberspace is part of the information environment which is relied to all the other physical domains, but also the physical domains are depended from cyberspace. This makes all the modern warfare domains interconnected (U.S. Air Force, 2011). The cross-referencing nature of cyberspace is shown in Figure 2.

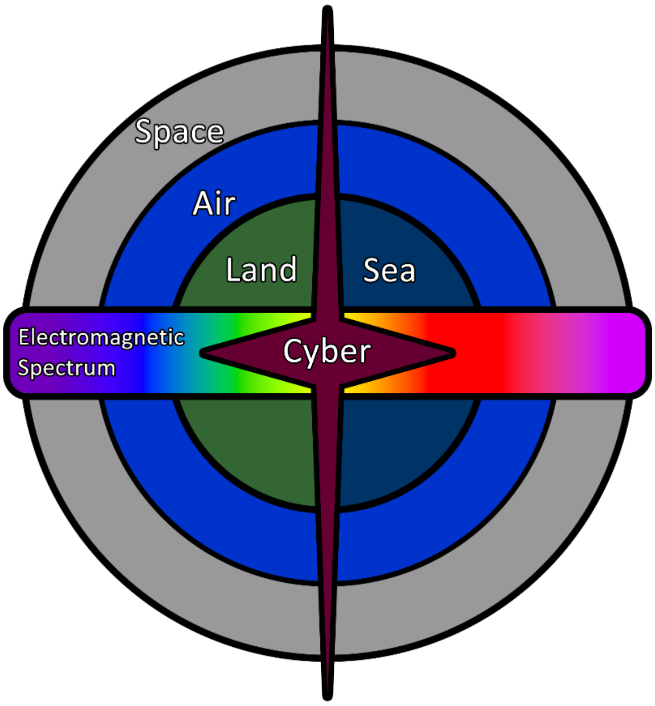


Figure 2. Cyber As the 5th Warfare Domain (U.S. Air Force, 2011, modified)

Joint Chiefs of Staff (2018) notes that infrastructure of cyber domain is located in all four physical domains. Actions done in physical world affects electromagnetic spectrum which may create events to happen in and through cyberspace. To explain this further, JCS presents cyberspace layer model (Figure 3) to clarify what kind of actions and events occur in different layers and how they can be utilized in the planning of cyber operations.

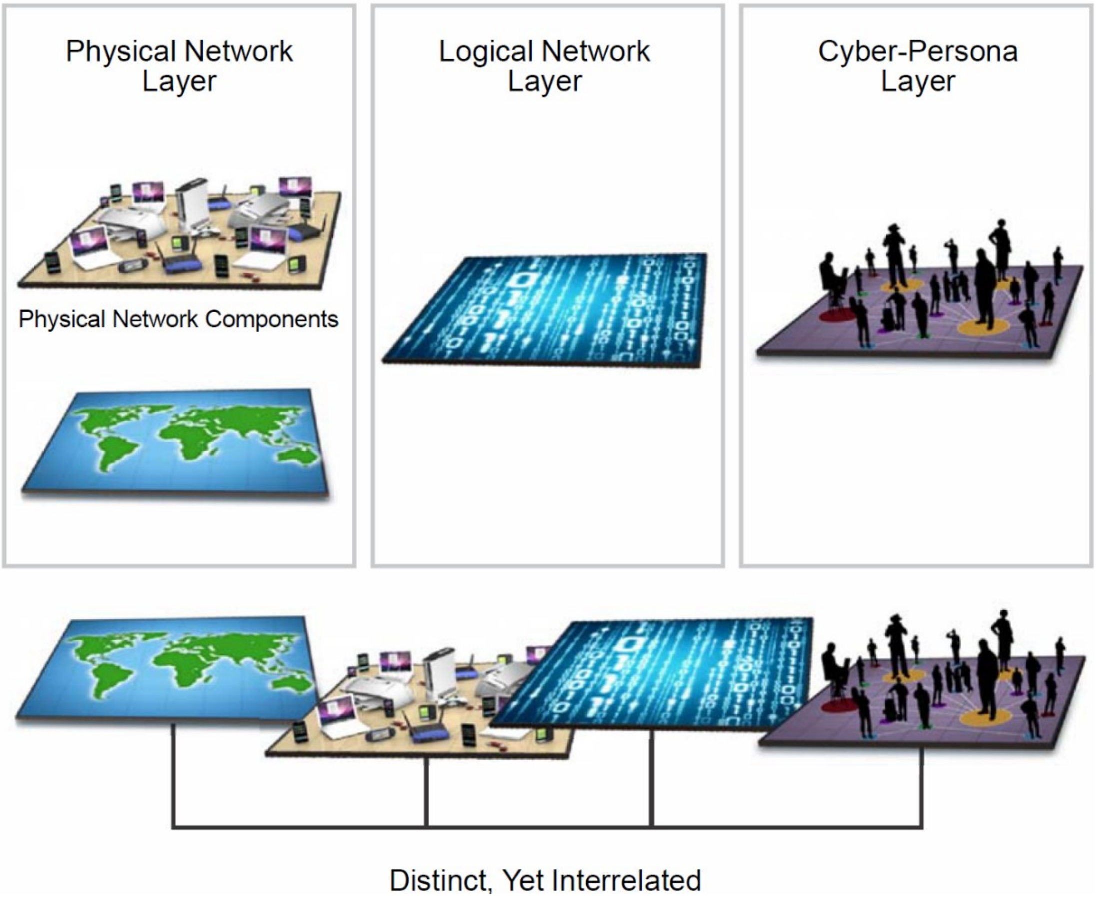


Figure 3. The Three Interrelated Layers of Cyberspace (Joint Chiefs of Staff, 2018)

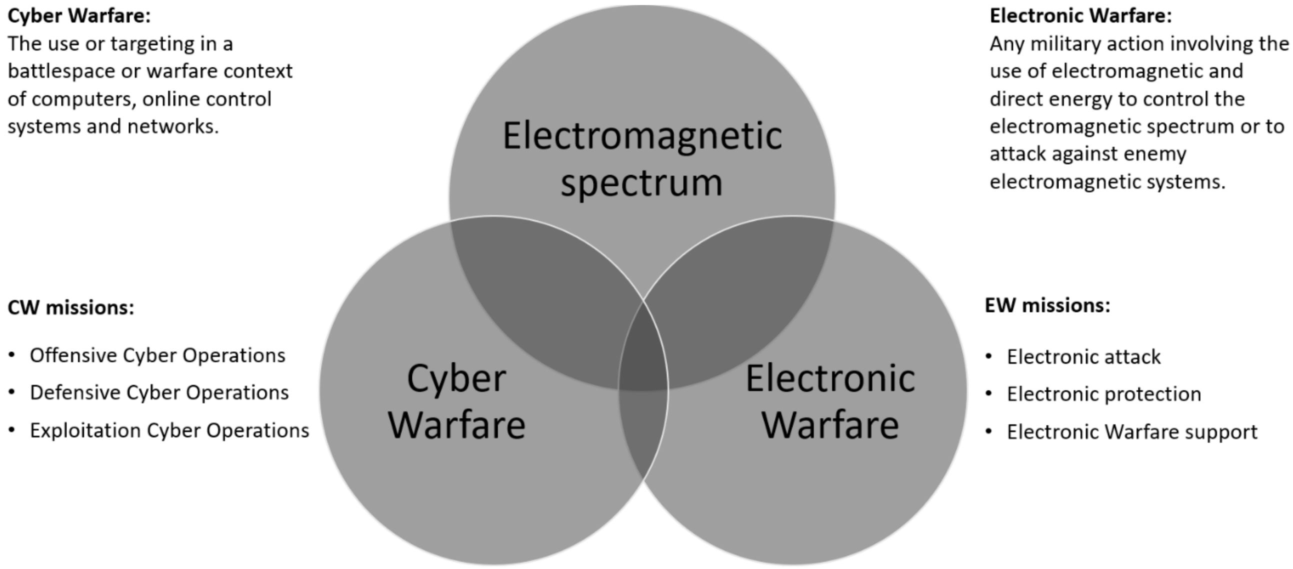
The first layer, by Joint Chiefs of Staff (2018) is the physical network layer. This is the part that contains all the hardware used to create networked computing and other infrastructural aspects of cyberspace: "e.g., computing devices, storage devices, network devices, and wired and wireless links" (Joint Chiefs of Staff, 2018, p. 23). Each of these devices have a physical geolocation, ruling them under that states' legislation. As these are physical devices, they can be affected with kinetic and non-kinetic actions.

The second layer in Joint Chiefs of Staff (2018) model is the logical network layer. This layer is consisted mostly of an ability to process data and to exchange data with protocols. In other words, this layer is based on logic programming and is not depended on physical locations. This opens them up for the possibility to be individual physical links and nodes or distributed ones which still can be presented as single entity. JCS's publication uses a website that is distributed to multiple geographic locations, but is having only one URL address as an example of this concept. Affecting this layer, according JCS, can be done only with cyberspace tools.

The third layer of Joint Chiefs of Staff’s (2018) model is the cyber-persona layer. This doesn’t reference to the end-users of cyberspace, but to network and user accounts located in cyberspace. A cyber-persona can or cannot be linked to a persona in the physical world because same account or credentials can be shared by several persons. Similarly, an actual persona can have several cyber-personae, as presented by JCS. This increases the complexity of cyberspace and creates more deniability when linking the cyber-persona to a real person.

Cyber Warfare and Electronic Warfare

As stated in previous chapter cyber warfare evolved from the electronic warfare, but their current descriptions still share a lot of similarities. Common features for CW and EW are that they are both considered being non-kinetic forms of warfare and both are operating in electromagnetic spectrum. Figure 4 illustrates shared EMS environment with different types of missions for each warfare classification (Lehto & Henselmann, 2019).



Cyber Warfare:
The use or targeting in a battlespace or warfare context of computers, online control systems and networks.

Electronic Warfare:
Any military action involving the use of electromagnetic and direct energy to control the electromagnetic spectrum or to attack against enemy electromagnetic systems.

CW missions:

- Offensive Cyber Operations
- Defensive Cyber Operations
- Exploitation Cyber Operations

EW missions:

- Electronic attack
- Electronic protection
- Electronic Warfare support

Figure 4. The Electronic Warfare and Cyber Warfare in EMS Environment (Lehto & Henselmann, 2019, modified)

In Finland CW and EW are still considered as their own independent warfare methods, but in some countries, like in the United States, military has seen benefits to start to merge these as a single warfare method. This change is loosely based on interpreting CW as a domain, but EW not being a domain. Traditionally EW has been defined by being modifying or controlling the EMS environment. In the past separating these two has made more sense as they both clearly were used in different methods to different targets. An example of this could be an analog radar - A classic target for EW to jam the signal or disturb its signal to point to the wrong location. Nowadays radar systems have become much more digital and this opens new attack vectors for combined CW and EW capabilities both operating in EMS. This could result as an attack where software (CW) is moved through the EMS (EW) to the target system (Pomerleau, 2021).

Kinetic or Non-kinetic?

One common classification or characteristic today is CW being non-kinetic use of the force, when the traditional warfare has always been the use of the kinetic force (rocks, arrows, bombs, missiles and all other ammunition). Non-kinetic definition is true for the most of the military operations executed on cyberspace, but we cannot rule out the kinetic effect of the some of the observed cyber-attacks (Colarik & Janczewski, 2012; Applegate, 2013).

While it is true that when cyber-attacks are executed the execution method itself is non-kinetic and, in many cases, the planed end-result of the attack is also non-kinetic (Nye, 2017). For example, hacking to the server to dump its databases is from the start to the end non-kinetic operation. The difficulty with this classification comes when we start to think embedded systems or similar cyber-physical-systems (Applegate, 2013). Targeting these has an end result that usually can have an actual kinetic effect.

We can divide kinetic nature of CW to two kinds of actions. One with physical actions affecting cyberspace and one with cyberspace having effects to the physical world. Examples of physical actions affecting cyber-realm are simply breaking the connectivity (e.g., data cables) or physically destroying a device to deny access to it or from it (Tarabay, 2022). For affecting the physical world from cyberspace, the first major event could be considered to be March 4, 2007, when the famous Operation Aurora (the Aurora generator test) was performed on Idaho National Laboratory by the U.S. Department of Energy. The test was done to demonstrate cyber-related vulnerabilities on power grids. During the test a 2.5 MW generator was made to run out-of-sync by opening and closing its control and protection relay with about 30 lines of malicious code resulting with running the generator inoperable (Department of Homeland Security, 2014). Department of Homeland Security's documents regarding the Operation Aurora suggests that during operation it was finally realised how significant cyber attacks against critical infrastructure can be.

Two years later, the first true kinetic cyber weapon, the STUXNET-worm was discovered. The worm was used against the Iranian nuclear program. As summarization its payload targeted the industrial control systems (ICS) and programmable logic controllers (PLC) affecting the set operating values and slowly rendering the gas centrifuges non-operable (Falliere et al., 2010).

Another new attack surface has been created by digitalization and Internet of Things (IoT) which has also started to gain a foot-hold in industrial systems with Industrial Internet of Things (IIoT) and Internet of Medical Things (IoMT) (Figliola, 2020). Simplified principle for IoT devices is to have networked devices or sensors. The data produced by these devices or sensors are usually processed in a cloud service provided by a third-party with machine learning or artificial intelligence-based tools to create more sophisticated analysis of the input data. In industrial environments this could be used for example to improve pre-emptive maintenance to decrease number of production disruptions caused by malfunctions (Padmalaya et al., 2022). Weaponization of these networked devices could possibly result with severe kinetic effects, especially when talking about "smart cities" or in case of IoMT even to assassinations. As we are still in an early phase of digitalization and IoT, it is hard to predict what the trend for these kinds of cyber-attacks will be, but it is relevant to note as a part of CW's kinetic or non-kinetic definition as suggested by Colarik and Janczewski (2012).

In Figure 5 is presented the three warfare methods sharing the non-kinetic battlefield. As we can see from the figure these warfare methods are overlaying each other while sharing the common battlefield. Each of these can be used for supporting another or through the another's medium. This is probably the reason why different nations classify these warfare types and their missions so differently.

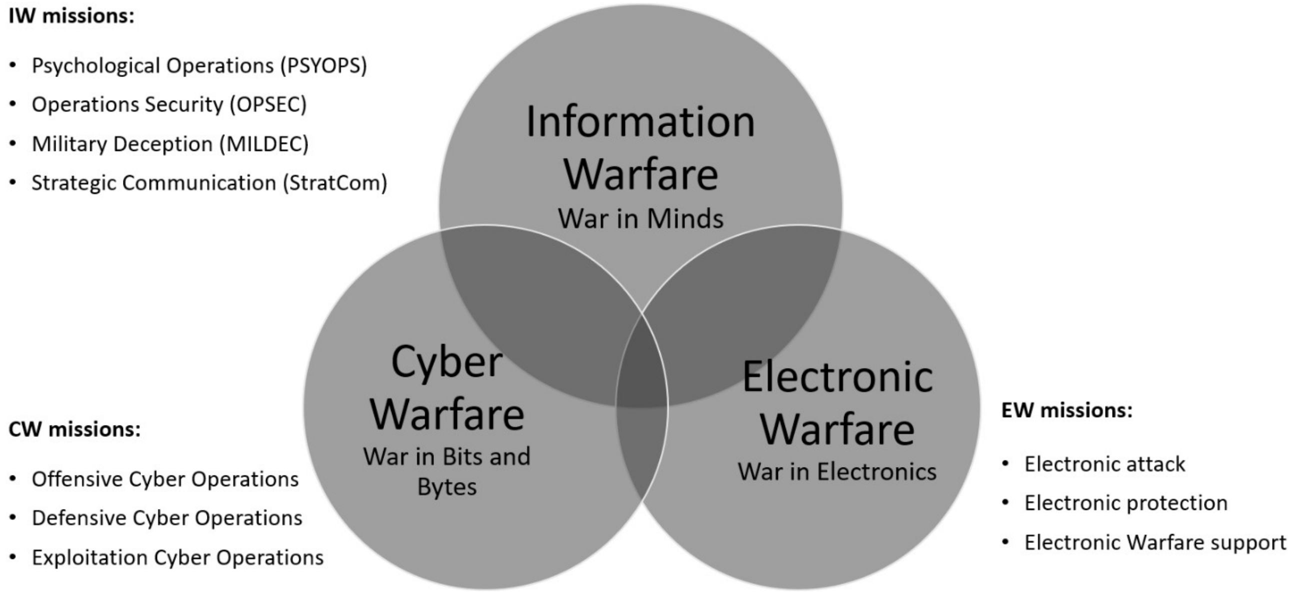

IW missions:
• Psychological Operations (PSYOPS)
• Operations Security (OPSEC)
• Military Deception (MILDEC)
• Strategic Communication (StratCom)
Information Warfare
War in Minds
Cyber Warfare
War in Bits and Bytes
Electronic Warfare
War in Electronics
CW missions:
• Offensive Cyber Operations
• Defensive Cyber Operations
• Exploitation Cyber Operations
EW missions:
• Electronic attack
• Electronic protection
• Electronic Warfare support

Figure 5. Non-kinetic Warfare Spectrum (Lehto & Henselman, 2020, modified)

For the classification of kinetic or non-kinetic characteristics of these warfare methods is also how the end results of missions are interpreted. If we compare the EW and CW both of these can have kinetic end-results. Using EW capabilities to modify radar output that causes a fighter jet to crash certainly has a kinetic end-result, but it is more indirect end-result. But when CW is used to modify set values of PLC to get a centrifuge to malfunction, the end-result is direct result and the actual goal why the CW capabilities were utilized.

As stated by Connell and Vogler (2016), we also must take in consideration the cyber-attacks executed against the critical infrastructure, as seen in the Russian cyber operations in the Ukraine. In one operation, as claimed by Connell and Vogler, attackers were able to remotely connect to a power company’s system and operate circuit breakers to cause a power outage. The effects of this kind of cyber-attack could be interpreted as a kinetic effect. The attack known as BlackEnergy will be discussed more in the chapter focusing on the major cyber events witnessed in Ukraine before the war.

3.4 Cyber Warfare Versus Conventional Warfare

Chen and Dinerman (2016) compare differences of conventional warfare and cyber warfare. Typical reasons for their use have different kind of objectives. When a state decides to use conventional warfare against another state, we have a reasonable cause to believe that there will be casualties, just by looking at historical events. But when a state decides to use cyber warfare against other state some damage to devices and equipment may occur, but commonly there are no lethal or even injuring events to the people, at least not directly. Indirect consequences of for example information operations still may cause such as seen in the United States' Capitol Hill riot (Peters et al., 2021). This less violent nature of cyber warfare makes it today the grey-zone between peace and war and leave more room to operate without too much fear for retaliation (Nye, 2017). Differences between these warfare methods are compared in Table 1.

Table 1. Conventional Warfare versus Cyber Warfare (Chen & Dinerman, 2016, modified)

	CONVENTIONAL WARFARE	CYBER WARFARE
Purpose of Warfare	To gain dominance (political, economic, religious, ideological etc.) of specified geolocation for a period of time or permanently.	To assist gaining dominance (political, economic, religious, ideological etc.) for a period of time or permanently. To gain information advantage or superiority.
Strategy	Use of covert and/or overt operations. Show of strength.	Use of covert and/or overt operations. Easy to deny involvement.
Actors	Typically, militaries or paramilitaries.	Anyone with a device and connectivity to network.
Targets	Targeting humans and human life.	Targeting information and information systems. Indirectly may target to human life in cyber-physical world.
Operational Environment	Limited geo-locational space.	Global environment.
Duration	A limited period of time.	Continuously ongoing with short active attack periods.
Preparation Time	Takes a long time to prepare.	Takes a short time to prepare.

Cost	Expensive to accomplish.	Inexpensive to accomplish.
Characteristics	Transparent.	Opaque.
Identification of Actors	Easy to identify.	Difficult to identify.
Rules of Engagement	Clear (Laws of War and International Humanitarian Laws).	Unclear.
Impact for Target	Human casualties. Major destruction of property and infrastructure.	Minor destruction of equipment. Significant data breaches. Crippling critical infrastructure, possible indirect human casualties.
Deterrence	Forceful and apparent.	Uncertain.
Dominance	Possible to achieve.	Difficult to achieve.
End-Results	Apparent.	Obscure.
Winner	Easy to identify.	Difficult to specify.
Time for Recovering	Requires long time period and major resources.	Requires short time period and few resources.

Like Chen and Dinerman (2016) suggest, reasons for conventional warfare are usually gaining more resources or dominance. For resources, this usually means occupying more land areas while in cyber warfare it is less likely that a state would want to occupy adversary's data center or network just to gain more presence and resources in cyberspace. But there might also be other political, economic or religious purposes why the means of conventional warfare is used against other state as noted by Chen and Dinerman. Cyber warfare itself can not solely be used to gain those, but it can be used to assist gaining them for example by modifying peoples' opinions and gaining information for leverage.

Also, cyber warfare is not depended from geography as conventional warfare is as stated by Chen and Dinerman (2016). While conventional warfare needs to move military (or paramilitary) troops with some means to the targeted state and logistic routes must be build and this makes conventional warfare expensive. Cyberspace does not share similar restrictions. Attacks and operations can be executed instantly to anywhere in the world and can be done with significantly less manpower and equipment, making it relatively cheap. From this Chen and Dinerman identified difference in nature and duration of these two warfare methods. Cyber warfare is constantly ongoing, but its operations are typically short-lived when warfighting in a real world takes from days to years.

Another aspect discussed by Chen and Dinerman (2016) is the time needed for recovering when the hostilities have ended. In cyber warfare recovery time is usually short, but in aftermath of conventional warfare re-building infrastructures and sometimes whole cities can take several years.

3.5 International Laws and Treaties

The regulation of lawful and just war is done by international laws and treaties. The two main rule collections are: The international law of war, or more commonly known as laws of armed conflict (LOAC) (*Jus in Bello*), and the definition of criteria when the war can be engaged (*Jus ad Bellum*). These are often incorrectly considered to be created from the viewpoint of traditional use of kinetic force and military troops. They apply also to cyber warfare and other modern warfare methods as well, when those are used as part of armed conflict (Springer, 2020). These international humanitarian laws (IHL) are based on the Charter of the United Nations and Statute of the International Court of Justice as well on the treaties of the Geneva Conventions. In summarization these laws of armed war for a just war can be defined to three basic principles (a) every nation has a right for self-defense; (b) use of force must not create unnecessary suffering for the civilians; (c) and use of force must be proportional to the caused threat (United Nations, 1977; Hasu, 2014).

Cyberspace as a battlefield has created a grey-zone between war and peace that is also bending the definition of a just war. In conventional warfare subjects for use of force must be military targets and causing suffering for civilians is forbidden unless it is necessary and related to the military target (United Nations, 1977). Problem arises from the nature of cyberspace. As stated by International Committee of the Red Cross (2013), we have only one single cyberspace which is shared by both, militaries and civilians and both are using same technologies and sometimes even same platforms. This makes separating non-military targets from military targets difficult. This raises a question of what makes a military target in cyberspace? For example, if armed forces are outsourcing some of its data center infrastructure to the multinational vendor’s cloud service, would that make the cloud service a legitimate military target? What about if the same cloud service is offering services for a hospital or a power company? In cyberspace targets often can be part of critical national infrastructure which has a potential to cause harm for civilians (Cybersecurity & Infrastructure Security Agency, 2022). These are discussed more deeply in the chapter focusing to the Total War aspect of CW.

The situation from stand point of IHL is complicated when the military cyber operations are executed outside of armed conflict. Those operations are not usually falling under obligations of IHL (International Committee of the Red Cross, 2013). This does not of course mean that every military cyber operation is an acceptable act when it is done outside of armed conflict. We need to separate cyber-attacks and their effects to violent and non-violent actions, as suggested by Sander (2019).

Operations aiming to have violent and destructive actions could be interpreted as armed conflicts or possibly even as acts of war. Even when it is not established in targeted nation’s military doctrine, national policy or national strategy as a such. NATO’s first attempt to create a rule set for cyber warfare, the Tallinn Manual, defines these violent actions as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmidt, 2017, p. 415). Sander (2019) raises a valid question of regarding what can be interpreted as a damage in cyberspace? More problematic this comes when these acts are targeting critical infrastructure. Some of the experts are suggesting that these should be considered more as cyber sabotage than cyber warfare when they are done outside of an armed conflict (Smith, 2013; Morag, 2014).

Non-violent operations are more grey-zone and in current LOAC and IHL frameworks can not be considered as acts of war and causes for war (*casus belli*) (Smith, 2013). Some examples of these would be targeting other nation’s election system, using IW operations in a social media to affect people’s attitudes or participating in cyber espionage (Springer, 2020; Bigelow, 2019). Doctrine of the United States known as “Military operations other than war” defined purpose of non-violent acts affecting to other state’s affairs as “deterring war, resolving conflict, promoting peace, and supporting civil authorities in response to domestic crises” (Joint Chiefs of Staff, 1995, p. 13), but the definition and the whole doctrine has been revoked.

Another problematic part of IHL is cyberspace's nature as a field where everyone can participate, even to the cyber warfare. Different actors in civil/military field and how their positioning as participants to warlike activities are commonly understood are presented in Figure 6. The IHL protects civilians during the armed conflict, but the Russo-Ukrainian war has introduced a new situation where civilian hackers are participating directly warfare hostilities. International Committee of the Red Cross (2013) has stated such actions would revoke the legal protection and make the hackers legitimate target for a retaliation. In any case, participating would basically render civilian hackers as unlawful cyber combatants. Same is considered also from stand-point of cyber operations resulting in violent actions in the Tallinn Manual: "Civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate" (Schmidt, 2017, p. 413).

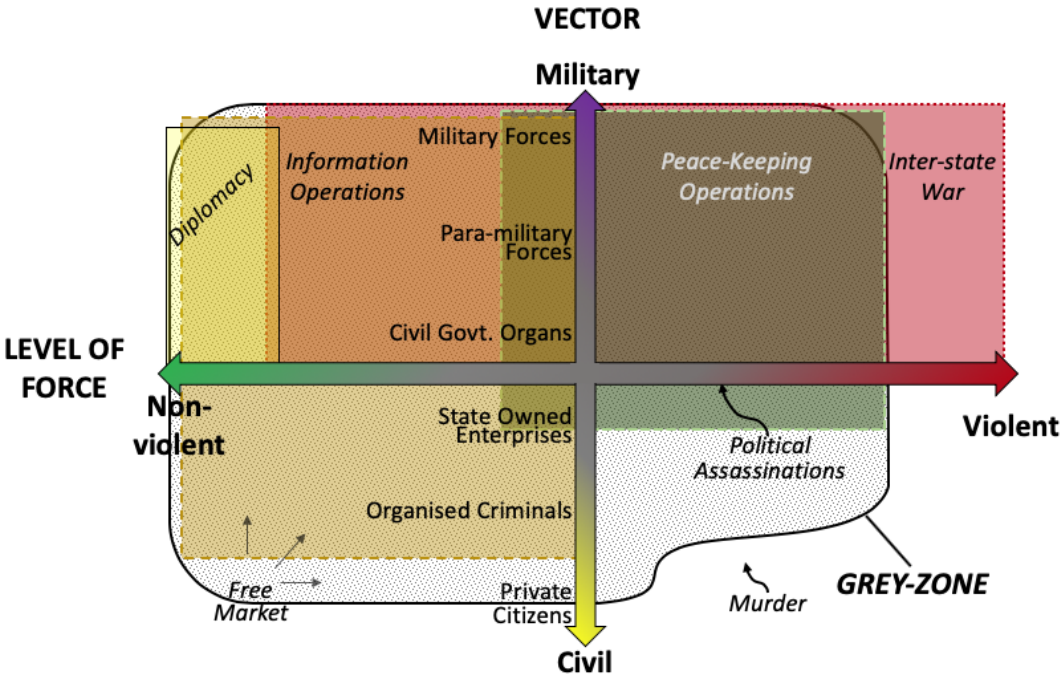


Figure 6. Peace/War and Civil/Military Paradigm (Dobbs et al., 2020)

Yet another problem is created by unpredictable nature of cyber weapons and cyber-attacks. Even when the attack would be planned and executed against some specified target complying with obligations of IHL, the consequences can still be unknown. A recent example would be the NotPetya ransomware, which was targeted against Ukraine, but ended up creating destruction all over the world (Schmidt, 2017).

3.6 Concept of Total War and Functions Vital to Society

The concept of Total War was pitched in the twentieth century, to present warfare against the whole society while using mass-bombings, starvation and similar methods for mass destruction and causing unnecessary suffering for the civilians (Sambaluk, 2020). Acts like these are forbidden by IHL, but when considering typical targets of cyber warfare, we see them constantly targeting critical infrastructure which has a potentially to cause unnecessary harm for civilian population (Nye, 2017). Effects to civilian population and to a person are different from how CW affects military targets. Today's society is similarly depended from data networks and information communication technologies as military is. As stated before, separating the two can sometimes be difficult from cyberspace perspective.

To understand how missing or non-available parts of the functions vital to society affects a person, we need to understand the five basic needs humans have, as proposed by Maslow (1943; 1954). According to Maslow, the most basic and the most important level of person's needs are the ones that makes survival possible. These physiological needs are air, water, food, warmth, rest, etc. The Maslow's second level is person's safety needs. To feel safe and in control of their lives people need things provided by family and society. Examples from these are security (emotional and financial), social stability, health and wellbeing. The Maslow's third level of needs are related to love and belongingness. A human is a social creature which is depended from social interactions. To satisfy these needs, Maslow suggests need to have feelings (e.g., feelings of intimacy, trust, love, acceptance, etc.) that are related to interpersonal relationships and belonging to a group. The Maslow's fourth level is one's needs for self-esteem. To satisfy these needs one can feel dignity (because some achievement or mastering a skill) or we can desire reputation (or respect) from others. The fifth, and the highest level of person's needs, as claimed by Maslow, is the self-actualization needs. These are related to person's own self-growth that is usually referred as person's self-fulfillment and peak experiences.

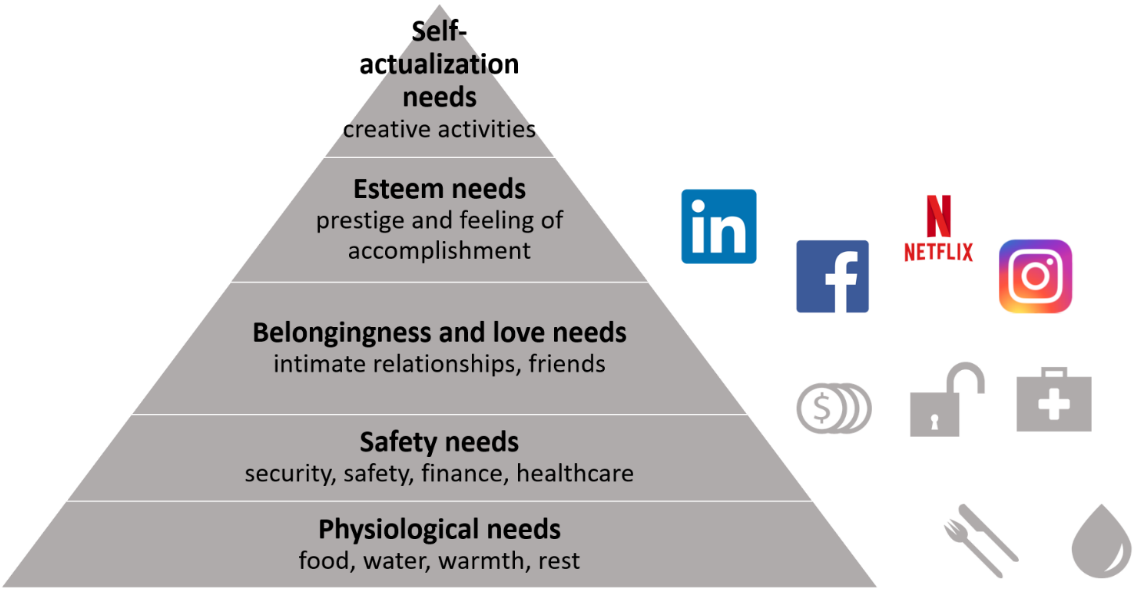

Self-actualization needs
creative activities
Esteem needs
prestige and feeling of accomplishment
Belongingness and love needs
intimate relationships, friends
Safety needs
security, safety, finance, healthcare
Physiological needs
food, water, warmth, rest
NETFLIX

Figure 7. Digitalization and Energy As a Part of Hierarchy of Needs (Hartikainen, 2022, modified)

These five basic needs presented by Maslow (1943; 1954) are still the same today, but as our world has been coming increasingly more depended from information and communications technologies (ICT) as a result of digitalization. In Figure 7, Hartikainen (2022) introduced how fulfillment of Maslow's hierarchy of needs are depended in today's world from digitalization and energy.

At least the first three levels of Maslow's hierarchy of needs are depended from energy and digitalization as stated by Hartikainen (2022). Attacks, cyberspace related or not, against the first level of hierarchy of need could start become life-threatening in three days if clean drinking water is not available. In winter disruptions on heating would become also lethal in a couple of days (Puolustusministeriö, 2010).

If the attacks are targeted to second level, situation is a much less acute for civilians. The biggest problems starts if the affected sector is finance related and prevents the use of credit and debit cards. The number and per centage of digital financial transactions are constantly increasing as cash is used less frequently. Another problem comes from digital point-of-sale systems in retail if the data networks are not working, then the store's servers are out of service. Situation like this was witnessed in Sweden when ransomware attack in a supply chain of store's point-of-sale system rendered over 800 store locations non-operational (Mukherjee & Fulton, 2021). Even if the customers would have cash to pay their purchases the stores cannot log those transactions and their inventory runs out-of-sync very soon. In a nation-wide emergency situation this probably would not be a such a big problem and inventory and sales could depend on other methods (e.g., pen and paper). Similar problem and solution were seen in Ukraine's border control when it was hit by wiper malware in February 2022 (Alspach, 2022).

As we move to higher tier in a need hierarchy, the less life threatening the effects come. In a third level communication disruptions would make people worried, sometimes critically so, from well-being of their loved-ones and friends. This certainly would be a source of increased stress and be a partial cause for other problems derived from it. For companies on the other hand communication disruptions can be quite critical. Communication would include social media platforms to some degree at least. When the disruptions are affecting working of entertainment services, like streaming services of videos and music it will start to be a more annoyance than serious condition for person's survival.

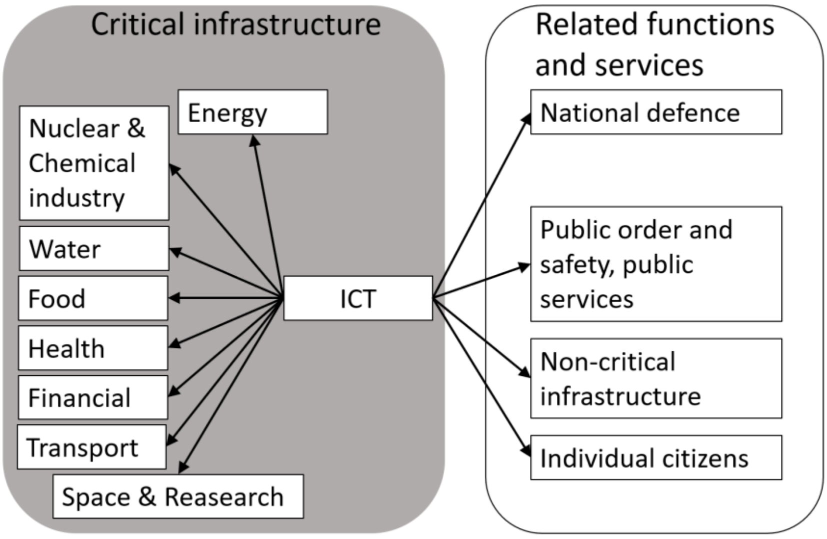

Critical infrastructure
Nuclear & Chemical industry
Energy
Water
Food
Health
Financial
Transport
Space & Reasearch
ICT
Related functions and services
National defence
Public order and safety, public services
Non-critical infrastructure
Individual citizens

Figure 8. Relation of ICT to Critical Infrastructure and Other Functions and Services (Lanto et al., 2019, modified)

In Figure 8 is shown how ICT is related to critical infrastructure and its related functions and services. To satisfy primal basic need to survive, as stated earlier, a person needs food to eat and clean water to drink. Both of these also have to be transported for the consumer and money is required to purchase them. All of these are depended from energy production and transmission.

Even the ICT itself is depended from the energy. This could indicate that the energy production is the most critical sector for todays digital and networked world.

To examine this more, we can take a look at Finland's National Emergency Supply Agency's research of how different lines of business are depended on each other in Figure 9.

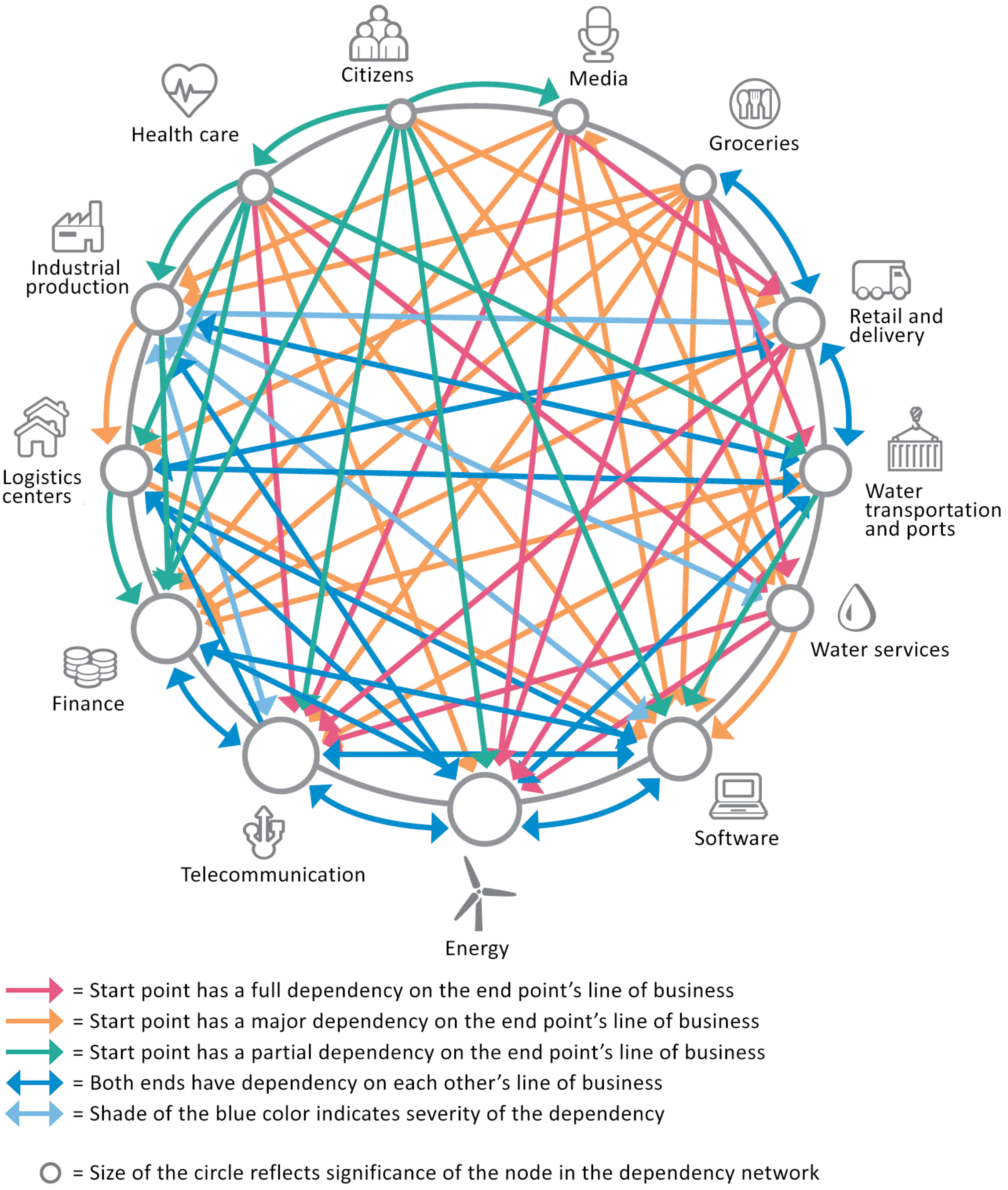

Citizens
Media
Health care
Groceries
Industrial production
Retail and delivery
Logistics centers
Water transportation and ports
Water services
Finance
Software
Telecommunication
Energy
→ = Start point has a full dependency on the end point's line of business
→ = Start point has a major dependency on the end point's line of business
→ = Start point has a partial dependency on the end point's line of business
↔ = Both ends have dependency on each other's line of business
↔ = Shade of the blue color indicates severity of the dependency
○ = Size of the circle reflects significance of the node in the dependency network

Figure 9. Dependency Network of Lines of Bussiness (Huoltovarmuusorganisaation Digipooli, 2020, modified)

As we can see from the figure, Finland's National Emergency Supply Agency's study confirms that most of the different lines of businesses have today a full or major dependency from telecommunication business. This is of course because everything is interconnected by internet and the systems used by businesses are based on software. Digitalization of the world has created a huge dependency of reliability of telecommunication networks and energy production.

This is also supported by recent study of Finnish Chamber of Commerce (2022), done in co-operation with National Emergency Supply Agency, where 49 % of studied companies stated being unable to operate during power outage. While 17 % of companies were told to be able to manage a day long power outage, meaning power outage continuing longer than a day would render 66 % of companies unable to continue their business. The study finds the situation being a little better regarding digital services. Only 22 % of companies could not manage a day without digital services while only 17 % told being able to fully manage a single day (Chamber of Commerce, 2022).

3.7 Military Cyber Operations

Military cyber operations, as the name states, are military operations conducted in the cyberspace by a nation-state actor or its proxy. Reason to conduct operations in cyberspace is same than it is for any other military operation conducted in the physical world. This is to have strategic, operational or tactical gain to fulfil some national interest (Brantly & Smeets, 2020).

As established earlier, there is no consensus on what is regarded as cyberspace and the situation is same for definition of cyber operations (CO). Different nations have different definitions for what is counted as CO, but there are common shared similarities in national doctrines. Depending on the nation, military cyber operations can be divided usually to sub-categories, their number ranging from three to five. These typically are defensive cyber operations (DCO), offensive cyber operations (OCO), cyber espionage, and Department of Defence internal network (DODIN) operations (Joint Chief of Staff, 2018). The fifth and more debatable category is information operations (IO) which is more often regarded as a part of information warfare even when the information influencing is done in or through the cyberspace. In any case IO executed through cyberspace are too significant part of ongoing cyber warfare to rule out in this context even if they wouldn't be classified as actual CO by most countries.

Usually, the lines between CO and IO are the part which has the greyest zones in the interpretation. In Figure 10 Laari (2019) presents one possible concept for how cyber operations and cyber actions (CA) could be categorized and is currently understood in Finnish Defence Forces. The model is refining the principal concept based on the idea of the United States' Joint Cyber Doctrine for how to separate different kind of missions done in and through cyberspace (Joint Chiefs of Staff, 2018).

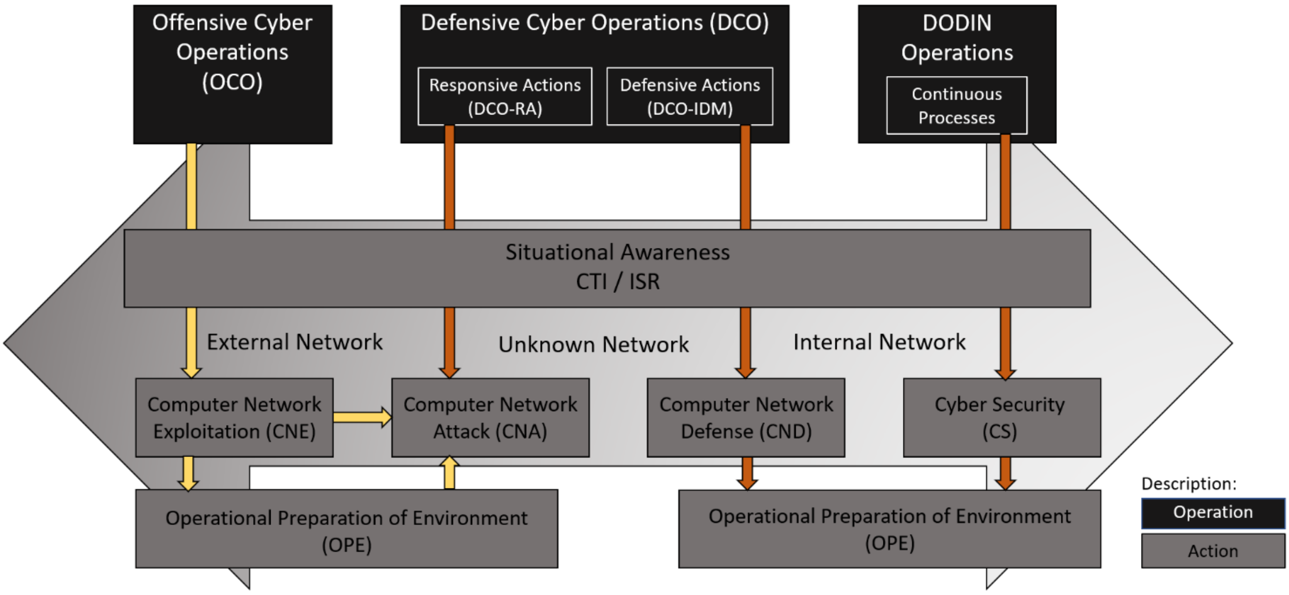

Offensive Cyber Operations (OCO)
Defensive Cyber Operations (DCO)
Responsive Actions (DCO-RA)
Defensive Actions (DCO-IDM)
DODIN Operations
Continuous Processes
Situational Awareness CTI / ISR
External Network
Unknown Network
Internal Network
Computer Network Exploitation (CNE)
Computer Network Attack (CNA)
Computer Network Defense (CND)
Cyber Security (CS)
Operational Preparation of Environment (OPE)
Operational Preparation of Environment (OPE)
Description:
Operation
Action

Figure 10. Cyber Operations and Actions (Laari, 2019, modified)

As we can interpret from Figure 10, the common part for every kind of CO is to have comprehensive situational awareness from organization's own internal networks and external networks, including possible adversary's networks. As Laari (2019) proposes, these activities can be divided into two main categories, cyber threat intelligence (CTI) and intelligence, surveillance and reconnaissance (ISR). CTI is a type of intelligence that is commonly used to improve self-protection by gaining information from different types of threats and threat actors. This can also be used for offensive purposes by gathering similar information from advisories networks and systems (Laari, 2019). ISR includes collecting and analysing more common information, monitoring of different type of activities or be targeted reconnaissance of some specific system. Another common feature for all CO is operational preparation of environment (OPE). This can be targeted to own internal networks or external networks, depending if it is part of DCO or OCO.

Cyber units in a military are usually not any different from any other kind of military units. Military personnel are divided same way to brigades, companies, platoons, and squads, depending of course from the size of the nation’s armed forces and number of cyber warriors. It is also common that each cyber unit is oriented for one of the operation types (defence, offense, etc.) depending the skill set of its members (Brantly & Smeets, 2020).

One notable feature is that many nations’ defensive cyber capabilities might not totally rely on military personnel only, but may also include civilian operators and outsourced vendors. This of course is not too distant from using private security companies fighting in physical battlefields, as seen on some of the latest wars (Swed & Crosbie, 2019). Especially the role of private vendors and civilians has increased in DODIN operations and defensive operations (Ministry of Defence, 2016).

3.7.1 Defensive Operations

The main reason for military or any other organization to have defensive cyber operations is to ensure the freedom of manoeuvring in cyberspace. This can be done through active or passive defence measures where the idea is to increase cyber resilience of the organization to decrease the risk level of cyber threats to accepted level (Ministry of Defence, 2016).

Typical way to classify DCO is to separate them to three different categories as presented earlier in Figure 10. These include technical capabilities as well administrative tasks such as creating and maintaining frameworks for cyber security. One note worthy aspect of defensive operations is deterrence. The United States, the United Kingdom and Russia for example state in their doctrines that cyber-attack can be retaliated with use of deadly kinetic force (Join Chiefs of Staff, 2018; Ministry of Defence, 2016). Russia takes this even further and permits use of nuclear weapons to retaliate military actions (Limnéll et al., 2014). This is affirmed in Russian research where cyber weapons and their use is commonly compared to strategic nuclear weapons (Dylevsky et al., 2015; Kukkola, 2021, p. 157).

As already shown in Figure 10, DCO are depended from situational awareness created by CTI and ISR capabilities to improve own OPE to correspond and mitigate current threats.

DODIN operations

This is the most common type of military operations done in cyberspace and it "includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN" (Joint Chiefs of Staff, 2018, p. 36). DODIN is an acronym used by the United States (Department of Defence information networks) to represent nation's operated military networks.

These are ongoing daily routine activities to ensure cyber security and cyber resilience of own organization as a whole. This includes cyber and information security management systems, hardening of software and hardware, having antivirus software or other end-point protection software, using honeypots etc. One part of the DODIN operations is also to monitor own networks, which could include anything from data flow monitoring to fingerprinting known indicators of compromise (IOC) data (Joint Chiefs of Staff, (2018).

DODIN operations are run against everyday malicious actions and not necessarily against specified threat. They could be presented as a baseline of organization's cyber resilience and support function for other types of CO (Joint Chiefs of Staff, 2018).

Defensive Cyber Operations – Internal Defensive Measures (DCO-IDM)

Definition for internal defensive measures is "where authorized defense actions occur within the defended network or portion of cyberspace" (Joint Chiefs of Staff, 2018, p. 38). This means they can be executed in own internal networks or some other networks like related to critical infrastructure depending on the legislation of a state. The main thing is that these are authorized actions by the owner of the defended network. One of the main aspects of the DCO-IDM is to have good situational awareness of the environment by means of intelligence, surveillance and reconnaissance (ISR).

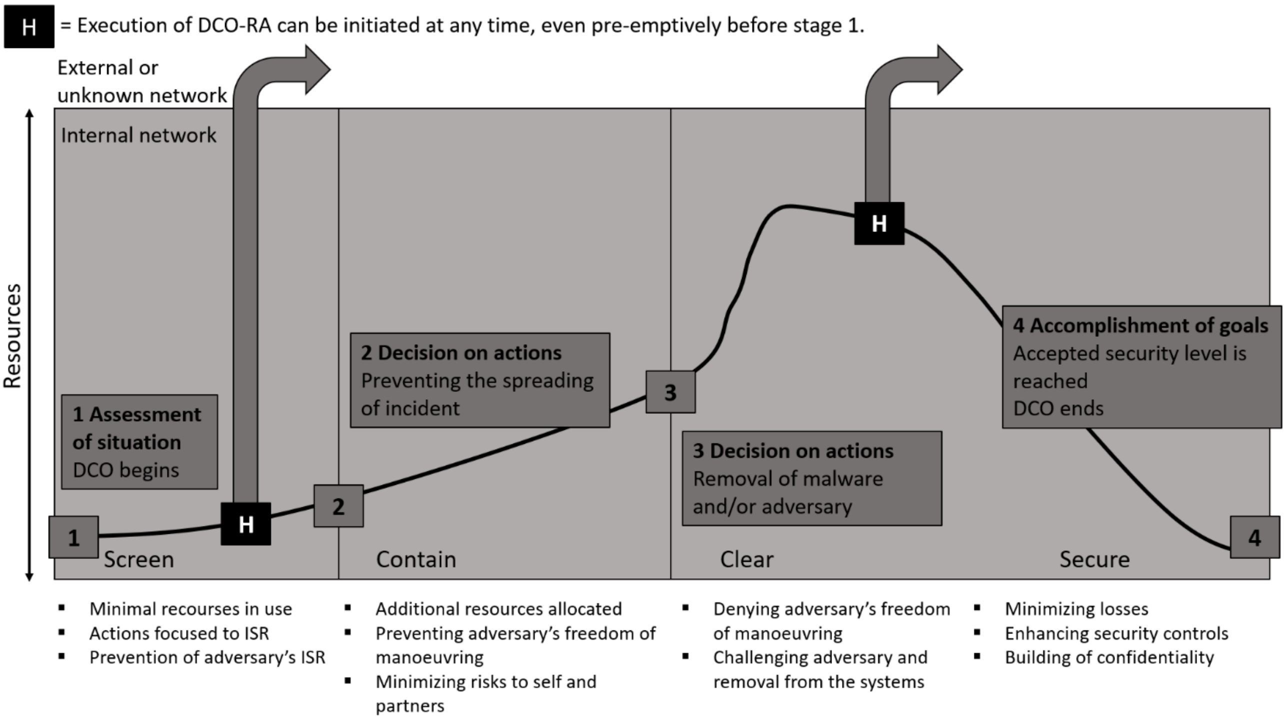

H = Execution of DCO-RA can be initiated at any time, even pre-emptively before stage 1.
External or unknown network
Internal network
Resources
1 Assessment of situation
DCO begins
2 Decision on actions
Preventing the spreading of incident
3 Decision on actions
Removal of malware and/or adversary
4 Accomplishment of goals
Accepted security level is reached
DCO ends
1
2
3
4
H
H
Screen
Contain
Clear
Secure
Minimal recourses in use
Actions focused to ISR
Prevention of adversary's ISR
Additional resources allocated
Preventing adversary's freedom of manoeuvring
Minimizing risks to self and partners
Denying adversary's freedom of manoeuvring
Challenging adversary and removal from the systems
Minimizing losses
Enhancing security controls
Building of confidentiality

Figure 11. Defensive Cyber Operations (Laari, 2019, modified)

As presented by Laari (2019) these DCO-IDM can be divided to four operational stages as shown in Figure 11. DCO-IDM operation is different from constantly ongoing DODIN operations as it has defined start and end points. It could be compered to be more like an incident handling situation in cyber security frameworks. As a process, it usually goes through the four stages (screen, contain, clear and secure), but as presented in the figure it can also initiate response actions which are more offensive by nature. Need for resources increases as process proceeds through the different stages. Handling operations like these are usually coordinated between different kind of cyber protection teams (CPT) like computer emergency response teams (CERT) and mission rapid response teams (MRRT) depending the number of needed resources and type of the operation (Ministry of Defence, 2016). Especially on the clearing and securing stages tasks can outsourced for the vendors.

Defensive Cyber Operations – Response Actions (DCO-RA)

Response actions are cyber operations "where actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system" (Joint Chiefs of Staff, 2018, p. 38). Operations like these are executed to unknown networks or identified networks used by adversary. Nature of these operations follows closely offensive cyber operations, but usually their execution time is shorter and operation is less pre-planned. One classic example of response actions is hackback as stated by Laari (2019). When the source of the attack is identified, sometimes the quickest solution to stop the cyber-attack is use of the deadly kinetic force (Vavra, 2019).

3.7.2 Offensive Operations

Offensive Cyber Operations (OCO)

Offensive cyber operations "are CO missions intended to project power in and through foreign cyberspace through actions taken in support of CCDR [combatant commander] or national objectives" (Joint Chiefs of Staff, 2018, p. 39). OCO could also be called as cyberspace attacks.

Typical OCO, according to Laari (2019), are missions to deny, manipulate or exploit the operational environment of adversaries. Denial missions can be split to three different effect levels: degrade, disrupt and destroy. These are presented in Table 2.

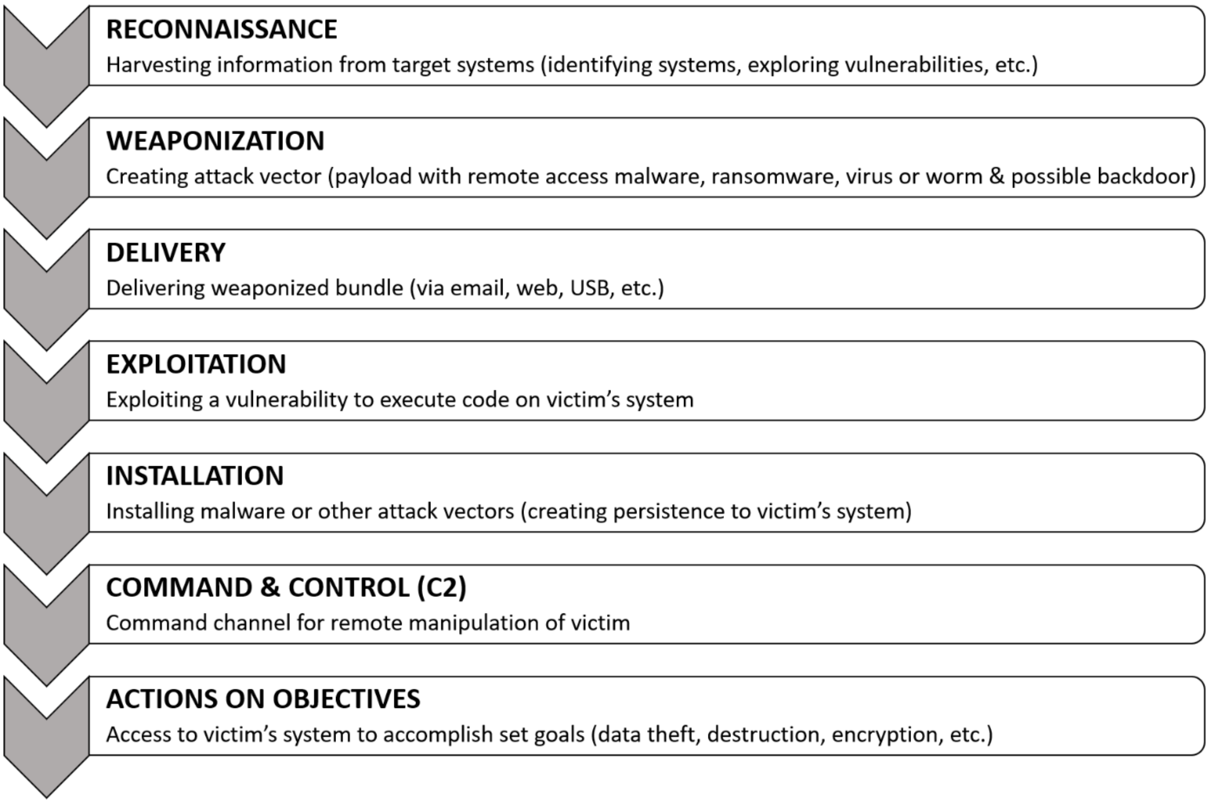
Table 2. Types of Denial Missions (Laari, 201)

ACTION	DESCRIPTION
Degrade	Deny access to partial operation of function in target for specified time.
Disrupt	Deny complete access for specified time.
Destroy	Deny access permanently until resource is replaced.

Manipulation missions are used when information or controls are wanted to be changed for deception or other reasons. An example of manipulation mission is Operation Orchard, where Israel allegedly manipulated Syrian's air-defence radars with feeding them false targets (Katz, 2010). Exploitation missions are military intelligence missions for information collecting. This kind of missions can be executed to support current missions or to prepare future missions (Joint Chiefs of Staff, 2018).

OCO are, like DCO, heavily depended from CTI's and ISR's capability to produce reliable information about adversaries' target systems. Information produced by ISR capabilities are used on tactical and operational level of planning and decision making (Joint Chiefs of Staff, 2018).

Planning and executing of offensive cyber operations follow stages presented in the Lockheed Martin's Cyber Kill Chain (Figure 12) or at least is refined form of it (Brantly & Smeets, 2020). In a military context moving from Cyber Kill Chain's stage to another is a decision point where continuation and direction of the operation is depending from the legislation of a state, especially if the question is about offensive actions. OCO are usually under oversight of the chain of command or other bureaucratic dependencies, as noted by Brantly and Smeets. This is because of their hostile and even possible destructive nature which calls for strict consideration of rules of engagement (Joint Chiefs of Staff, 2018).



RECONNAISSANCE
Harvesting information from target systems (identifying systems, exploring vulnerabilities, etc.)

WEAPONIZATION
Creating attack vector (payload with remote access malware, ransomware, virus or worm & possible backdoor)

DELIVERY
Delivering weaponized bundle (via email, web, USB, etc.)

EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

INSTALLATION
Installing malware or other attack vectors (creating persistence to victim's system)

COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES
Access to victim's system to accomplish set goals (data theft, destruction, encryption, etc.)

Figure 12. Lockheed Martin's Cyber Kill Chain (Lockheed Martin, 2011, modified)

Steps presented in the Cyber Kill Chain are usually divided to three separate activities in military operations: Digital network intelligence (DNI) provides information of specific target system. Operational preparation of environment (OPE) improves own defenses or creates attack vectors and needed cyber weapons for launching an attack. Computer network attack (CNA) launches the offensive actions against the targeted network or system (Laari, 2019).

Cyber Weapons

Prunckun (2018) describes weapon as an object that is meant to cause harm. This is true also for digital weapons even when they are meant to be less lethal than their real-world counterparts. Cyber weapons, as stated by Prunckun, can be software or hardware based. Software based are typically more complex malicious programs (malware, worm, virus, etc.) utilizing vulnerabilities in different kind of systems. Hardware based cyber weapons use some electronic device as an attack platform. Prunckun mentions one example of these to be a keylogger used to monitor input between keyboard and computer.

It is reasonable to assume that every capable nation is building their own cyber weapon arsenal as a part of their offensive capabilities. As stated by James McGhee (2016) nations may have these cyber weapons “on the self”, but using them is not so straight forward. This is because the situational awareness and knowledge from target systems increases to critical role. Timeline needed for planning and executing OCO depends from the end goals of the operation. A long-term undetectable espionage operation is much more difficult to plan and execute than for example a destructive operation (Hayden, 2016).

Cyber Weapons are not solely created by nation-state actors, as claimed by Prunckun (2018), even civilians and criminals build cyber weaponry to be sold in malware marketplaces. This makes it easier for both criminal and warfare actors when a complete cyber weapon can simply be purchased to be used against a targeted system without the need for know-how or long timespan to research and build one.

Often discussed question regarding a cyber weapon arsenal is its nature as a deterrence. But as we have not yet seen cyber weapon so horrendous, that it could be the digital nuclear weapon of cyberspace the deterrence created by cyber weapons is unclear at best, like noted by Chen and

Dinerman (2016). This, of course does not mean one could not be built in the future, so updating international laws to meet today's challenges and pre-emptive regulation of cyber weapons should be taken more seriously.

3.7.3 Information Operations

One of the currently used concepts of information warfare is presented in Figure 13. As stated before, different nations have different definitions for information warfare and information operations executed in cyberspace so the definition and different types of operations is broad.

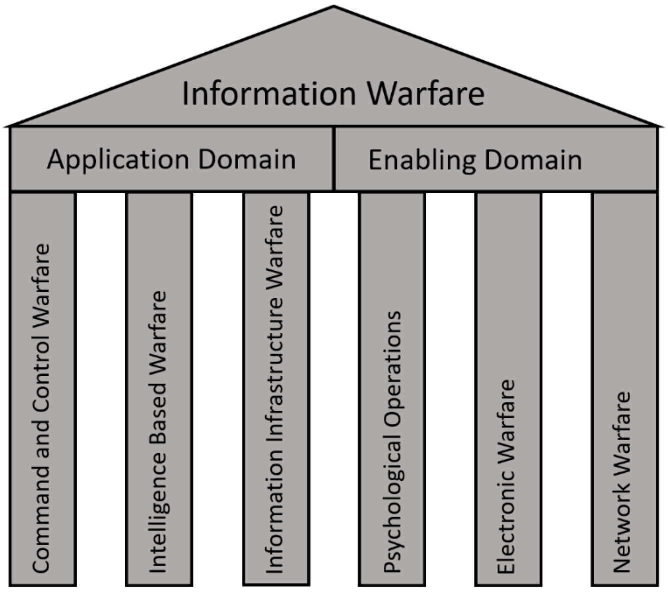


Figure 13. Application and Enabling Domains of Information Warfare (van Niekerk & Maharaj, 2010, modified)

Probably currently the most spoken part of information warfare in public discussion is information influencing operations. These are operations which, like the name suggest, are targeting influence to people's opinions and attitudes towards some specified agenda. For this Kari (2018) discusses the three often wrongly used terms of information influencing; propaganda, disinformation, and misinformation. Propaganda is spreading of some specific agenda. The term is usually understood as a negative thing, but it does not necessarily have to be done in malicious purposes, as proposed by Kari, it is just meant to affect opinions. Disinformation is knowingly and intentionally created false information. Misinformation is intentional or unintentional spreading of false information.

Cyberspace and its global presence have opened up new more effective and cheaper ways for a state to interfere to another state's internal politics and affairs. Examples of these are presented by Aro (2019) in her book regarding recent influence operations run by Russia and pro-Russian actors. Among other things, Aro discusses about "troll factories" where the name refers to internet trolling. Trolling is a slang word for internet phenomenon of "the act of leaving an insulting message on the internet in order to annoy someone" (Cambridge University Press, n.d., Definition 1), but the term is used more widely regarding information influencing. These so-called troll factories are nation-state sponsored and controlled internet companies where employees create disinformation campaigns targeted to other states as presented by Aro. Russia has been alleged to using these troll factories as a part of its influence operation of interfering with the United States Presidential elections in 2016 (Mueller, 2019; Bowen, 2021). Mueller (2019) states in the report how this offensive influence operation was also supported with other offensive cyber operations (mainly hacking) by Russian Main Intelligence Directorate (GRU) and Federal Security Service (FSB).

Revealing of attack as a strategy

One important aspect of information operations, which also affects the reliability of data collection of this thesis, is the national strategy of information sharing when it has been a victim to an offensive cyber operation. Why the victim chooses to share or not to share information and how much information it chooses to share? Baram and Sommer (2019) discuss this in their article about different information strategies for a nation when it has been targeted by a detected cyber-attack. The process chart of decision making is presented in Figure 14.

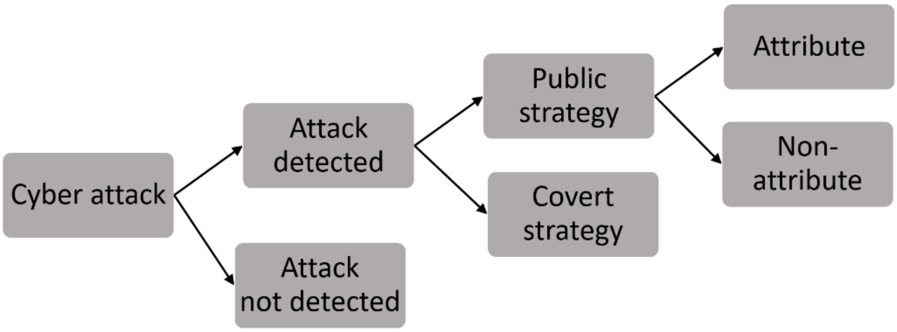


Figure 14. Victim's Strategies During a Cyber Attack (Baram & Sommer, 2019, modified)

The process chart is pretty straight forward. If the attack is not detected, there is nothing to decide. When the attack is detected, the first decision must be made if the covert strategy is chosen or if the occurred attack will be made public.

In this decision-making step, Baram and Sommer (2019) proposes four different strategies for victim to choose:

- Pointing finger, the victim reveals that attack occurred and names the suspected attacker.
- Admitting injury, the victim discloses that an incident occurred, but no-one is blamed for the attack.
- Revealing damage, the victim discloses incident which caused a damage, but denies it being result of hostile actions.
- Maintaining ambiguity, the victim denies any damage or attack has occurred.

For choosing the covert strategy Baram and Sommer (2019) identified two possible reasons: safety of intelligence sources and preventing escalation. Both of these assumptions are reasonable. If the victim does not have the technical capabilities for detecting the intrusion, the tip could come from an intelligence asset or from a friendly intelligence service as happened in 2013 when severe intrusion by the Russian nation-state actor was discovered from the Finnish Foreign Ministry's data network. The tip from the ongoing intrusion was given by an undisclosed outside actor. (YLE, 2014; YLE, 2017) Preventing escalation of ongoing conflict could come to question if there is a large difference in victim's and attacker's capabilities. As a third option, not identified by Baram and Sommer, the author suggests the interest of not to reveal one's own technical detection capabilities and to let the attack continue as it is being monitored in a more controlled environment.

According to Baram and Sommer (2019), when the occurred attack is decided to made public, the victim usually has one of the three motivations; name and shame, avoid humiliation, and show of strength. In name and shame the main challenge is the anonymous characteristic of cyberspace, so a decision could be done without full confidence and technical evidence. By Baram and Sommer, a classical explanation for this could be shaming the aggressor in the eyes of the international community. Depending from the severeness of the occurred incident, one reason to reveal the attack is proactive damage control. Not disclosing an attack could be a humiliation if it is revealed by a third party or by the attacker. The third suggested motivation could be victim's will to show its technical capabilities or issue a warning of retaliation to the attacker.

From the viewpoint of the aggressor, the situation is a bit different as stated by Baram and Sommer (2019). Usually, a nation executing an offensive cyber operation wants it to be a covert or clandestine operation, at least the technical part of the attack. The sole reason for the attacker to reveal OCO afterwards would be humiliation of its target if the attacker is not worried about any retaliation actions. In many cases, any detected ongoing OCO are failed operations.

3.7.4 Cyber Intelligence

Cyber intelligence is done by any available intelligence methods to support cyber operations as stated by Laari (2019). Cyber intelligence differs from traditional intelligence as it is done solely in cyberspace. It utilizes different information collection methods of traditional intelligence from overt and covert sources while enriching the products of traditional intelligence (Seedyk, 2018). The methods can be classified for several ways dividing those to even more specific data types. One common main classification is presented in Table 3. Classifications have been evolving during the years and also different actors use different kinds of classifications.

Table 3. Classification of Intelligence Collection Methods (Clark, 2014; Seedyk, 2018)

ACRONYM	DESCRIPTION
HUMINT	Human Intelligence
SIGINT	Signals Intelligence
IMINT	Imagery Intelligence
GEOINT	Geospatial Intelligence
OSINT	Open Sources Intelligence
MASINT	Measurement and Signature Intelligence
ACINT	Acoustic Intelligence
TECHINT	Technical Intelligence
MEDINT	Medical Intelligence

While cyber intelligence usually is mostly consisted from signals intelligence, but also open sources intelligence is a huge information source in today’s digitalized society. Omand (2016) claims, that over 40 % of worlds population has nowadays access to the internet. This has introduced pressure to increase mass surveillance in the digital realm. Omand makes a valid concern of how the vast amounts of collected data could be kept out of reach of misuse and exploiting.

While mass surveillance is the one probably most talked topic of intelligence collection, it has limited use in military perspective. To support and protect cyber operations military commanders needs near real-time analysed intelligence data for the base of decision making. The data are also needed to locate and identify targets as well to protect one's own communication methods and weapons systems (Omand, 2016). Recent example of cyber intelligence's produced data usage is from Ukraine where dating app's (e.g., Tinder or Grindr) location data has been used to geo-locate Russian troops (Fabiani, 2022; Elgueta, 2022).

3.7.5 Cyber Espionage

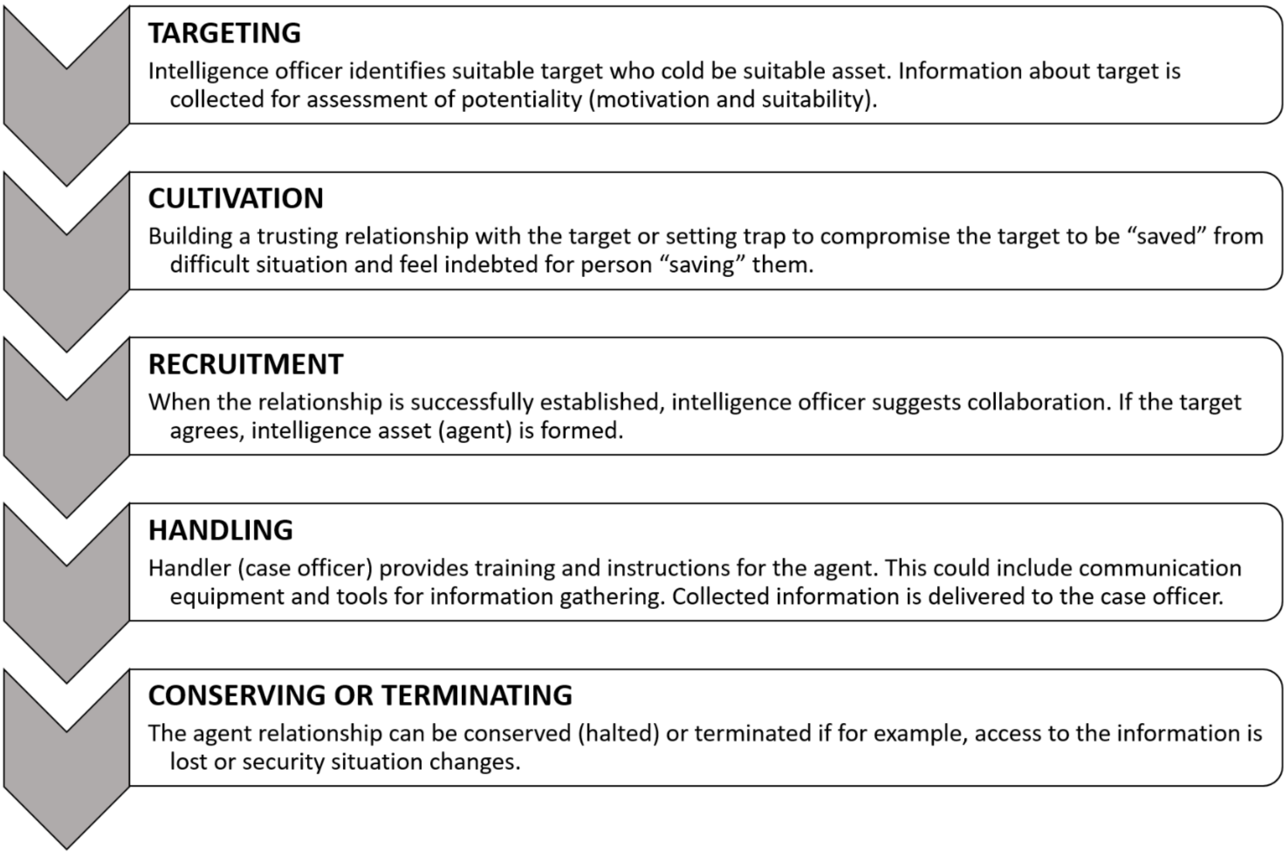
Cyber espionage is a sub-category of intelligence operations performed in cyberspace. Cyber espionage or cyber exploitation operations are clandestine form of intelligence and offensive cyber operations. As pointed out by Clark (2014), clandestine operations must not be confused with covert operations. Covert operations leave a room for deniability, so the target can not specify the source even when it knows about the operation. In a clandestine operation the target is not suppose to be aware that any operation was executed. These type operations are usually run by foreign intelligence agencies and military intelligence units or their proxies (Maurer, 2018).

World's rapid digitalization has brought security and intelligence agencies to critical period of adapting new tactics for cyberspace (Omand, 2016). Cyberspace, and its anonymizing nature creates new kind of challenges and possibilities, depending whose (own counter-intelligence or foreign intelligence) espionage operations are being examined.

Traditionally, according to Weissbrodt (2013), espionage operations have relied on spies or agents operating in foreign nations. These operations have been run under diplomatic covers as well infiltrating with non-official cover. This has set some natural boundaries for the states. Too keen foreign agents can be revoked from their diplomatic status and sent back home, even possibly as *persona non-grata*. The bolder ones operating with non-official cover can be tried in the court of law from espionage. Essence of cyberspace has removed these restrictions with plausible deniability and sanctions being less harsh if the digital spy ever gets caught (Weissbrodt, 2013).

Cyberspace and especially social media have made identifying suitable targets to be used in espionage easier. Traditionally recruitment of spies as part of human intelligence can today begin in cyberspace. Estonian Foreign Intelligence Service (2022) has released steps for agent recruitment known to be used by the Russian military intelligence service (GRU), Figure 15.

Even when cyberspace has made finding candidates easier, cyber espionage operations are not depended from agent networks like in traditional espionage. Cyber espionage operation can be fully performed by hacking, resulting in a data breach of the information system (Estonian Foreign Intelligence Service, 2022). Operations like these usually follow the same methods introduced in chapter regarding offensive cyber operations. This kind of perpetrators are typically called as advanced persistent threat (APT) actors when operating in cyberspace (Stech & Heckman, 2018). The APT actors and how they are identified will be discussed in a more detail in the chapter focusing to different actors monitored in the Ukrainian cyber-theatre.



TARGETING

Intelligence officer identifies suitable target who cold be suitable asset. Information about target is collected for assessment of potentiality (motivation and suitability).

CULTIVATION

Building a trusting relationship with the target or setting trap to compromise the target to be "saved" from difficult situation and feel indebted for person "saving" them.

RECRUITMENT

When the relationship is successfully established, intelligence officer suggests collaboration. If the target agrees, intelligence asset (agent) is formed.

HANDLING

Handler (case officer) provides training and instructions for the agent. This could include communication equipment and tools for information gathering. Collected information is delivered to the case officer.

CONSERVING OR TERMINATING

The agent relationship can be conserved (halted) or terminated if for example, access to the information is lost or security situation changes.

Figure 15. Recruitment of an Agent (Estonian Foreign Intelligence Service, 2022, modified)

The APT actors can be targeting everything from single individuals to companies, organizations and other nation-state actors. Cyber espionage is one of those actions known to be outsourced for organized-crime groups to add more deniability for the nation-state actors ordering the operations (Akoto, 2022). It is also important to note, that cyber espionage is not done only by the nation-state actors with their proxies, but also by private companies. Cyber espionage is a modern-day tool used as well in a corporate espionage (Morag, 2014).

While cyberspace has opened ways for more intrusive intelligence and espionage methods, Quinlan (2007) proposes the need for regulating intelligence community with similar treaties than laws of war. Proposed treaties by Quinlan are *jus ad intelligentiam* (rules for intrusive capabilities) and *jus in intelligentia* (circumstances when use of specific capabilities could be authorized).

4 Different Actors in the Ukrainian Theater

As stated before, connecting the cyber-personae to real world person or persons is challenging. This is because of the nature of cyberspace of which anonymity and deniability is a crucial part. It makes identifying different actors on cyberspace difficult and resource consuming (Romanosky & Boudreaux, 2019). Identifications are done by both, intelligence agencies and private security vendors as part of the cyber threat intelligence. While not reaching total certainty of actor's true identity, usually a reasonable confidence is enough, especially if different independent organizations make same conclusions in their own investigations (Romanosky & Boudreaux, 2019).

There are multiple organizations that are investigating APT actors and there is no common naming scheme for these groups. This makes it a bit challenging to follow which APT group was responsible of an attack since all organizations are using their own names for each APT actor, as stated by Romanosky and Boudreaux (2019). Sometimes it can be hard to follow which APT was behind of which attack. This thesis uses mainly APT names given by the CrowdStrike, but if one is not available, some other vendor's (e.g., Mandiant, Microsoft, ESET, FireEye, Kaspersky, Cisco Talos, Dell Secure Works, Symantec, U.S. National Security Agency, U.S. Department of Homeland Security, or a national CERT, to name a few to clarify the complexity of naming scheme) given name will be used instead. Appendixes one to three presents tables of APT actors whose operations have been monitored in Ukraine and aliases (if any) linked to those actors.

Sometimes separating nation-state sponsored the proxy organization from nation-state actor is difficult and not even meaningful. In such cases, this thesis links proxy organization to the nation-state actor as for this study's purposes it is not as much relevant to be certain of *who did* something, but *what was* done.

Identifying who was behind the cyber-attack is a challenge requiring a lot of intelligence work. Information is collected from multiple sources, and when these are connected and analyzed, the picture of the perpetrator starts to take shape. To help CTI, there are some public frameworks available, like MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework (MITRE, 2021). When CTI of APT actors was taking it first steps, Bianco (2014) came up with model of challenge level for different kind of technical IOCs as the part of identification of the threat actors. Bianco's model is presented in Figure 16.

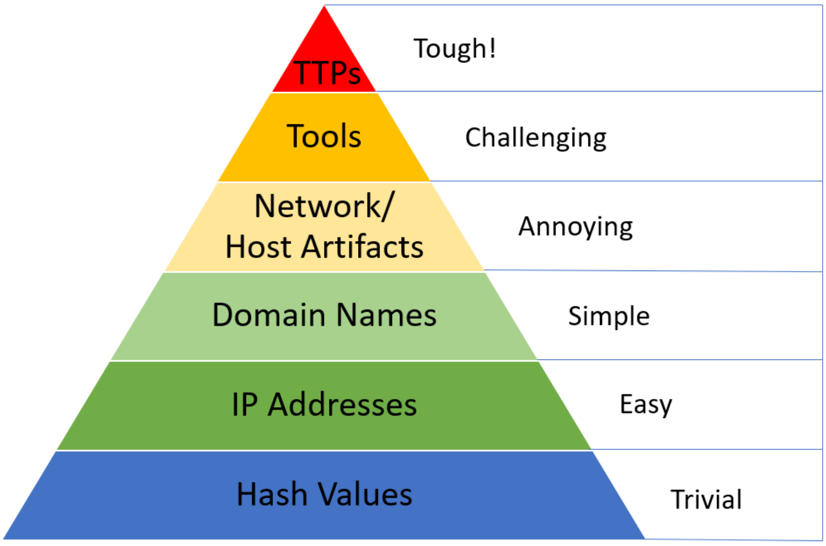


Figure 16. The Pyramid of Pain (Bianco, 2014, modified)

Sometimes these can be a really obvious and simple things like ones related to the actor's behaviour. If the attacks are constantly done only during the office hours of a nation's agencies (McWhorter, 2014) it might be the first clue, but of course in clues like this possibility of deception and framing of another actor should not be ruled out. Or if an actor is constantly witnessed taking part in some specific political motivation (or propaganda), it can give clues of affiliation of the actor (Romanosky & Boudreaux, 2019).

Another way is to investigate the technical side of the cyber-attacks and the cyber weapons used in them. Linking the attacks can be done with a reasonable doubt when the tactics, techniques, and procedures (TTPs) are identified to match with some other investigated incident (Cybersecurity and Infrastructure Security Agency, 2021; MITRE, 2021). This is because humans have a tendency to do things with a familiar way with familiar tools. Another example of possible identification source is to look the base code of the cyber weapons. Sometimes cyber weapons use the same parts of the code or refined from some older version. This can sometimes to be used to identify and to create links between different actors when a nation-state has shared tools for their proxies (Mercer & Ventura, 2021). Even simple methods like collecting IP addresses, domain names or other indicators of compromised data of known APT actors, and command-and-control channels used by them, can help linking the actors (Romanosky & Boudreaux, 2019). Successful identification of APT actors is usually a combination of OSINT, SIGINT, and HUMINT, as stated by Romanosky and Boudreaux (2019).Figure 1

4.1 Russian State-Sponsored Actors and Pro-Russian Actors

When discussing about Russian state-sponsored actors, the cyber operations are usually attributed to four different agencies, the Russian Federal Security Service (FSB), Russian Foreign Intelligence Service (SVR), two branches of Russian General Staff Main Intelligence Directorate (GU) and Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM). These agencies are known to be targeting different sectors and lines of businesses with their attacks, and also their TTPs are a bit different from each other (Cybersecurity & Infrastructure Security Agency, 2022).

It is unclear how much joint directorship and information sharing Russia’s nation-state actors are internally having, but sometimes joint operations are detected. Joint operation group of Cozy Bear (SVR) and Fancy Bear (GRU) is usually called as GRIZZLY STEPPE (National Cybersecurity and Communications Integration Center, 2016; 2017). The APT groups introduced here are the “hacker teams”, but they are supported by multiple specialized units (e.g., in PSYOPS), as stated by Bowen (2021).

Organization chart of the Russian cyber units is presented in appendix 4. Information for creating the chart and present dependencies between different Russian nation-state actors is collected from multiple sources (Digital Security Unit, 2022; Muller, 2019; Office of Information Security, 2022; National Cybersecurity and Communications Integration Center, 2016; Estonian Foreign Intelligence Service, 2022; Bowen, 2021; United States district court western district of Pennsylvania, 2020; Security Service of Ukraine, 2021; Bowen, 2022).

4.1.1 Russian Federal Security Service (FSB)

Berserk Bear

The main APT team of the FSB is known as Berserk Bear. The group is typically targeting its cyber operations to Western energy companies. Typical aliases for Berserk Bear are Energetic Bear, Dragonfly and Crouching Yeti (Cybersecurity & Infrastructure Security Agency, 2022). Full list of known aliases is presented in appendix 1.

There are also other APT groups attributed to the FSB, but it is somewhat unclear if those are proxy organizations or another hacker teams inside the FSB.

Primitive Bear

Primitive Bear originally got its name in 2013 from displaying rudimentary techniques and the use of off-the-shelf tools. Since then, the group has evolved to be highly adaptive with the use of complex custom-made malware and has become a prominent actor on the field (Telsy, 2020). Primitive Bear is better known by one of its aliases, Gamaredon. Primitive Bear is allegedly attributed to the FSB as claimed by the Security Service of Ukraine (SSU) (2021).

Nowadays, Primitive Bear is believed to support other Russian APT groups by offering them services, and is questionable if it even is an actual group. The TTPs of Primitive Bear are different from other APT actors as it is not especially stealthy in its actions (Mercer & Ventura, 2021).

Venomous Bear

Venomous Bear is an APT group known to use sophisticated techniques and is notably good at operations security (OPSEC). The Venomous Bear is probably better known from its alias Turla, referring to Turla malware used in cyber espionage campaigns targeting often NATO, defence contractors and other similar sources for intelligence (Cybersecurity & Infrastructure Security Agency, 2022).

Venomous Bear is believed to be related to some Russian signals-intelligence organization (currently speculated to the FSB) and its TTPs are known to use hijacked satellite internet communications as command-and-control channels.

4.1.2 Russian Foreign Intelligence Service (SVR)

The SVR's highly sophisticated APT group is commonly known as Cozy Bear, with typical aliases APT29, Nobelium, Dark Halo and CozyDuke. The group is known from good OPSEC and limiting its digital footprint (Mandiant, 2022; Cybersecurity & Infrastructure Security Agency, 2022). Full list of known aliases is presented in appendix 1. Cozy Bear is known to be targeting critical infrastructure organizations.

A recent famous OCO executed by Cozy Bear was the SolarWinds case where the group was able to infiltrate to several organizations of the United States with supply-chain attack (Cybersecurity and Infrastructure Security Agency, 2021).

4.1.3 Main Directorate of the General Staff of the Armed Forces (GU)

The Russian military intelligence organization was formerly known as the Intelligence Main Directorate, whose GRU acronym is still commonly used while referencing the organization (BBC News, 2021).

85th Main Special Service Centre's (GTsSS)

The GRU's 85th Main Special Service Centre's military unit 26165 is called Fancy Bear (Bowen, 2021). Other typical aliases are APT28, Group 74, Sednit and Strontium. Full list of known aliases is presented in appendix 1. Usual targets of Fancy Bear are governmental organizations, militaries, NATO, critical infrastructure organizations, universities and other research institutes (McWhorter, 2014; Cybersecurity & Infrastructure Security Agency, 2022).

Main Centre for Special Technologies (GTsST)

The GRU's Main Centre for Special Technologies' military unit 74455 is usually called as Voodoo Bear, along with aliases Sandworm, BlackEnergy and Iron Viking (Bowen, 2021). Full list of known aliases is presented in appendix 1. Voodoo Bear is also known from targeting the critical infrastructure organizations, especially energy sector, but other known attacks have included financial sector organizations as well transportation systems (Cybersecurity & Infrastructure Security Agency, 2022).

Voodo Bear's TTPs are noticeably different from most of the other Russian nation-state actors. The group relies commonly to attacks with disruptive and destructive nature. These include distributed denial of service (DDoS) attacks and use of destructive wiper malware (Cybersecurity & Infrastructure Security Agency, 2022). NotPetya is one of the attacks with global effects attributed to Voodoo Bear (United States district court western district of Pennsylvania, 2020).

Ember Bear

Ember Bear is an APT group linked to WhisperGate wiper and tracked by Microsoft as DEV-0586 (Digital Security Unit, 2022), but it is a somewhat unclear if it is sub-group inside GRU's organization or nation-sponsored proxy. Several other APT actors have also been linked to Ember Bear, but it is still unknown if they are actually the same group or sub-groups controlled by Ember Bear. CrowdStrike (2022) suggests groups TTPs being similar with GRU's Voodoo Bear and Fancy Bear.

4.1.4 Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM)

Central Scientific Institute of Chemistry and Mechanics is a research institute under Russian Ministry of Defence which is known for destructive Triton malware attacks. The group is commonly known as XENOTIME (Cybersecurity & Infrastructure Security Agency, 2022).

4.1.5 Organized-Crime Groups & Other

There are several organized-crime groups working in as nation-sponsored actors or have publicly stated their support for the Russian war effort. In appendix 1 is a current list of pro-Russian actors monitored to run cyber-attacks in Ukraine during this year. A few of the more active and visible actors are introduced here.

Wizard Spider

Wizard Spider is an organized-crime group known for its malware and ransomware attacks and often known as Conti or TrickBot. The group is believed to operate with a sophisticated business-like organization structure with several dedicated subgroups from Saint Petersburg, Russia (SOCRadar, 2021).

According to SOCRadar (2021), the Federal Bureau of Investigation (FBI) has claimed the group having over 400 successful attacks all over the world, 290 of those in the United States. Typical targets for the group were government organizations, health care and various law enforcement agencies.

Wizard Spider's infrastructure was taken down 19th of May, 2022, according to SOCRadar (2022). Members of the ransomware group are believed to have join to other criminal groups. Before its takedown the group had own alleged data breach (Conti Leaks) by Ukrainian security researcher (Kovacs, 2022a). The leak revealed that the group was working on new version of the ransomware, now with firmware exploits (Kovacs, 2022c). The leak also suggested that the group could have connections to the FSB (Kovacs, 2022a).

InvisiMole

InvisiMole is an APT actor linked loosely to FSB's Primitive Bear and it possibly is a state-sponsored proxy. The group is usually engaging in cyber espionage activities with sophisticated and complex cyber weapons. According to Ilascu (2020), the security research has been able to link these cyber weapons used by the group back to the FSB's Primitive Bear. Though their targets and TTPs are noticeably different which leads to the assumption of them being two different actors. In some attacks, as claimed by Ilascu, InvisiMole has infiltrated the target network by using access gotten from Primitive Bear.

4.2 Ukrainian Cyber Defense Actors and IT Army of Ukraine

4.2.1 State Service of Special Communication and Information Protection of Ukraine (SSSCIP)

According to the website of the State Service of Special Communication and Information Protection of Ukraine is a defense and security agency whose main priority is to improve the cyber security of the nation. SSSCIP provides several different services to other government agencies as well to the armed forces (SSSCIP, n.d.-c).

One of the tasks of the SSSCIP is to run the national CERT as part of investigating and analyzing cyber threats. CERT-UA (n.d.) is working in co-operation with other national authorities and law enforcement agencies. They also issue warnings and releases IoC data to help public and private organizations to counter discovered cyber-attacks.

4.2.2 Security Service of Ukraine (SSU/SBU)

Security Service of Ukraine, as stated on their website, is an organization whose priorities are in protecting the statehood of the nation, counterintelligence, and counterterrorism activities. The agency is one of the many Ukrainian organizations responsible for countering the cyber security threats. The agency notes it is having a long time focus on countering hybrid warfare (Security Service of Ukraine, n.d.-a).

The SSU is also running 24/7 its own Cyber Security Situation Centre whose mission is to counter cyber threats from cyber intelligence to cyber terrorism. The center is also mentioned to run operational investigations for cyber threats and to conduct counterintelligence operations (Security Service of Ukraine, n.d.-b).

4.2.3 Cyber Police of Ukraine

The cyber police of Ukraine states being a part of the National Police of Ukraine, governed by the Ministry of Internal Affairs of Ukraine. On the webpage of the cyber police some of the law enforcement agency’s tasks are introduced to be combating cybercrime and informing citizens from emerging cyber threats caused by the criminals (Cyber Police of Ukraine, n.d.-a).

4.2.4 Defence Intelligence of Ukraine (GUR)

Defence Intelligence of the Ministry of Defence of Ukraine is one of the Ukrainian intelligence agencies whose responsibility is to collect and analyze information regarding “the defence, development of military capability, military and military-technical as well as cybersecurity areas” (Defence Intelligence of Ukraine, 2022).

Ukraine's Defense Intelligence Service (GURMO) Cyber Operations Unit

Offensive cyber operations of Ukraine’s military intelligence are run by a cyber operation unit, commonly referred as cyber unit or cyber team. By being an intelligence unit, its mission is intelligence gathering done by computer network exploitation (Lapienytė, 2022). Because of the clandestine nature of the organization, not much information is available regarding the unit though some of the OCOs claimed to be executed by the unit have been reported on the public websites. For example, cyber-attacks targeting the Russian gas company Gazprom on April 2022 have been attributed to the cyber unit by Carr (2022). Carr claims that the attacks were suggested to have kinetic results as the gas pipe ruptured and caught on fire. Though it is important to note that these claims have not been verified by any other sources. Jeffrey Carr is a known cyber security consultant, but his reliability as a source for this matter is severely questionable at best. These allegations could be fog of war by being Russian or Ukrainian propaganda as supporting a narrative seemingly benefitting both parties.

4.2.5 IT Army of Ukraine

Hacktivism as a phenomenon related to the Russo-Ukrainian war is discussed in this chapter’s subchapter 4.3, but IT Army of Ukraine is something we cannot ignore while introducing Ukrainian cyber actors. The IT army is a totally new concept and it is a bit difficult to classify it by any existing definition of cyber warfare participants.

The formation of IT Army of Ukraine takes place somewhere between February 24 and 26 of 2002 when co-founder of several cyber security companies, Yegor Aushev, presented the idea of using volunteers as a base for creating a cyber army to Minister of Digital Transformation, Mykhailo Federov (Burgess, 2022a). Aushev was already assembling volunteer cyber army by the request of

Ukrainian Defense Ministy official according the interview Aushew gave to the Reuters on February 24 (Schectman & Bing, 2022). The idea was to form a cyber military force that would divide to defensive unit and offensive unit. The interview claims that the offensive unit was planned to help Ukrainian intelligence community by executing offensive cyber espionage operations. Ukrainian Ministry of Defense did not want to comment on the matter (Schectman & Bing, 2022).

On February 26 the recruiting of volunteers began at Fedorov's Telegram channel as a call for international mobilization of IT specialists. Just on a single day over 175,000 volunteers had subscripted to the channel (Burgess, 2022a). According to Burgess, also the tasks and targets for the IT army are given via multiple Telegram channels. The number of volunteers has been fluctuating, but typical guess is around 300 000 which is loosely based on the number of the subscriptions to the Telegram channels (Stokel-Walker & Milmo, 2022).

The IT Army has been participating in several offensive cyber operations targeting Russia. These attacks include DDoS attacks and more exploitative and sophisticated cyber-attacks (Stokel-Walker & Milmo, 2022; Burgess, 2022a). Soesanto (2022) who has investigated IT Army in more detail raises an interesting remark of IT Army's structure; Soesanto suggests IT Army being two different offensive units. The first one is the global volunteer collective where any one can participate and TTPs are mainly consisted from DDoS attacks targeting critical infrastructure affecting civilians. The second part is suggested to be a more in-house unit where more sophisticated attacks are coordinated and executed by Ukrainian intelligence and defense personnel alongside with some of the volunteers. As Soesanto explains, these both units conduct offensive operations.

This alone, as also suggested by Soesanto (2022), brings up a severe concern for the ethicality of recruiting civilians to a para-militaristic IT Army performing hostile acts. Because of its unclear nature, how should it be considered when IHL and LOAC are interpreted in cyberspace? Especially when the group is, in addition to military targets, intentionally targeting critical infrastructure as well and that way potentially causing unnecessary harm for civilians. This kind of actions are unquestionably contradicting the IHL and the LOAC and should be condemned by the international community. Though the author suggests that international community is most likely currently focusing on ending the humanitarian crisis caused by the war instead of strictly monitoring violations of IHL and LOAC that are not directly affecting the number of casualties.

Another question is how these volunteers should be interpreted as it is difficult to assess them as civilians, but clearly, they are also not military personnel. Status of this kind unlawful combatants is discussed a bit earlier in the chapter focusing the international laws. In any case, this will likely to have some impact to how these laws and treaties are interpreted and amended in the future.

4.3 Private Companies

Microsoft, ESET Security, Starlink, etc.

The Russo-Ukrainian war has been a good example and really underlines the importance of co-operation between government agencies and private vendors regarding the cyber defence. Even when the nation-states have their own agencies and armed forces with cyber security specialists, their resources are still limited and tasked to defend their own critical networks. When there is a sudden increase of resource needs for experts and specialists to defend civilian agencies and critical infrastructure it is natural to turn to the private companies (Garson & Furlong, 2022).

During the war we have been witnessing several companies operating as part of the Ukraine's cyber defence, helping to mitigate constant cyber-attacks. One noteworthy example of this is Microsoft which has contributed publicly and released information regarding at least some of the attacks and cyber weapons used by the Russian forces (Microsoft Security, 2022; Microsoft, 2022). Sole example of these efforts is when Microsoft used a court order to take down 7th of May 2022 seven domain addresses allegedly belonging to Fancy Bear (Kovacs, 2022b). The domains were allegedly used to target Ukrainian organizations, including media companies.

Another source is cyber security company ESET which has released several technical analyses of the witnessed new cyber weapons. ESET has been in a frontline to detect and analyse new cyber weapons used by the Russian APT actors and helped to publish IOC data regarding them. This helps to counter and detect these attack attempts (ESET, 2022a; 2022b; 2022c).

When Russian forces started to disrupt and destroy land-line based communications infrastructure with kinetic strikes and cyber-attacks, private company, SpaceX volunteered to provide its satellite communications network and started to ship thousands of needed ground-station equipment to

Ukraine (Zhadan, 2022a). This has helped both civilians and armed forces to have working communications on the battlefield and other targeted areas where all land-based and mobile-based communication networks are down. SpaceX is told to also counter cyber-attacks on Ukraine's networks as claimed by Zhadan.

The list presented here is not meant to be comprehensive; there are many other private companies providing support to Ukraine. The companies presented here were selected due to their visibility on the media.

4.4 Hacktivists

Anonymous, Network Battalion 65, Belarusian Cyber Partisans, Cyber Defence, etc.

Probably one of the most interesting aspects of Russo-Ukrainian war is the rapid increase of the ideological hacktivism. Several hacktivism groups with speculated numbers of over 400,000 participants have entered the cyber battlefield (Shore, 2022). This is the first time when we have witnessed civilians from all over the world taking part in a war with two conflicting nations (Horejsi & Pernet, 2022; Delcker, 2022). It has been speculated that it could be the result of people finding reactions of their own nations to be too slow and in people's mind the ongoing war is not considered to be a just war as the conflicting sides are an attacking military super power and a small European country being invaded (Delcker, 2022).

Even though nations are recommending their citizens to abstain from taking part to the hacktivism against Russia, there still seems to be at least some level of silent acceptation for the hacktivism efforts. The only country to actively support and to call new hacktivists to participate is currently Ukraine (Peterson & Cimpanu, 2022). These volunteer hackers are coordinated in a group known as IT Army of Ukraine like stated earlier on this chapter. (Burgess. 2022).

Hacktivists, known as Anonymous, have been able to steal gigabytes of information from the Russian government agencies, several companies and military research institutes (Pitrelli, 2022; Lee, 2022). Also, Russian State's "propaganda wall" has been breached for several times to show Western news of the war to Russian people, or sometimes just to try to enlist some solidarity for

Ukraine (Pitrelli, 2022). To prevent military troop movements also attacks against railroad networks have been somewhat successful causing at least some delays for the troop movements (Sly, 2022). Several DDoS attacks has also been seen to affect and to try to disturb the everyday life in Russia (Pitrelli, 2022; Burgess, 2022b).

5 Summary of Russo-Ukrainian Cyber Warfare during 2010-2021

The Russo-Ukrainian war or at least hostilities began with the illegal annexation of Crimea on 2014 when Russian forces occupied the Crimean Peninsula from Ukraine and escalated when war in Donbas broke out a few months later. Russian cyber operations targeting Ukraine started long before the occupation and increased in late 2013. This could loosely be used as a reference point for when the of cyber warfare between the Russian Federation and Ukraine began. Most of the major cyber-attacks targeting Ukraine have happened since then (Przetacznik & Tarpova, 2022).

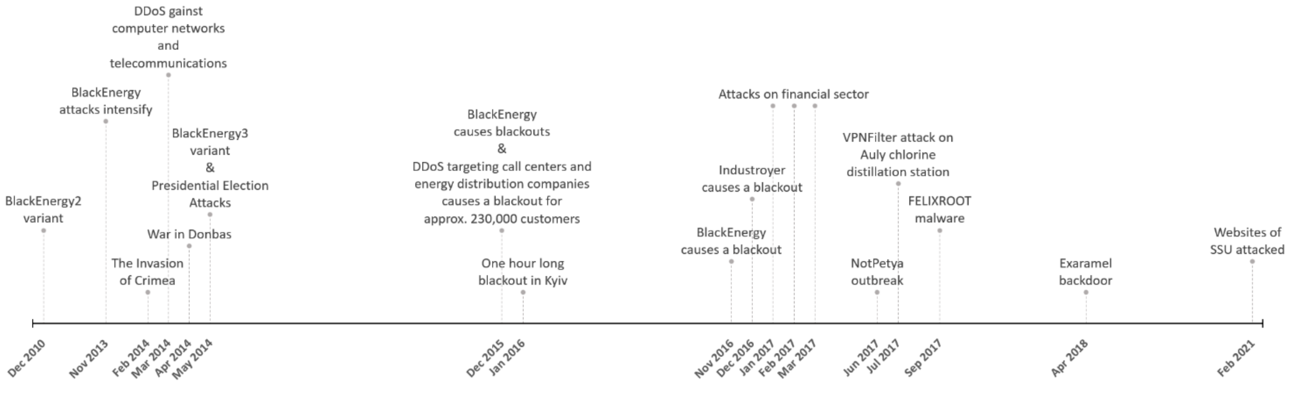

DDoS gainst computer networks and telecommunications
BlackEnergy attacks intensify
BlackEnergy3 variant & Presidential Election Attacks
BlackEnergy2 variant
War in Donbas
The Invasion of Crimea
BlackEnergy causes blackouts & DDoS targeting call centers and energy distribution companies causes a blackout for approx. 230,000 customers
One hour long blackout in Kyiv
Attacks on financial sector
Industroyer causes a blackout
BlackEnergy causes a blackout
VPNFilter attack on Auly chlorine distillation station
FELIXROOT malware
NotPetya outbreak
Exaramel backdoor
Websites of SSU attacked
Dec 2010
Nov 2013
Feb 2014
Mar 2014
Apr 2014
May 2014
Dec 2015
Jan 2016
Nov 2016
Dec 2016
Jan 2017
Feb 2017
Mar 2017
Jun 2017
Jul 2017
Sep 2017
Apr 2018
Feb 2021

Figure 17. Timeline of Major Cyber Warfare Events 2010-2021 (Cherepanov & Lipovsky, 2018b; Przetacznik & Tarpova, 2022; F-Secure Labs, 2019)

Some sources have calculated over 900 cyber-attacks happening after the cyber warfare between these two countries broke out a decade ago (Rousku et al., 2022). To summarize the events before the 2022's invasion began some of the most noteworthy cyber-attacks have been chosen as examples. Some of these are presented on a timeline in Figure 17. These chosen incidents were selected because of their global scale effects and some because they raise a legitimate concern of ethics and tactics used in cyber warfare. As suggested in the chapter discussing international humanitarian laws, these attacks, done during the time between the occupation and the current invasion, are falling outside of the laws of armed conflict and probably should be considered as cyber sabotage. The current invasion on the other hand is an act of war and any offensive cyber operation should be considered under the LOAC as well the IHL.

The cyber-attacks discussed in this chapter are nowadays attributed to GRU’s Voodoo Bear, but they are discussed here by the APT group names and malware names (BlackEnergy, TeleBots, GreyEnergy) used at the time of the cyber-attacks.

5.1 Cyber-Attacks Against Energy Sector

BlackEnergy & GreyEnergy

The first variant of BlackEnergy trojan malware surfaced somewhere around 2007 and was actively sold among the Russian criminal underground (F-Secure Labs, 2019). Mid-2014 a third variant of the malware surfaced and according to F-Secure Labs’ (2019) analytics was customized for targeting Ukrainian government agencies. Most likely it was spread by phishing emails which is used as a method in today’s attacks as well. BlackEnergy malware was used as an intrusion vector and a command-and-control channel. The attacks themself were utilizing other more destructive malware like KillDisk and later on with GreyEnergy malware accompanied by Moonraker Petya (Cherepanov, 2018).

The BlackEnergy attacks in Ukraine were mainly targeting companies in the energy industry. According to Cherepanov and Lipovsky (2018b) BlackEnergy’s attack on December 2015 was a first ever cyber-attack to cause blackout, rendering almost 230,000 customers without energy. During the same time period the same group, but now with GreyEnergy alias, was conducting similar attacks in Europe and later on continued in Ukraine. During GreyEnergy’s attacks on Ukraine a new attack-vector was introduced to side with spear phishing. The target of the group was also to compromise web-facing servers as a way in. (Cherepanov & Lipovsky, 2018b). Also, the malware was developed to be more sophisticated and it was deployed in two stages: A lightweight GreyEnergy Mini working as a backdoor and the actual main module. The malware itself was made modular, so it was possible to add new functions to it after installation (Cherepanov, 2018).

Industroyer and Exaramel

On December 2016 another de-energization of electrical substation occured as result of a cyber-attack. This is the first known time when malware was specifically designed to attack ICS used in electrical substations, especially to operate circuit breakers and protection relays of a substation (Cherepanov, 2017). The malware utilizing itself was constructed from several modules including main backdoor (core component of the malware) with additional backdoor, additional tools (Denial of Service tool), launcher, data wiper and four different payloads (for different industrial protocols). The Industroyer was designed to take control of the electrical substation, de-energize it and maximize the blackout time by executing a destructive data wiper (Cherepanov, 2017).

The attack was never directly attributed to BlackEnergy/TeleBots group, but Industroyer shared part of the code base of BlackEnergy, NotPetya, GreyEnergy and Exaramel malware (Cherepanov & Lipovsky, 2018a; 2018b). Exaramel backdoor discovered on April 2018 was an upgraded version of Industroyer (Cherepanov & Lipovsky, 2018a).

5.2 Destructive Fake Ransomware Attacks

TeleBots & NotPetya

A group called TeleBots targeted multiple Ukrainian financial sector's organizations with destructive malware attacks by using KillDisk malware similarly as they did when using BlackEnergy alias last year. TTPs of the group continued to use spear phishing emails, but now included also malicious websites to their toolset. The targeted victims were lured to an infected website ("watering hole") to download updates for tax and accounting software (Nakashima, 2018).

One month after North Korean WannaCry caused damage to ICT systems in over 150 countries, TeleBots targeted Ukrainian financial sector and ICS networks with NotPetya malware. NotPetya was made to look like ransomware, but it was lacking any functions to decrypt the systems files (Nakashima, 2018).

NotPetya is sophisticated and complicated set of tools which are utilized to move in a network and to infect discovered machines. One of the attack methods used in NotPetya was a modified version of EternalBlue exploit and other zero-day vulnerabilities (Thomson, 2017). Even though the malware was targeted to Ukraine, it started to spread all over the world infecting networks of large companies. Probably one of the largest victims of the malware was the shipping company Maersk (Thomson, 2017). The financial damages made by NotPetya is difficult to estimate, but it has been called “the most devasting cyber-attack in history” (CBS News, 2018) and has been estimated to have caused damages of total cost of over $10 billion (CBS News, 2018).

Experts have been speculating past five years if NotPetya’s spread all over the world was accidental or was it done intentionally by the Russian GRU. Microsoft (2022) suggests in its early report analyzing the events of the ongoing war that this time Russia’s destructive cyber-weapons have been much more carefully created to target specific networks and cannot move from computer domain to another. This prevents used cyber weapons from spreading outside of the Ukrainian networks (Microsoft, 2022). This might be an indication of “lessons learned” from NotPetya’s catastrophic effects to international companies (Kaminska et al., 2022). Though these newly used cyber weapons are, according to Microsoft, much more outspread and sophisticated than many of the reports are letting on.

5.3 Ukrainian Cyber Operations

The Ukrainian OPSEC has been excellent regarding their cyber operations and not much is known about them in public. Only one offensive cyber operation has been attributed to Ukraine before 2022.

According to ESET (2016) a cyber espionage operation (Operation Groundbait) was launched against high political targets in Donbas region in May 2016. The operation was run as a classic spear phishing campaign targeting individuals with customized email lures with malicious attachment. The used malware had not been detected earlier even when ESET’s researchers claim it had been active the past eight years. This reveals Ukraine having at least some capability and know-how to build cyber weapons.

There have been several cyber-attacks performed by Ukrainian hacktivist groups whose affiliation level to the Ukrainian nation-state is unknown. One of the most actively attributed has been a collective of several hacktivist groups known as Ukrainian Cyber Alliance which has been claimed to have executed several hacks and data leaks against Russian and Eastern-Ukrainian targets (in Donetsk and Luhansk) (Censor.net, 2016). For example, on May 9th they launched multiple cyber-attacks to deface websites of nine different Russian private military companies and propaganda sites of self-claimed Donetsk People's Republic. Defacements included also a video message (Censor.net, 2016).

6 Cyber Operations Supporting Traditional Warfare in 2022

Details of all observed major cyber-attack launched by the Russian Federation or Pro-Russian actors are itemized and explained by the author in more detail in appendix 9. Types and number of these cyber-attacks are presented in Figure 18. The figure shows that most of the reported cyber-attacks have been phishing attempts for gaining initial footholds to computer systems or to launch destructive attacks.

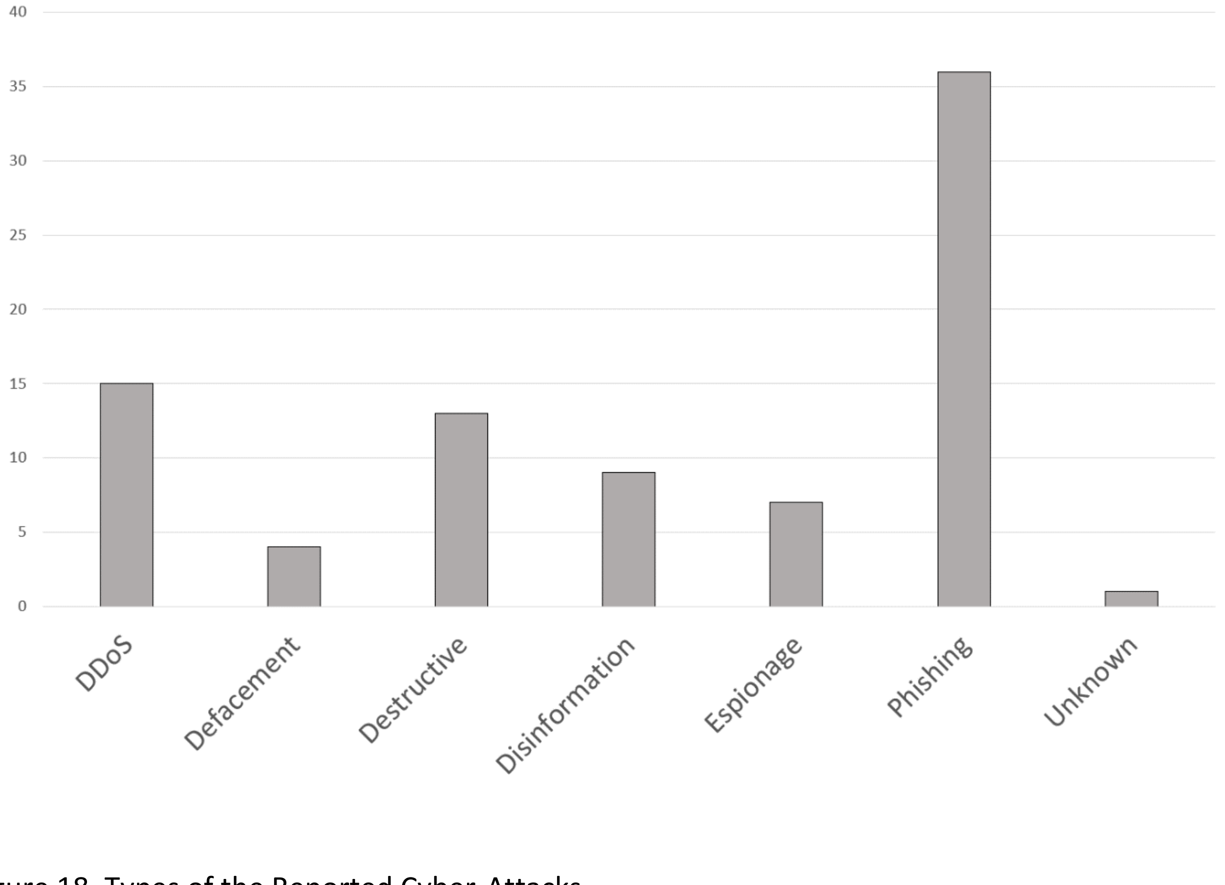


Figure 18. Types of the Reported Cyber-Attacks

6.1 Cyber Operations of the Russian Federation and Pro-Russian APTs

The number of major cyber-attacks attributed to the Russian cyber units had been increasing in February, but a sudden increase on large scale cyber-attacks was seen on the February 23rd. Especially Voodoo Bear (the hacker unit of Russian military intelligence), became more active (Digital Security Unit, 2022). The APT group launched multiple attacks and released new destructive wiper malware (ESET, 2022a; Digital Security Unit, 2022).

On the next day the number of the attacks kept increasing and yet another wiper malware was discovered (ESET, 2022b; Digital Security Unit, 2022). Probably the most complex and audacious cyber-attack observed between January and end of July was launched against Viasat's KA-SAT satellite internet network, just an hour before the invasion of Ukraine started (Viasat, 2022). The attack destroyed more than 30,000 satellite terminals and the attack spilled over to other European countries causing problems for several thousands of customers (Martin, 2022).

On the February 25th, the attacks kept utilizing the same wiper malware, but now targeting border control station causing difficulties for fleeing refugees (Berger, 2022). Also, disinformation campaigns were launched on social media trying to spread image of weak and surrendering Ukrainian soldiers (Gleicher & Agranovich, 2022). During the next days, new destructive wiper malware was discovered (Digital Security Unit, 2022), organizations of public sector and media companies were attacked with various DDoS attacks (Microsoft, 2022; Slaney, 2022), and several phishing campaigns were launched (Censor.net, 2022).

The first half of March was continuing the theme of DDoS attacks targeting government organizations (Schwarz, 2022; Satter, 2022b), and sophisticated phishing attacks were targeting civilians and government workers (Lakshmanan, 2022). Two major telecommunications providers were hacked with destructive methods. It took almost 12 hours to restore network services (Brewster, 2022). Also, Ukrtelecom suffered 40 minutes of nationwide downtime as the result of a cyber-attack (Moss, 2022a). New destructive wiper malware attributed to Voodoo Bear was discovered from undisclosed Ukrainian organizations (ESET, 2022c).

In the middle of March, it started to become apparent that the Russian military intelligence (GRU) and its hacker units were leading the Russian cyber operations and other nation-state actors like

FSB and SVR were in supporting role (in Figure 19). Voodoo Bear and Fancy Bear seemed to be the most active actors on the Ukraine's cyber theater (Digital Security Unit, 2022; Huntley, 2022; Microsoft, 2022; Gatlan, 2022; Censor.net, 2022; Martin, 2022; Chirgwin, 2022).

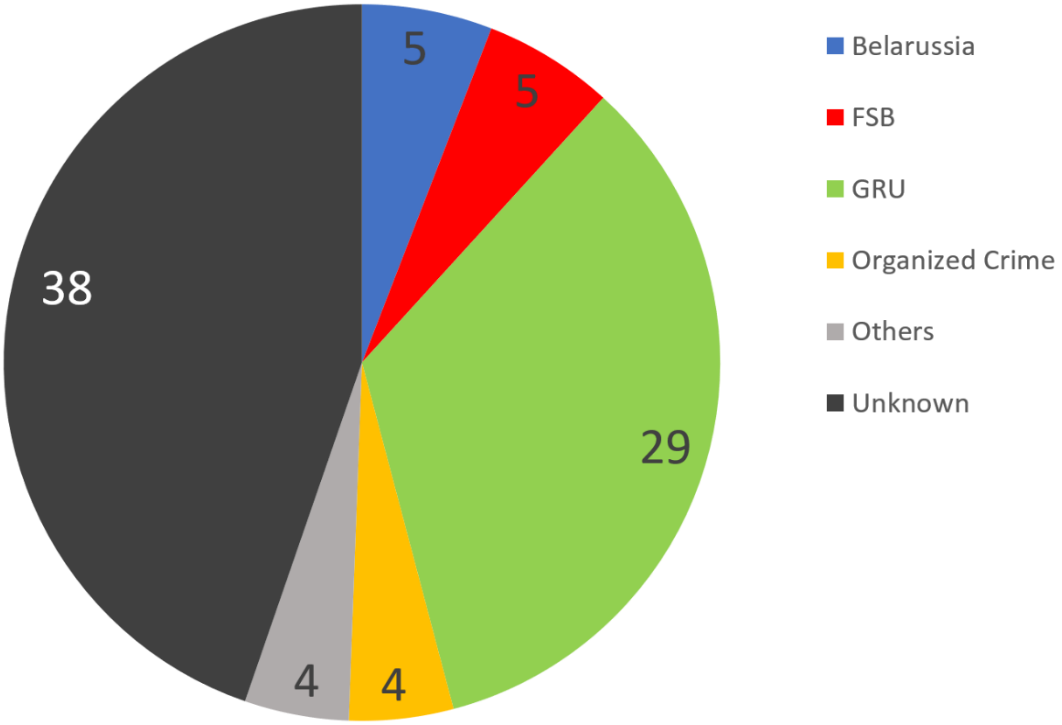


Figure 19. Distribution of Reported Attributed Attacks.

During the second half of the March, the number of major attacks started to decrease while their variety stayed similar, including disinformation campaigns (Digital Forensics Lab, 2022), phishing campaigns (Threat Intelligence Team, 2022; CERT-UA, 2022ag; 2022ai), and attacks aimed to take down major telecommunication networks continued. The largest outage in network services was when a massive cyber-attack took down Ukrtelecom's nationwide services, this time for over 15 hours (Bing & Satter, 2022).

The next major event was observed on April 8th when Voodoo Bear launched cyber-attack against the energy sector with new and more malicious version of its Industroyer malware, now known as Industroyer2 (ESET, 2022d; CERT-UA, 2022aj). The attack itself was thwarted quickly with the help of the Microsoft and ESET (CERT-UA, 2022aj). The rest of the month followed similar path as the previous month and number of the major attacks decreased.

In May, several phishing campaigns were launched targeting public sector and civilians (CERT-UA, 2022an; 2022ao; 2022ap; 2022aq; Trellix, 2022). These attacks were mainly utilizing old malware, sometimes with some modifications (CERT-UA; 2022ap).

A new zero-day remote code execution vulnerability known as Follina was adapted by Russian hackers in early June and several attacks utilizing the vulnerability were made (CERT-UA, 2022ar; 2022as; 2022at; 2022au). Also, campaigns spreading disinformation continued with hijacking a Ukrainian online broadcasting platform during a soccer game (OLL.TV, 2022).

On July decreasing the trend of major cyber-attacks attributed to Russian nation-state actors continued, but overall trend was increasing due to attacks performed by unknown actors. The most interesting campaign was launched by Venomous Bear targeting volunteering civilian hacktivists by releasing a fake Denial of Service Android application. The application was similar to the application used by the IT Army of Ukraine for their volunteers.

6.2 Cyber Operations of Ukraine and Pro-Ukrainian Hacktivists

In the beginning of the war the hacktivists allegedly breached Russian Ministry of Defence and were able to leak personal data of its employees. These included names, email addresses and hashed passwords of the accounts (Metro, 2022). The leak was followed by an alleged leak of personal information of over 120,000 Russian military personnel. This included full names, dates of birth, passport numbers and assigned military unit (Stanton, 2022).

Soon after hacktivists started to breach Russian military broadcast UVB-76, known as the Buzzer. The short-wave broadcast has been claimed to send coded Russian military signals for several decades. Now the hackers were able to include broadcasts of their own with flooding the broadcast with memes and music. Ultimately these hacks forced Russian troops to switch to encrypted communications (Williams, 2022).

The hacktivists have been targeting also Russian media to promote Pro-Ukrainian propaganda by playing Ukrainian national anthem with other war opposing songs on Russian radio stations and defacing Russian TV broadcasts with messages promoting peace and claiming Russian people having blood on their hands. Russian media has been compromised with similar attacks for several times since February 2022 (Pannett & Shammas, 2022).

On March the Security Service of Ukraine (2022) claims it has taken down five different botnets since the beginning of the war in February. Allegedly the botnets were operating over 100,000 fake accounts spreading misinformation used in Russia's influence operations.

Early on March also Belarusian hacktivists began targeting their own critical infrastructure, especially railways, to prevent Russian logistics and troop movement to assault Ukrainian capitol, Kyiv (Sly, 2022). The railway networks were shutdown for days and as suggested by Lee, this resulted in a formation of the infamous 40-mile-long military column. This is one of the actions of hacktivists that could have had some sort of impact on Russia's war efforts.

Other cyber-attacks performed by multiple hacktivist groups includes DDoS attacks against Russian companies and organizations. Targets have been including financial sector and at some point, most of the Russian government websites were alleged to have been inaccessible because of ongoing attacks (Pitrelli, 2022; Burgess, 2022b).

We must note that Ukraine has had high OPSEC regarding its own cyber operations. As suggested by Kaminska et al. (2022) the U.S. Cyber Command and other nations of the Five Eyes have been conducting defensive and offensive cyber operations during the war, but the contents or impact of these operations have not been published. As speculation, it would be reasonable to assume that some of the more sophisticated cyber-attacks attributed to the hacktivist groups might actually be conducted by the Western or Ukrainian nation-state actors.

Hacktivists Targeting Companies and Organizations with Data Leaks

Between 26 February and 1 May the hacktivists have targeted several private companies and organizations in Russia and Belarus leaking at least 7.28 Terabytes of emails and documents. Major data leaks done during that time period are presented in Table 4. Most of the stolen and published content, as suggested by Lee (2022) is written in Russian and this makes it a bit difficult for Western researchers and journalists to investigate them if they are not fluent in Russian language. The published data are mainly emails of the companies, but some leaks are suggested by Lee to include also company documents. These companies and organizations seem to be uninteresting and unrelated to any war efforts with the exception of Tetraedr, which is a Belarussian weapons manufacturer.

Table 4. Leaked Data by the Hacktivists (Lee, 2022)

TARGET		PUBLISHED DATA (GB)
Tetraedr	A Belarussian weapons manufacturer **Data:** Emails	200
Roskomnadzor	The Russian federal agency of mass censoring and controlling of media **Data:** Documents	817
Omega Co.	Research and development subsidiary of Transneft **Data:** Emails	79
Central Bank of Russia	**Data:** Documents	22.5
Rosatom	A Russian state-owned nuclear company **Data:** Photographs, documents, SQL databases	15.3
Rostproekt	A Russian construction company **Data:** Documents	2.4
Mashoil	A drilling and mining equipment manufacture **Data:** Emails	110
Thozis Corp.	An investment firm **Data:** Emails	5.9
Marathon Group	An investment firm **Data:** Emails	51.9
Russian Orthodox Church	Charitable wing of the Church **Data:** Emails	15
Mosekspertiza	A Russian state-owned business services provider **Data:** Documents, databases	483
VGTRK	A Russian state-owned television and radio broadcasting company **Data:** Emails, documents	786

Petrofort	An office space and business centers company **Data:** Emails	244
Aerogas	An engineering company **Data:** Emails	145
Forest	A logging and wood company **Data:** Emails	37.5
Capital Legal Services	A law firm **Data:** Emails	65
The Ministry of Culture of The Russian Federation	**Data:** Emails	446
The City Administration of Blagoveshchensk	**Data:** Emails	150
The Governor's Office of Tver Oblast	**Data:** Emails	116
Technotec	An oil and gas field services provider **Data:** Emails	440
Gazprom Linde Engineering	An engineering company for refineries etc. **Data:** Emails	728
The Education Department of The Russian City of Strezhevoy	**Data:** Emails	221
Continent Express	A travel agency **Data:** Documents, databases	399
Gazregion	A construction company **Data:** Emails, documents	222
Neocom Geoservice	An engineering company **Data:** Emails	107
Synesis Surveillance System	A Belarussian surveillance systems developer **Data:** Videos, documents, software	1.2
GUOV i GS	A construction company working for projects of Russian Ministry of Defence **Data:** Emails	9.5

Tendertech	A company specialized to processing financial and banking documents **Data:** Emails	160
Worldwide Invest	An investment firm **Data:** Emails	130
Sawatzky	A property management company **Data:** Emails	432
Enerpred	A hydraulic tools manufacturing company **Data:** Emails	432
Accent Capital	A commercial real-estate investment company **Data:** Emails	211
	TOTAL OF	7.28 Tb

7 Analysing the Observations

Russia has launched a massive number of cyber-attacks against Ukraine. The tactics used by Russia have been ranging between denying access to the basic services to cyber espionage operations resulting to data thefts. Russia has deployed multiple new wiper malware and quickly adapted the Follina zero-day as part of its toolset when the vulnerability was discovered (CERT-UA, 2022ar).

Especially Microsoft has been tracking Russia's cyber-attacks' relations to kinetic strikes (Digital Security Unit, 2022). According to Microsoft's observations, cyber-attacks have been launched on multiple occasions to disable the systems and networks of the target before assaulted with military troops or targeted with missile strikes or shelling.

According to Microsoft's Digital Security Unit (2022), 40 percent of the attacks has been targeting the critical infrastructure. The nature of these attacks has been destructive by utilizing different wiper malware. The probable purpose of these destructive attacks can be divided to at least four different objectives. The first objective being the attempt to blind Ukraine's military command by disrupting its ability to have near real time situational awareness from the frontlines. The second one is to disrupt telecommunications for preventing the spread of real information in and from Ukraine. By controlling the information environment, it is much easier to disrupt troop and war effort coordination of Ukraine, and also to spread uncertainty and propaganda among the civilian population. The third objective would be the attempt to shutdown the critical infrastructure and use that to affect the minds of Ukrainians and especially their will to fight. It is worth mentioning that targeting critical infrastructure is a violation against IHL and LOAC. The fourth objective would be economic warfare done through cyberspace. Russia's attacks against Ukrainian companies could be an attempt to increase the pressure to weaken political will. This was seen with attacks to agriculture companies.

In end of June, SSSCIP (2022c) published statistics of cyber-attacks collected from observations of Ukrainian authorities and partnering private vendors. The total number of incidents was suggested be 796 for the first four months of the war. These monitored incidents published by SSSCIP are presented in Table 5 by lines of business they have been targeting and number of different identified attack-techniques are shown in
Table 6.

Table 5. The Number of Monitored Cyber-Attacks by End of June (SSSCIP, 2022c, modified)

SECTOR	NUMBER OF INCIDENTS
Public Sector	179
Military	104
Financial	55
Commercial	54
Energy	54
Other	350

Table 6. Monitored Techniques for Cyber-Attacks by End of June (SSSCIP, 2022c, modified)

TECHNIQUE	NUMBER OF INCIDENTS
Information Gathering	242
Malicious Code	192
Intrusion	92
Intrusion Attempts	82

Availability	56
Other	132

The numbers published by SSSCIP (2022c) in Table 5 are a bit difficult to correlate with the ones published by Microsoft (Digital Security Unit, 2022) since the category “other” most likely includes some of the services of critical infrastructure. However, SSSCIP’s data supports Microsoft’s observations since by combining the numbers of cyber-attacks targeting public sector, financial sector, and energy sector we get 36.2 percent.

In July SSSCIP (2022e) released more statistics regarding observed cyber-attacks targeting Ukraine during the first two quarters of 2022. The total number of observed attacks was claimed to be 1,350, which contained 802 attacks on the first quarter and 548 attacks on the second quarter. This would suggest over 30 percent decrease during the second quarter. These numbers seem to be inline with decreasing number of major cyber-attacks, suggesting that the Russian hacker units’ capabilities to carry out operations have been exhausted. 525 of the attacks were monitored before the war began and 825 of the attacks happened during the war. Though while the number of attacks has been decreasing their nature has been also chancing as suggested by SSSCIP (2022d). In the second quarter of 2022 the spread of malware was increased by 38 percent compared to the previous quarter.

Strategical and even operational success of these attacks has been staying on a level of annoyance (especially when compared to damage caused by kinetic strikes) than anything that would actually be helpful for the Russian war plans. Most of the internet service disruptions have been reported to last for a few hours or less than a day. While the traditional kinetic warfare has been more devastating for the telecommunications networks, Ukraine has been supported with providing satellite telecommunications to counter these loses.

7.1 Destructive Wiper Malware and Critical Infrastructure

According to Fortinet’s Revay (2022) there has been only 15 notable destructive wiper malware in the last decade. What makes the situation in Ukraine interesting is that eight of those wipers have been deployed against Ukrainian organizations and companies. Seven of those in the current year. Timeline of these wiper malware is presented in Figure 20.

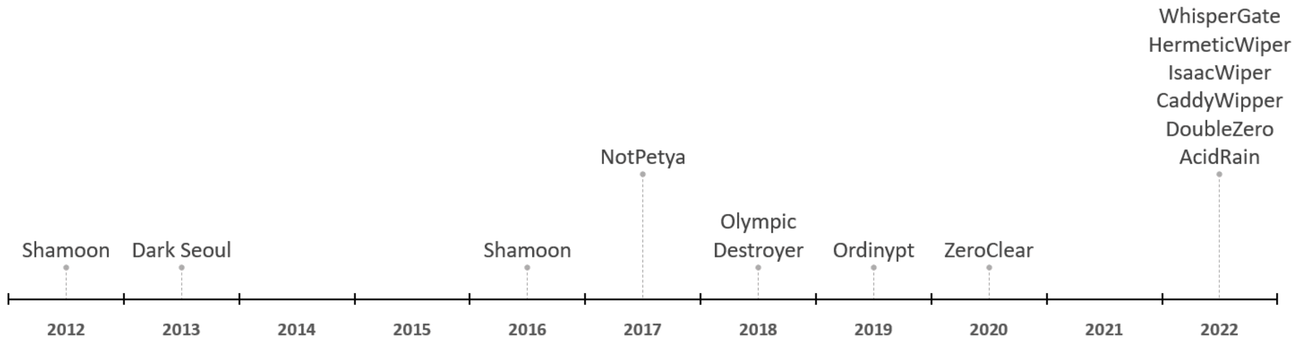


Figure 20. Timeline of Wiper Malware (Revay, 2022, modified)

The use of these destructive malware and targeting them against public sector, telecommunications, electrical power grids etc. parts of critical infrastructure seem to be similar than Russia’s irresponsible conventional warfare tactics where they use kinetic force, such as massive missile strikes and shelling, against similar targets.

Probably the most interesting of these attacks is AcidRain malware used in Viasat’s KA-SAT cyber-attack (Martin, 2022; Viasat, 2022). The AcidRain was successfully deployed to satellite modems in a supply-chain attack. This is a sophisticated tactic, and has most likely needed a very long time for planning and executing pre-war. This is also the only cyber-attack performed by Russia that has shown in the current war Russia’s typical high tolerance for taking operational risk (Przetacznik & Tarpova, 2022) with the attack spilling over to other European countries.

The other wipers used against Ukraine have been more or less effective. According the reports they have managed to destroy hundreds if not even thousands of computers, but it seems that the effects of these attacks have stayed relatively low and the attacks have not been able to cripple their targets.

Another example is the attempt to overthrow Ukrainian electrical power grid with a new variant of the Industroyer malware which also seemed to have only a limited effect.

Most likely the quick reaction to the new emerging malware threats has been thanks to the multiple private vendors participating in cyber defence. For example, in one case Microsoft was reported to have been able to enable some features on their Windows Defender product to stop spreading of the new malware. These actions usually require network administrator level permissions (Microsoft, 2022).

7.2 Phishing Campaigns and Disinformation

Russian cyber units seem to be relaying heavily on the usage of phishing campaigns while targeting different Ukrainian organizations. These phishing campaigns include really sophisticated spear phishing attempts to lure their victims to open malicious attachments (CERT-UA, 2022ah; 2022ak; 2022ar; 2022aw). In some cases, classical watering-hole attacks have been used, too (Nakashima, 2018).

The lures used in the campaigns are cleverly utilizing current topics regarding the war and have been specifically targeted to personnel whose responsibility those topics are. In some campaigns fear and urgency are used to trick the victim, for example in the messages about chemical attack and evacuation plans (CERT-UA, 2022ao).

The need to relay to these tactics in so massive scale is most likely because of Ukraine’s improved and heightened cyber resiliency and detection capabilities. Ukrainian systems are most likely up-to-date and finding working vulnerabilities to exploit them is difficult. To gain access to these systems without getting the initial access by tricking an end user would require discoveries of severe zero-day vulnerabilities. While it is impossible to estimate if Russia’s cyber weapon arsenal includes such vulnerabilities, at least those have not been used in recent attacks.

As noted earlier, the Russia’s armed forces does not acknowledge cyber warfare as part of their doctrine or military terminology, but instead they are focusing on information warfare. Part of the dominance in information environment is also the capability to control and affect the narrative of war by spreading disinformation. Russia has been able to display a vast toolset of different methods for spreading disinformation in Ukraine. These methods have been ranging from defacements of websites (Slovo i Dilo, 2022) to hijacking TV broadcasts (Digital Forensics Lab, 2022; OLL.TV, 2022). Also using of SMS text messages to specified targeted areas have been observed (Cyber police of Ukraine, 2022b; Digital Security Uni, 2022). One of the more sophisticated methods has been the use of so called deepfake videos of President Zelensky (Digital Forensics Lab, 2022).

7.3 Actions of Hacktivists

Cyber-attacks performed by the Pro-Ukrainian and the Pro-Russian hacktivist collectives have not really had an effect on the war efforts of either side. Most of the attacks have been DDoS attacks targeting government websites and finance sector to make every day life of citizens on both sides more difficult. Some data leaks have been certainly embarrassing for the Russian Federation (e.g., leak of personal data of 120,000 Russian soldiers) (Stanton, 2022) and with identifying Russian personnel affiliated to the military unit responsible for the massacre of Bucha (Halpert, 2022). Other typical examples of hacktivists' operations are influence operations promoting peace or blaming the other side for brutalities.

Attacks targeting Belarussian railways are probably the only cyber-attack that could have had some limited effects on the outcome of the Russia's assault targeting Kyiv. But on the other hand, acts like disrupting Russia's unencrypted military communications forced Russian troops to quickly adapt encrypted communications. This has had negative effects by preventing easy monitoring of Russian armed forces' actions and presence.

Typically, data leaks such as those published by the hacktivists are less useful for intelligence community than their own access to those hacked systems. Sometimes they can even be counterproductive in long term intelligence gathering since they expose vulnerabilities of Russia's security system.

7.4 Influence Operations and Propaganda

Even when the influence and other PSYOPS done in or through cyberspace are not counted as cyber operations in the West's military doctrines, one cannot ignore their presence and significance during this war. As noted by Kaminska et al. (2022) influence operations have been in crucial role in building of a narrative for the war. These operations began when the West's intelligence community published a pre-warning of the incoming invasion of Ukraine.

On the Russian side Kaminska et al. (2022) suggests the two major PSYOPS being the Viasat's KA-SAT hack and attacking to the Ukrainian power grid with Industroyer2 malware. Russia has launched several smaller influence operations during the war targeting civilians and military personnel. Mostly these operations have been used to encourage Ukrainians to stop fighting. Also, Russia's statements with talking big and idle threats are also part of their PSYOPS. These are most likely targeted more to domestic than to international audience, though.

Ukraine on the other hand has played their propaganda game well. In the early days of the war hero stories were built around e.g., mysterious fighter pilot "the Ghost of Kyiv" (Bubola, 2022), soldiers of the Snake Islands (BBC News, 2022a) and President Volodymyr Zelensky. The last two have clearly formed as the symbols of this war. The hearts of western audience were won with flood of images of Ukrainian soldiers with cute animals on the front lines (Tucker, 2022b) and later on with a hero dog, Patron (Treisman, 2022). Several internet phenomena have also been surfaced in support of Ukraine. Some examples of these would be St. Javelin – The protector of Ukraine meme (referencing to Javelin anti-tank weapons system) (Debusmann, 2022) and the hit song, the Bayraktar drone song, which was later on revealed to be made by a Ukrainian soldier at the request of Ukrainian armed forces (Weichert, 2022).

7.5 Russia's Lack of Successful Cyber Offensive?

The cyber-attacks executed by the Russian cyber units have not yet been able to cripple Ukraine's telecommunications or introduce mass scale destruction to the critical infrastructure. This could be interpreted as lack of success for Russia's offensive cyber operations. If we make the assumption that Russia's cyber warfare capabilities really are appearing weak in this war, as suggested by several specialists, then we must speculate, why that is? We know from historical cyber-attacks attributed to the Russian APT actors that they certainly are among the best in the world so why they seem to be lacking now? One reason could be that they were not really prepared for long conflict. This could be a plausible hypothesis if we accept that the western intelligence community's analysis was correct when claiming that (Corera, 2022) the Russia was believing that the war would be won in a few days to maximumly few weeks. We saw the war starting with massive cyber-attacks trying to overcome telecommunications and other mission critical infrastructure. End of February and some weeks in to March were full of cyber-attacks dropping a new wiper malware once a week. Russia certainly was supporting their traditional warfare with cyber-attacks by trying to overpower the information domain (including communications). While the cyber-attacks have continued, the number of the major attacks trying to achieve nation level effects has been decreasing (e.g., see appendix 6) since the first month of the war, but as suggested by SSSCIP (2022c) the number of smaller attacks has been staying steady.

Secondly, we must keep in mind how unorganized, especially with the lack of logistics, the traditional warfare was on Russia's side. Do we have any reason to assume that the situation was not the same regarding the cyber capabilities, or were they noted and coordinated any better by the chain of command? It is plausible to assume that war planning between different warfare methods was lacking similarly. Though from Microsoft's (Digital Security Unit, 2022) report we know that is not entirely true. Microsoft presents how cyber capabilities were supporting kinetic warfare. First disruptive and destructive cyber-attacks against some specific target start and soon after the same target is affected with use of kinetic force or assault troops. This of course does not prove if those cyber-attacks were successful or accomplishing their set goals, but it proves there was some coordination between cyber units and traditional warfare units.

Another reason could be speculated to be that Russia is simply holding back. In favour of this, it is not reasonably to believe that couple of new wiper malware are the full cyber weapon arsenal of the Russian cyber units. Russia's failure in traditional warfare efforts and lacking effects of previous cyber-attacks could be the reason to not to spend any more cyber weapons than really is needed. We must remember that effective use of a cyber weapon is for single time only and when its IOC are known, it is easier to detect and counter. Holding back could also be because of fear of escalation. Russia has almost its full military potential tied to Ukraine, so escalation of the conflict with the Western World or NATO could be a serious strategical error. Yet some experts are speculating that Russia is just waiting for the right moment to hit second massive cyber-attack.

A fourth option could be that we have been overestimating Russia's capability in offensive cyber operations. The assessment of one's capability to successfully manoeuvre in cyberspace is a difficult task. But by looking the historical data of Russia's sophisticated cyber operations this option seems unlikely.

While it is true that Russia's cyber warfare has been limited warfare with limited success rate, but with relaying in this matter only to currently available information on public sources it is not possible to make determination of root cause for it. This is certainly an area that needs more detailed research when more information from the events of war will be available. Making the definitive conclusion for the reasons behind the Russia's limited success in their cyber operations requires a longer monitoring period of Russia's cyber capabilities.

7.6 Strategical Meaningfulness and Ukraine's Strong Cyber Defence

We cannot disregard the note of Maschmeyer and Cevelty (2022) that not a single cyber-attack witnessed to date on Ukraine has had any meaningful strategical impact to the outcomes of war and their strategical meaningfulness has probably been overestimated for current operations. But we do not know, as also suggested by Maschmeyer and Cevelty, how much Ukraine's strong capabilities in cyber defence operations distorts the estimation of success of cyber-attacks. Ukraine's cyber defence has been referred to be among strongest ones in the Europe and it is boosted up with specialist teams from abroad and private security vendors. What the results of Russia's cyber-attacks would have been without Ukraine's over decade long learning curve for successful cyber defence? How different would the results be, if Russia was facing an adversary with less defensive capability?

8 Conclusions

Determining the effectivity of Russia's cyber warfare is difficult when relying solely on public sources. When Microsoft released their early lessons report (Microsoft, 2022) they stated that they had witnessed more than 230 cyber-attacks against Ukraine since the beginning of the war. On the same day than the Microsoft's report was published, the number of cyber-attacks reported in public sources was 83. Some of those were left out from this thesis as their occurrence could not be verified trustworthily. It is a worth of noting, that Microsoft is only one organization that is participating in the cyber defence of Ukraine and that there are other major companies engaged in similar activities, for example Google, Amazon, ESET, TrendMicro and many other. For this reason, the total number of detected attacks must be much higher than the 230 announced by Microsoft. This observation is supported by SSSCIP (2022c), whose statistics count 1,350 cyber-attacks during the first six months of 2022. From analysis point of view, the fact that less than 10 % of the cyber-attacks gets published, it is hard to draw conclusions on Russia's cyber capabilities. This is also a probable reason why we keep currently hearing so contrary statements from cyber warfare experts regarding importance (or lack of it) of cyber operations during an armed conflict.

Part of this bias is created by Ukraine's national publishing policy and propaganda regarding the cyber-attacks. As discussed in the chapter 3.7.3 regarding information warfare and a nation's strategy to publish or not publish information of cyber-attacks. We do know that Russian cyber weapons, for example destructive wiper malware, has destroyed hundreds or even thousands of computers. We do not know what data were lost and what has been recovered from backups. Nor do we know strategical value of that information if any. However, as stated earlier, these attacks have had only a minor effect on the Russia's war effort. As noted by Kaminska et al. (2022) Ukraine has not been forthcoming regarding cyber-attacks targeting the military targets or military hardware.

Regarding the type of the attacks, attacks trying to exploit human factor are the most common. However, there are also attacks whose intrusion vector remains unknown. In any case, the end users seem to be remaining as the weakest link of cyber security.

Suitability of Cyber Operations for Armed Conflicts

As suggested by Smith (2013) the nature of the cyber-attacks might be the reason why they are not so suitable during an active conflict or war. It takes a long time to plan and prepare sophisticated cyber-attacks and to create a needed initial access vector to the targeted systems. These things need covertness, which is harder to achieve when the adversary's defence capabilities are already in heightened state. Cyber weapons are inherently more unpredictable than conventional ones; for example, an update in the targeted system might render a cyber weapon ineffective, whereas a missile would still be effective against that target. These challenges can be overcome to some degree with pre-war operations like supply-chain attacks to create the much-needed foothold to different systems (e.g., the Viasat KA-SAT attack). Since the experts' opinions on cyber warfare's suitability for armed conflict are divided, more research is needed when more data of this conflict becomes available.

It is safe to assume that cyber espionage and other cyber intelligence activities are currently the capabilities getting the most benefit out of cyber operations. We must not underestimate their value for producing near-real time situational awareness needed for successful planning and managing operations of war. However, as traditional espionage is not usually counted as a warfare why should cyber espionage be categorized any different?

The Role of Hacktivism in Conflicts

Hacktivism as a part of war is problematic and its end-results are still unknown and difficult to predict. From western legislation's viewpoint, the actions of the hacktivists are illegal, but they are actionable offences, meaning meaning that Russia should report such offences to the officials in Western countries as being the victim (Gaffney, 2022). The other problem arises from the civilian hacktivists acting in a field of military cyber units, creating more fog of war and obscuring the roles of different cyber actors, especially the ones used in proxy warfare (Collier, 2017; Akoto, 2022). From the perspective of military cyber operations, and especially from the viewpoint of cyber espionage operations, the unawareness of the hacktivists could disturb planned cyber operations, for example revealing breach vectors which could cause harm for long-term success (Lyngaas, 2022).

Another valid concern for the acts of the hacktivists is the fear of escalation of the crisis (Lyngaas, 2022). Actions of the hacktivists could be taken advantage of in the Russian propaganda and Russia could interpret them as hostile and offensive actions by the Western World (Peterson & Cimpanu, 2022). This could give Russia a self-claimed mandate to start exploiting its own cyberspace capabilities against the West and the supporters of the Ukraine (Shore, 2022).

Hacktivists can also cause risk of escalation on a national level. One may feel a hacktivist's participation in war efforts is a personal matter and that he/she is putting only himself/herself in harm's way. This is not entirely true. After all, citizens represent their state with their actions and those actions could be violating international treaties. An example of this is brought up by Gaffney (2022) as U.S. citizens could be violating the Neutrality Act from 1794 when participating in a military expedition or enterprise. Though in this case, the activities performed solely in cyberspace might not be enough to be considered as a military expedition.

Probably the most overlooked part of the hacktivism is the significance of skilled individuals. Most likely nations were not prepared how quickly this kind of new capability could form and to become an actual noteworthy force. This will most likely lead to several agencies to re-valuate the hacktivism's significance in their risk management. Another possible outcome is that the hacktivism gains more socially accepted status.

The Future of Cyber Warfare

Both parties of this armed conflict are practicing unethical selection of targets for cyber-attacks which can be seen conflicting with IHL and LOAC. Russia's nation-state actors and their criminal nation-sponsored proxy groups have been conducting these malicious acts of cyber sabotage for over a decade. Ukraine on the other hand is fighting for its very survival, but does it make use of unethical but non-lethal tactics more acceptable? The author thinks yes, but in any case, acts of the hacktivists and the formation of civilian IT Army could have long-lasting affects to the future direction of IHL and LOC regarding cyber warfare.

Regardless how cyber war and its meaningfulness in Russo-Ukrainian war is interpreted, our lives grow a daily basis more depended on the security of information systems as the world constantly becomes more digital. It is almost certain that we have not yet seen the truly devasting effects of cyber war. To counter this, we need to develop more secure technologies for our everyday life and to have the rules of just war to include actions performed in cyberspace.

References

360 Netlab. (2022, February 25). Some details of the DDoS attacks targeting Ukraine and Russia in recent days. *360 Netlab Blog*. https://blog.netlab.360.com/some_details_of_the_ddos_attacks_targeting_ukraine_and_russia_in_recent_days/

Abrams, L. (2022, March 28). *Hacked WordPress sites force visitors to DDoS Ukrainian targets*. BleepingComputer. https://www.bleepingcomputer.com/news/security/hacked-wordpress-sites-force-visitors-to-ddos-ukrainian-targets/

Akoto, W. (2022, January 31). Hackers for hire: Proxy warfare in the cyber realm. *Modern War Institute*. https://mwi.usma.edu/hackers-for-hire-proxy-warfare-in-the-cyber-realm/

Alberts, D. S., Gartska, J. J., & Stein, F. P. (2000). *Network-centric warfare: Developing and leveraging information superiority* (2nd ed.). National Defence University Printing.

Alspach, K. (2022, February 28). Ukraine border control hit with wiper cyberattack, slowing refugee crossing. *VentureBeat.* https://venturebeat.com/2022/02/27/ukraine-border-control-hit-with-wiper-cyberattack-slowing-refugee-crossing/

Amazon. (2022, March 4). *Amazon's cybersecurity assistance for Ukraine*. https://www.aboutamazon.com/news/community/amazons-cybersecurity-assistance-for-ukraine

Applegate, S. D. (2013). The dawn of kinetic cyber. *2013 5th International Conference on Cyber Conflict (CyCon),* Estonia. https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf

Arene. (2019, September 12). *Ethical recommendations for thesis writing at universities of applied sciences.* Arene ry. http://www.arene.fi/wp-content/uploads/Raportit/2020/ETHICAL%20RECOMMENDATIONS%20FOR%20THESIS%20WRITING%20AT%20UNIVERSITIES%20OF%20APPLIED%20SCIENCES_2020.pdf?_t=1578480382

Aro, J. (2019). *Putinin trollit: Tositarinoita Venäjän infosodan rintamilta* [Putin's trolls: True stories from frontlines of Russian infowar]. Helsinki: Johnny Kniga.

Baram, G., & Sommer, U. (2019). Covert or not covert: National strategies during cyber conflict. *2019 11th International Conference on Cyber Conflict (CyCon)*, Estonia, 1–16. https://doi.org/10.23919/CYCON.2019.8756682

Barno, D., & Bensahel, N. (2021, May 4). *Why the United States needs an independent cyber force*. War on the Rocks. https://warontherocks.com/2021/05/why-the-united-states-needs-an-independent-cyber-force/

BBC News. (2021, April 19). Why Russia's GRU military intelligence service is so feared. *BBC News*. https://www.bbc.com/news/world-europe-56798001

BBC News. (2022a, February 25). Snake Island: Ukraine says soldiers killed after refusing to surrender. https://www.bbc.com/news/world-europe-60522454

Berger, M. (2022, February 26). 400,000 Ukrainians flee to European countries, including some that previously spurned refugees. *Washington Post*. https://www.washingtonpost.com/world/2022/02/26/europe-welcomes-refugees-ukraine-russia/

Bianco, D. (2014, January 17). *The Pyramid of Pain.* Detect & Response. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Bigelow, B. (2019). What are military cyberspace operations other than war? *2019 11th International Conference on Cyber Conflict (CyCon)*, Estonia, 1–16. https://doi.org/10.23919/CYCON.2019.8756835

Bing, C., & Satter, R. (2022, March 28). Ukrainian telecom company's internet service disrupted by "powerful" cyberattack. *Reuters*. https://www.reuters.com/business/media-telecom/ukrainian-telecom-companys-internet-service-disrupted-by-powerful-cyberattack-2022-03-28/

Bolt, Beranek & Newman Inc. (1981). *A history of the ARPANET: The first decade* (Report No. 4799). Defense Advanced Research Projects Agency. https://apps.dtic.mil/sti/pdfs/ADA115440.pdf

Bosquet, A. J. (2009). *The Scientific way of warfare: Order and chaos on the battlefields of modernity.* Columbia University Press.

Bowen, A. S. (2021). *Russian military intelligence: Background and issues for congress* [Report No. R46616]. Congressional Research Service. https://fas.org/sgp/crs/intel/R46616.pdf

Bowen, A. S. (2022), *Russian cyber units* [Report No. IF11718, Version 4]. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11718

Brantly, A., Smeets, M. (2020). Military operations in cyberspace. In Sookermany, A. (eds). *Handbook of Military Sciences.* Springer, Cham. https://doi.org/10.1007/978-3-030-02866-4_19-1

Brewster, T. (2022, March 10). *As Russia invaded, hackers broke into a Ukrainian internet provider. Then did it again as bombs rained down*. Forbes. https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/

Bubola, E. (2022, May 1). Ukraine acknowledges that the 'Ghost of Kyiv' is a myth. *The New York Times*. https://www.nytimes.com/2022/05/01/world/europe/ghost-kyiv-ukraine-myth.html

Burgess, M. (2022a, February 27). Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory. *Wired*. https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/

Burgess, M. (2022b, April 27). *Russia is being hacked at an unprecedented scale*. Wired. https://www.wired.com/story/russia-hacked-attacks/

Cambridge University Press. (n.d.). Trolling. In *Cambridge dictionary.* Retrieved June 16, 2022, from https://dictionary.cambridge.org/dictionary/english/trolling

Carr, J. (2022, April 5). GURMO hackers go kinetic against Gazprom—Two pipeline fires so far. *Inside Cyber Warfare*. https://jeffreycarr.substack.com/p/gurmo-hackers-go-kinetic-against

CBS News. (2018, August 22). *What can we learn from the "most devastating" cyberattack in history?* https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/

Censor.net. (2016, May 9). *"Operation May 9": Ukrainian hackers deface several terrorists' propaganda sites. Video+Photo*. https://censor.net/en/photo_news/387695/operation_may_9_ukrainian_hackers_deface_several_terrorists_propaganda_sites_videophoto

Censor.net. (2022, February 28). *Імейли нібито від імені СБУ про електронні плани евакуації – це ФЕЙК!* [Emails allegedly on behalf of the SBU about electronic evacuation plans are fake!]. Censor.net. https://censor.net/ua/news/3320069/imeyily_nibyto_vid_imeni_sbu_pro_elektronni_plany_evakuatsiyi_tse_feyik

CERT-UA. (2022aa, March 7). *Кібератака групи UAC-0051 (unc1151) на державні організації України з використанням шкідливої програми MicroBackdoor (CERT-UA#4109)* [Cyberattack by UAC-0051 (unc1151) on state organizations of Ukraine using the MicroBackdoor malware (CERT-UA # 4109)]. https://cert.gov.ua/article/37626

CERT-UA. (2022ab, March 12). *Кібератака на державні організації України з використанням шкідливих програми Cobalt Strike Beacon, GrimPlant та GraphSteel (CERT-UA#4145*) [Cyberattack on state organizations of Ukraine using malicious programs Cobalt Strike Beacon, GrimPlant and GraphSteel (CERT-UA # 4145)]. https://cert.gov.ua/article/37704

CERT-UA. (2022ac, March 17). Кібератака групи UAC-0020 (Vermin) *на державні організації України з використанням шкідливої програми SPECTR (CERT-UA#4207)* [Cyber attack of UAC-0020 (Vermin) group on state organizations of Ukraine using malicious program SPECTR (CERT-UA # 4207)]. https://cert.gov.ua/article/37815

CERT-UA. (2022ad, March 18). *Кібератака групи UAC-0035 (InvisiMole) на державні організації України (CERT-UA#4213)* [Cyber attack of UAC-0035 group (InvisiMole) on state organizations of Ukraine (CERT-UA # 4213)]. https://cert.gov.ua/article/37829

CERT-UA. (2022ae, March 22). *Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243)* [Cyberattack on Ukrainian enterprises using the DoubleZero destructor program (CERT-UA # 4243)]. https://cert.gov.ua/article/38088

CERT-UA. (2022af, March 22). *Кібератака групи UAC-0026 з використанням шкідливої програми HeaderTip (CERT-UA#4244)* [UAC-0026 Cyberattack using HeaderTip malware (CERT-UA # 4244)]. https://cert.gov.ua/article/38097

CERT-UA. (2022ag, March 30). *Масове розповсюдження шкідливої програми MarsStealer серед громадян України та вітчизняних організацій (CERT-UA#4315)* [Mass spread of MarsStealer malware among citizens of Ukraine and domestic organizations (CERT-UA # 4315)]. https://cert.gov.ua/article/38606

CERT-UA. (2022ah, April 4). *Кібератака групи UAC-0010 (Armageddon) на державні організації України (CERT-UA#4378)* [Cyber attack of UAC-0010 group (Armageddon) on state organizations of Ukraine (CERT-UA # 4378)]. https://cert.gov.ua/article/39138

CERT-UA. (2022ai, April 5). *Отримання доступу до облікових записів Telegram (CERT-UA#4360*) [Information on cyberattacks aimed at gaining access to Telegram accounts (CERT-UA # 4360)]. https://cert.gov.ua/article/39253

CERT-UA. (2022aj, April 12). *Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)* [Cyberattack of Sandworm group (UAC-0082) on energy facilities of Ukraine using malicious programs INDUSTROYER2 and CADDYWIPER (CERT-UA # 4435)]. cert.gov.ua. https://cert.gov.ua/article/39518

CERT-UA. (2022ak, April 14). *Кібератака на державні організації України з використанням шкідливої програми IcedID (CERT-UA#4464)* [Cyberattack on state organizations of Ukraine using the malicious program IcedID (CERT-UA # 4464)]. https://cert.gov.ua/article/39609

CERT-UA. (2022al, April 19). *Онлайн-шахрайство з використанням тематики "грошової допомоги від країн ЄС"* (CERT-UA#4492) [Online fraud using the topic "financial assistance from EU countries" (CERT-UA # 4492)]. https://cert.gov.ua/article/39727

CERT-UA. (2022am, April 26). *Кібератака групи UAC-0056 з використанням шкідливих програм GraphSteel і GrimPlant та тематики COVID-19 (CERT-UA#4545)* [Cyberattack by UAC-0056 using GraphSteel and GrimPlant malware and COVID-19 (CERT-UA # 4545)]. https://cert.gov.ua/article/39882

CERT-UA. (2022an, May 6). *Кібератака групи APT28 із застосуванням шкідливої програми CredoMap_v2 (CERT-UA#4622)* [APT28 cyberattack using the malware CredoMap_v2 (CERT-UA # 4622)]. https://cert.gov.ua/article/40102

CERT-UA. (2022ao, May 7). *Масове розповсюдження шкідливої програми JesterStealer з використанням тематики хімічної атаки (CERT-UA#4625)* [Mass distribution of the Jester-Stealer malware using the subject of chemical attack (CERT-UA # 4625)]. https://cert.gov.ua/article/40125

CERT-UA. (2022ap, May 12). *Кібератаки групи UAC-0010 (Armageddon) з використанням шкідливої програми GammaLoad.PS1_v2 (CERT-UA#4634,4648)* [Cyberattack by UAC-0010 (Armageddon) using the malware GammaLoad.PS1_v2 (CERT-UA # 4634,4648)]. https://cert.gov.ua/article/40240

CERT-UA. (2022aq, May 14). *Онлайн-шахрайство з використанням тематики "грошової допомоги в рамках соціальної програми ООН" (CERT-UA#4657)* [Online fraud using the topic of "financial assistance under the UN social program" (CERT-UA # 4657)]. https://cert.gov.ua/article/40263

CERT-UA. (2022ar, June 2). *Кібератака на державні організації України з використанням шкідливої програми Cobalt Strike Beacon та експлойтів до вразливостей CVE-2021-40444 і CVE-2022-30190 (CERT-UA#4753)* [Cyberattack on state organizations of Ukraine using the malicious program Cobalt Strike Beacon and exploits to vulnerabilities CVE-2021-40444 and CVE-2022-30190 (CERT-UA # 4753)]. https://cert.gov.ua/article/40559

CERT-UA. (2022as, June 10). *Масована кібератака на медійні організації України з використанням шкідливої програми CrescentImp (CERT-UA#4797)* [Massive cyberattack on media organizations of Ukraine using the malicious program CrescentImp (CERT-UA # 4797)]. https://cert.gov.ua/article/160530

CERT-UA. (2022at, June 20). *Кібератака групи APT28 з використанням шкідливої програми CredoMap (CERT-UA#4843)* [APT28 cyberattack using CredoMap malware (CERT-UA # 4843)]. https://cert.gov.ua/article/341128

CERT-UA. (2022au, June 20). *Кібератака групи UAC-0098 на об'єкти критичної інфраструктури України (CERT-UA#4842)* [Cyber attack of UAC-0098 group on critical infrastructure facilities of Ukraine (CERT-UA # 4842)]. https://cert.gov.ua/article/341128

CERT-UA. (2022av, June 24). *Кібератака у відношенні операторів телекомунікацій України з використанням шкідливої програми DarkCrystal RAT (CERT-UA#4874)* [Cyber attack against telecommunications operators of Ukraine using the DarkCrystal RAT malicious program (CERT-UA#4874)]. https://cert.gov.ua/article/405538

CERT-UA. (2022aw, July 6). *Кібератака UAC-0056 на державні організації України з використанням Cobalt strike beacon (CERT-UA#4914)* [Cyber attack UAC-0056 on state organizations of Ukraine using Cobalt strike beacon (CERT-UA#4914)]. https://cert.gov.ua/article/619229

CERT-UA. (2022ax, July 11). *Атака групи UAC-0056 на державні організації України з використанням Cobalt strike beacon (CERT-UA#4941)* [Attack by UAC-0056 group on state organizations of Ukraine using Cobalt strike beacon (CERT-UA#4941)]. https://cert.gov.ua/article/703548

CERT-UA. (2022ay, July 14). *Онлайн-шахрайство з використанням тематики “грошової компенсації” (CERT-UA#4964)* [Online fraud using the subject of “monetary compensation” (CERT-UA#4964)]. https://cert.gov.ua/article/761668

CERT-UA. (2022az, July 20). *Кібератака на державні організації України з використанням теми ОК “Південь” та шкідливої програми AgentTesla (CERT-UA#4987)* [Cyber attack on state organizations of Ukraine using the OK theme “South” and the malicious program AgentTesla (CERT-UA#4987)]. https://cert.gov.ua/article/861292

CERT-UA. (2022ba, July 25). *Масове розповсюдження стілерів (Formbook, Snake Keylogger) та використання шкідливих програм RelicRace/RelicSource як засобу доставки (CERT-UA#5056)* [Mass distribution of stealers (Formbook, Snake Keylogger) and use of RelicRace/RelicSource malware as a means of delivery (CERT-UA#5056)]. https://cert.gov.ua/article/955924

CERT-UA. (2022bb, July 26). *Кібератаки групи UAC-0010 (Armageddon) з використанням шкідливої програми GammaLoad.PS1_v2 (CERT-UA#5003,5013,5069,5071)* [Cyber attacks of the UAC-0010 group (Armageddon) using the malicious program GammaLoad.PS1_v2 (CERT-UA#5003,5013,5069,5071]. https://cert.gov.ua/article/971405

CERT-UA. (2022bc, July 27). *Онлайн-шахрайство з використанням тематики “допомоги від Червоного Хреста”* (CERT-UA#5063) [Online fraud using the subject of “aid from the Red Cross” (CERT-UA#5063)]. https://cert.gov.ua/article/987552

CERT-UA. (n.d.). *About CERT-UA*. Retrieved June 30, 2022, from https://cert.gov.ua/about-us

Chamber of Commerce. (2022). Yrityksiin kohdistuva hybridivaikuttaminen [Hybrid influencing targeted to companies]. Chamber of Commerce. https://kauppakamari.fi/wp-content/uploads/2022/06/Yrityksiin-kohdistuva-hybridivaikuttaminen-selvitys.pdf

Chen, J., & Dinerman, A. (2016). On cyber dominance in modern warfare. *Proceedings of the 15th European Conference on Cyber Warfare and Security*, Germany, 52–57. https://www.proquest.com/openview/9ed6393bce9c040007ba80f892744b2c/1.pdf

Cherepanov, A. (2017). *WIN32/INDUSTROYER: A new threat for industrial control systems*. ESET. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Cherepanov, A. (2018). *GREYENERGY: A Successor to BlackEnergy* [White paper]. ESET. https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

Cherepanov, A., & Lipovsky, R. (2018a, October 11). *New TeleBots backdoor: First evidence linking Industroyer to NotPetya.* WeLiveSecurity. https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/

Cherepanov, A., & Lipovsky, R. (2018b, October 17). *GreyEnergy: Updated arsenal of one of the most dangerous threat actors*. WeLiveSecurity. https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

Chirgwin, R. (2022, March 18). *Sandworm crafts malware to run on ASUS routers*. ITnews. https://www.itnews.com.au/news/sandworm-crafts-malware-to-run-on-asus-routers-577530

Clark, R. M. (2014). *Intelligence collection*. Thousand Oaks: CQ Press.

Cluster25. (2022, March 8). Ghostwriter / UNC1151 adopts microbackdoor variants in cyber operations against Ukraine. *Cluster25*. https://cluster25.io/2022/03/08/ghostwriter-unc1151-adopts-microbackdoor-variants-in-cyber-operations-against-targets-in-ukraine/

Colarik, A. M., & Janczewski, L. (2012). Establishing cyber warfare doctrine. *Journal of Strategic Security, 5*(1), 31–48. http://dx.doi.org/10.5038/1944-0472.5.1.3

Collier, J. (2017). Proxy actors in the cyber domain: Implications for state strategy. *St Antony's International Review*, *13*(1), 25–47. https://www.jstor.org/stable/26229121

Connell, M., & Vogler, S. (2016). *Russia's approach to cyber warfare*. Center for Naval Analyses. https://apps.dtic.mil/sti/pdfs/AD1019062.pdf

Corera, G. (2022, April 8). *Ukraine: Inside the spies' attempts to stop the war*. BBC News. https://www.bbc.com/news/world-europe-61044063

CrowdStrike. (2022, March 30). *EMBER BEAR: Threat actor profile*. Crowdstrike.Com. https://www.crowdstrike.com/blog/who-is-ember-bear/

Cyber Police of Ukraine. (n.d.-a). *Новини—Департамент Кіберполіції [News—Cyber police department]*. Cyber police department of the national police of Ukraine. Retrieved June 30, 2022, from https://cyberpolice.gov.ua/

Cyber police of Ukraine. (2022b, February 15). *Кіберполіція встановлює осіб, причетних до розсилання смс-повідомлень щодо збоїв у роботі банкоматів—Департамент Кіберполіції* [Cyberpolice identifying persons involved in sending SMS messages about ATM failures]. Cyber Police Department of the National Police of Ukraine. https://cyberpolice.gov.ua/news/kiber-policziya-vstanovlyuye-osib-prychetnyx-do-rozsylannya-sms-povidomlen-shhodo-zboyiv-u-roboti-bankomativ-7072/

Cybersecurity and Infrastructure Security Agency. (2021). *SolarWinds and active directory/m365 compromise: Detecting advanced persistent threat activity from known tactics, techniques, and procedures.* Department of Homeland Security. https://us-cert.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf

Cybersecurity & Infrastructure Security Agency. (2022, April 20). *Russian state-sponsored and criminal cyber threats to critical infrastructure*. Department of Homeland Security. https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

Darcy, O. (2022, February 26). *"We want to get the news out": How Ukraine's journalists are covering the invasion of their country*. CNN. https://www.cnn.com/2022/02/25/media/kyiv-post-ukraine-journalists/index.html

Debusmann, B., Jr. (2022, March 10). How "Saint Javelin" raised over $1m for Ukraine. *BBC News*. https://www.bbc.com/news/world-us-canada-60700906

Department of Homeland Security (2014). *Response to FOIA request for Operation Aurora documents.* Department of Homeland Security. https://cdn.muckrock.com/foia_files/14f00304-Documents.pdf

Delcker, J. (2022, March 24). *Ukraine's IT army: Who are the cyber guerrillas hacking Russia? | DW | 24.03.2022*. DW. https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527

Digital Forensics Lab. (2022, March 16). Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/

Digital Security Unit. (2022, April 27). *Special report: Ukraine - An overview of Russia's cyberattack activity in Ukraine.* Microsoft. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Dobbs, T., Marsh, T., Fallon, G., Fouhy, S., & Melville, L. (2020). *Grey-zone activities and the ADF.* The Perry Group. https://theforge.defence.gov.au/sites/default/files/2020-10/Grey%20Zone_0.pdf

Dwyer, J., & Henson, K. (2022, March 4). New wiper malware used against Ukranian organizations. *Security Intelligence*. https://securityintelligence.com/posts/new-wiper-malware-used-against-ukranian-organizations/

Dykstra, J., & Paul, C. L. (2018). Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. *2018 11th USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, United States. https://www.researchgate.net/profile/Celeste-Paul/publication/328563149_Cyber_Operations_Stress_Survey_COSS_Studying_fatigue_frustration_and_cognitive_workload_in_cybersecurity_operations/links/5bd4cc7da6fdcc3a8daa3ff3/Cyber-Operations-Stress-Survey-COSS-Studying-fatigue-frustration-and-cognitive-workload-in-cybersecurity-operations.pdf

Dylevsky, I. N., Zapivakhin, V. O., Komov, S. A., Petrunin, A. N., & Elias, V. P. (2015). Военно-политические аспекты государственной политики Российской Федерации вобласти международной информационной безопасности [Military and political aspects of the state policy of the Russian Federation in the field of the international information security]. *Военная мысль* [Military Though], 1(1), 11–17. https://www.elibrary.ru/item.asp?id=22905434

Elgueta, A. (2022, March 6). *British spies use Grindr and social networks to track Putin's soldiers.* Mirror. https://www.mirror.co.uk/news/world-news/british-spies-use-dating-app-26397220

Ehrlich, A. B. S. (2022, March 15). *Threat actor UAC-0056 targeting Ukraine with fake translation software*. SentinelOne. https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/

ESET. (2016, May 18). *Операция Groundbait: Украинские окупированные территории подверглись атакам кибершпиона* [Operation Groundbait: Ukrainian occupied territories were attacked by a cyberspy]. https://eset.ua/ru/news/view/447/Operation-Groundbait-Ukrainian-occupied-territories-were-subjected-to-attacks-cyberspy

ESET. (2022a, February 24). *HermeticWiper: New data-wiping malware hits Ukraine.* WeLiveSecurity. https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

ESET. (2022b, March 1). *IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine*. WeLiveSecurity. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

ESET. (2022c, March 14). *CaddyWiper: New wiper malware discovered in Ukraine*. WeLiveSecurity. https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

ESET. (2022d, April 12). *Industroyer2: Industroyer reloaded*. WeLiveSecurity. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Estonian Foreign Intelligence Service. (2022). *International security and Estonia 2022.* Estonian Foreign Intelligence Service. https://www.valisluureamet.ee/doc/raport/2022-en.pdf

F-Secure Labs. (2019). *BLACKENERGY & QUEDAGH: The convergence of crimewar and APT attacks* [White paper]. F-Secure. https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf

Fabiani, A. (2022, March 23). *Join the Tinder war: How the dating app is helping fight Russian propaganda and house Ukrainian refugees.* Screenshot. https://screenshot-media.com/technology/apps/tinder-war-ukraine/

Falliere, N., Murchu, L. O., & Chien, E. (2010). W32.Stuxnet dossier. Symantec Security Response.

Figliola, B. M. (2020), *The internet of things (IoT): An overview* [Report No. IF11239, Version 5]. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11239

Gaffney, J. M. (2022). *"Hacktivists" and the Ukraine-Russia conflict: Legal considerations* (No. LSB10743, Version 2). Congressional Research Service. https://crsreports.congress.gov/product/pdf/LSB/LSB10743

Garson, M., & Furlong, P. (2022). *Disrupters and Defenders: What the Ukraine War Has Taught Us About the Power of Global Tech Companies*. Tony Blair Institute for Global Change. https://institute.global/policy/disrupters-and-defenders-what-ukraine-war-has-taught-us-about-power-global-tech-companies

Gatlan, S. (2022, March 3). *Ukraine says local govt sites hacked to push fake capitulation news*. BleepingComputer. https://www.bleepingcomputer.com/news/security/ukraine-says-local-govt-sites-hacked-to-push-fake-capitulation-news/

Gleicher, N., & Agranovich, D. (2022, February 28). Updates on Our Security Work in Ukraine. *Meta*. https://about.fb.com/news/2022/02/security-updates-ukraine/

Greenberg, A. (2018, August 22). the untold story of NotPetya, the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Guerrero-Saade, J. A., & van Amerongen, M. (2022, March 31). *AcidRain | A modem wiper rains down on Europe*. SentinelOne. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

Halpert, M. (2022, April 28). *Ukraine charges Russian soldiers for involvement in Bucha massacre*. Forbes. https://www.forbes.com/sites/madelinehalpert/2022/04/28/ukraine-charges-russian-soldiers-for-involvement-in-bucha-massacre/

Hartikainen, J. (2022, May 3–5). *Sähkönjakelun kyberturvallisuus ja huoltovarmuus* [Cyber security and maintenance reliability of electricity distribution] [Conference Presentation]. Teknologia 22, Helsinki, Finland.

Hasu, T. (2014). Kybersodankäyntiä koskevan lainsäädännön tarkastelua [Analysis of legislation regarding of cyber warfare]. In Kuusisto, T. (Ed.), *Kybertaistelu 2020* (pp. 62–66). Maanpuolustuskorkeakoulu.

Hayden, M. (2016). *Playing to the edge: American intelligence in the age of terror*. New York: Penguin Random House.

Horejsi, J., & Pernet, C. (2022, March 8). *New RURansom wiper targets Russia*. Trend Micro. https://www.trendmicro.com/en_us/research/22/c/new-ruransom-wiper-targets-russia.html

Huntley, S. (2022, March 7). *An update on the threat landscape*. Google Threat Analysis Group. https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/

Huoltovarmuusorganisaation Digipooli. (2020). Kyberturvallisuuden nykytila eri toimialoilla [Current state of the cyber security in different fields]. https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Ilascu, I. (2020, June 18). *InvisiMole malware delivered by Gamaredon hacker group*. BleepingComputer. https://www.bleepingcomputer.com/news/security/invisimole-malware-delivered-by-gamaredon-hacker-group/

International Committee of the Red Cross. (2013). *Cyberwarfare and international humanitarian law: the ICRC's position.* https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf

JAMK. (2018). *Ethical principles for JAMK university of applied sciences approved by the student affairs board on 11 December 2018.* Jyväskylä University of Applied Sciences. https://www.jamk.fi/en/media/34826

Janofsky, A. (2022, March 4). This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites. *The Record by Recorded Future*. https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites/

Joint Chiefs of Staff. (1995). Military operations other than war (JP 3-07). https://www.bits.de/NRANEU/others/jp-doctrine/jp3_07.pdf

Joint Chiefs of Staff. (2010). Joint operations (JP 3-0). http://edocs.nps.edu/dod-pubs/topic/jointpubs/JP3/JP3-0_100322.pdf

Joint Chiefs of Staff. (2014). *Information operations* (JP 3-13). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Joint Chiefs of Staff. (2018). *Cyberspace operations* (JP 3-12). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Kaminska, M., Shires, J., & Smeets, M. (2022). *Cyber operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)* [Workshop report]. European Cyber Conflict Research Initiative. https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf

Kaplan, F. M. (2016). *Dark territory: The secret history of cyber war.* New York: Simon and Schuster.

Kari, M. J. (2018). *Venäläinen strateginen kulttuuri - miksi Venäjä toimii niin kuin se toimii?* [Russian strategic culture - Why Russia does what it does?] [Video lecture]. University of Jyväskylä. https://m3.jyu.fi/jyumv/ohjelmat/it/panu/kyber/hybridivaikuttaminen-ja-turvallisuus/031218

Ketelhut, S., Martin-Niedecken, A. L., Zimmermann, P., & Nigg, C. R. (2021). Physical activity and health promotion in esports and gaming–discussing unique opportunities for an unprecedented cultural phenomenon. *Frontiers in Sports and Active Living, 3.* https://doi.org/10.3389/fspor.2021.693700

Kovacs, E. (2022a, March 21). Ukrainian security researcher leaks newer Conti ransomware source code. *SecurityWeek.* https://www.securityweek.com/ukrainian-security-researcher-leaks-newer-conti-ransomware-source-code

Kovacs, E. (2022b, April 8). Microsoft disrupts infrastructure used by Russia’s hackers in Ukraine attacks. *SecurityWeek.* https://www.securityweek.com/microsoft-disrupts-infrastructure-used-russias-hackers-ukraine-attacks

Kovacs, E. (2022c, June 2). Leaks show Conti ransomware group working on firmware exploits. *SecurityWeek.* https://www.securityweek.com/leaks-show-conti-ransomware-group-working-firmware-exploits

Kreuzer, M. P. (2021, July 8). *Cyberspace is an analogy, not a domain: Rethinking domains and layers of warfare for the information age*. The Strategy Bridge. https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age

Kukkola, J. (2021). *Rakenteellisen kyberasymmetrian strategiset vaikutukset: Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä* [Strategical influence of structural cyber asymmetry: Russia's national internet segment as a military strategic phenomenon] [Master's thesis, Maanpuolustuskorkeakoulu]. Doria. https://urn.fi/URN:NBN:fi-fe2021110353681

Laari, T. (Ed.). (2019). *#kyberpuolustus* [#cyberdefence]. Helsinki: Maanpuolustuskorkeakoulu.

Lakshmanan, R. (2022, March 7). *Ukrainian CERT Warns Citizens of Phishing Attacks Using Compromised Accounts*. The Hacker News. https://thehackernews.com/2022/03/ukrainian-cert-warns-citizens-of.html

Lantto, H., Åkesson, B., Kukkola, J., Nikkarila, J., & Ristolainen, M. (2019). Wargaming a closed national network: What are you willing to sacrifice? In Kukkola, J., Ristolainen, M., & Nikkarila, J. (Eds.). *Game player* (pp. 135–152). Maanpuolustuskorkeakoulu.

Lapienytė, J. (2022, March 16). *Russia's cyber weapons might be as weak as its artillery, says expert*. CyberNews. https://cybernews.com/cyber-war/russias-cyber-weapons-might-be-as-weak-as-its-artillery-says-expert/

Lee, M. (2022, April 22). *Russia is losing a war against hackers stealing huge amounts of data*. The Intercept. https://theintercept.com/2022/04/22/russia-hackers-leaked-data-ukraine-war/

Lehto, M. (2014). Kybersodankäyntiä koskevan lainsäädännön tarkastelua [Analysis of legislation regarding of cyber warfare]. In Kuusisto, T. (Ed.), *Kybertaistelu 2020* (pp. 157–178). Maanpuolustuskorkeakoulu.

Lehto, M., & Henselmann, G. (2019). Where cyber meets the electromagnetic spectrum. In T. Cruz, & P. Simoes (Eds.), *ECCWS 2019: Proceedings of the 18th European Conference on Cyber Warfare and Security* (pp. 209-218). Academic Conferences International. Proceedings of the European conference on information warfare and security.

Lehto, M., & Henselmann, G. (2020). Non-kinetic warfare – The new game changer in the battle space. In B. K. Payne, & H. Wu (Eds.), *ICCWS 2020: Proceedings of the 15th International Conference on Cyber Warfare and Security* (pp. 316-325). Academic Conferences International. The proceedings of the international conference on cyber warfare and security. https://doi.org/10.34190/ICCWS.20.033

Leonard, B. (2022, July 19). *Continued cyber activity in Eastern Europe observed by TAG*. Google Threat Analysis Group. https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/

Libicki, M. C. (1995). *What is information warfare?* United States Government Printing.

Limnéll, J., Majewski, K., & Salminen, M. (2014). *Kyberturvallisuus.* Docendo Oy.

LMR press service. (2022, May 14). *The hackers tried to break into the Internet networks and services of the Lviv City Hall*. Lviv City Council. https://city-adm.lviv.ua/news/society/security/291547-khakery-namahalys-zlamaty-internet-merezhi-ta-servisy-merii-lvova

Lockheed Martin. (2011). *Cyber kill chain*. Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Lyngaas, S. (2022, June 2). *US confirms military hackers have conducted cyber operations in support of Ukraine.* CNN. https://www.cnn.com/2022/06/02/politics/us-hackers-ukraine-support/index.html

Malhotra, A. (2022, March 24). Threat Advisory: DoubleZero. *Talos Intelligence*. http://blog.talosintelligence.com/2022/03/threat-advisory-doublezero.html

Mandiant. (2022, April 27). *Assembling the Russian Nesting Doll: UNC2452 Merged into APT29.* Mandiant. https://www.mandiant.com/resources/unc2452-merged-into-apt29

Martin, A. (2022, May 10). *Ukraine War: UK, US, and EU officially blame Russia for cyber attack targeting satellite company*. Sky News. https://news.sky.com/story/ukraine-war-uk-us-and-eu-officially-blame-russia-for-cyber-attack-targeting-satellite-company-12609862

Maschmeyer, L., & Cevelty, M. D. (2022). Goodbye cyberwar: Ukraine as reality check. *CSS Policy Perspectives*, *10*(3), 1–4. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf

Maslow, A., H. (1943). A theory of human motivation. *Psychological Review, 50*(4), 370–396.

Maslow, A., H. (1954). *Motivation and personality.* New York: Harper and Row.

Maunder, M. (2022, March 1). Ukraine universities hacked as Russian invasion started. *Wordfence*. https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/

Maurer, T. (2018). Cyber proxies and their implications for liberal democracies. *The Washington Quarterly, 41*(2), 171-188. https://doi.org/10.1080/0163660X.2018.1485332

McGhee, J. (2016). Liberating cyber offense. *Strategic Studies Quarterly, 10*(4), 46–63. https://www.jstor.org/stable/26271529

McWhorter, D. (2014, October 27). *APT28: A window into Russia's cyber espionage operations?* Mandiant. https://www.mandiant.com/resources/apt28-a-window-into-russias-cyber-espionage-operations

Mercer, W., & Ventura, V. (2021, February 23). Gamaredon—When nation states don't pay all the bills. *Talos Intelligence*. http://blog.talosintelligence.com/2021/02/gamaredonactivities.html

Metro. (2022, February 26). Anonymous leaks Russian MoD database in major victory during cyberwar. *Metro*. https://metro.co.uk/2022/02/26/anonymous-leaks-russian-mod-database-in-major-victory-during-cyberwar-16179039/

Microsoft. (2022, June 22). *Defending Ukraine: Early lessons from the cyber war.* Microsoft. https://aka.ms/June22SpecialReport

Microsoft Security. (2022, January 16). *Destructive malware targeting Ukrainian organizations.* https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Ministry of Defence. (2016). *Cyber primer* (2nd ed.). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf

MITRE. (2021). MITRE adversarial tactics, techniques, and common knowledge (ATT&CK®) framework [Version 8.2]. Retrieved June 16, 2022, from https://attack.mitre.org/versions/v8/techniques/enterprise/

Morag, N. (2014). *Cybercrime, cyberespionage and cybersabotage: Understanding emerging threats* [White paper]. Colorado Technical University. https://www.coloradotech.edu/media/default/CTU/documents/resources/cybercrime-white-paper.pdf

Moss, S. (2022a, March 10). *Ukraine's Ukrtelecom goes down nationwide for 40m, ISP Triolan outage caused by cyber attack*. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/ukraine-ukrtelecom-goes-down-nationwide-for-40m-isp-triolan-outage-caused-cyber-attack/

Moss, S. (2022b, March 14). *Ukraine: Internet outages in Sumy and Vinnytsia Oblast.* Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/ukraine-internet-outages-in-sumy-and-vinnytsia-oblast/

Mueller, R. S. (2019). *Report on the investigation into Russian interference in the 2016 presidential election.* U. S. Department of Justice. https://www.justice.gov/storage/report.pdf

Mukherjee, S., & Fulton, C. (2021, July 5). *Coop, other ransomware-hit firms, could take weeks to recover, say experts*. Reuters. https://www.reuters.com/technology/coop-other-ransomware-hit-firms-could-take-weeks-recover-say-experts-2021-07-05/

Murphy, M. (2010, July 1). War in the fifth domain. *The Economist*, *396*(8689). https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

Nakashima, E. (2018, January 12). Russian military was behind ‘NotPetya’ cyberattack in Ukraine, CIA concludes. *Washington Post*. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

Nakashima, E. (2022, March 4). Ukraine says its nuclear plants and other key systems are more vulnerable to physical than cyberattacks. *Washington Post*. https://www.washingtonpost.com/national-security/2022/03/04/ukraine-nuclear-cyberattack/

National Cybersecurity and Communications Integration Center. (2016). *GRIZZLY STEPPE – Russian malicious cyber activity* [Report No. JAR-16-20296A]. U.S. Department of Homeland Security. https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

National Cybersecurity and Communications Integration Center. (2017). *Enhanced Analysis of GRIZZLY STEPPE Activity* [Report No. AR-17-20045]. U.S. Department of Homeland Security. https://www.cisa.gov/uscert/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 43*(3): 44–71. https://doi.org/10.1162/ISEC_a_00266

Office of Information Security. (2022). *Major Cyber Organizations of the Russian Intelligence Services* [Report No. 202205191300]. The Health Sector Cybersecurity Coordination Center.

https://www.hhs.gov/sites/default/files/major-cyber-organizations-of-russian-intelligence-services.pdf

OLL.TV. (2022, June 5). *Заздрісна русня намагається зіпсувати глядачам перегляд матчу Збірної за вихід до ЧС-2022. Докладаємо максимальних зусиль для якнайшвидшої нейтралізації кібератаки.* [The envious Russia is trying to spoil the viewing of the National Team's match for the 2022 World Cup. We make every effort to neutralize the cyber attack as soon as possible.] [Image]. https://www.facebook.com/OLL.TV/photos/a.362196673828899/4991376950910825/

Omand, D. (2016). Understanding digital intelligence. In Silva, E. D. (Ed.), *National security and counterintelligence in the era of cyber espionage* (pp. 97–121). Hershey: Information Science Reference.

Ormrod, D., & Turnbull, D. (2016). The cyber conceptual framework for developing military doctrine. *Defence studies, 16*(3), 270–298. https://doi.org/10.1080/14702436.2016.1187568

Padmalaya, N., Niranjan, R., & Ravichandran, P. (Eds.). (2022). *IoT applications, security threats, and countermeasures (Internet of everything IoE)*. CRC Press.

Pannett, R., & Shammas, B. (2022, June 9). Hacked Russian radio station broadcasts Ukrainian anthem. *Washington Post*. https://www.washingtonpost.com/world/2022/06/09/russia-radio-station-hacked-ukraine-anthem-kommersant/

Patella-Rey, P. (2012, February 1). *There is no “cyberspace.”* https://thesocietypages.org/cyborgology/2012/02/01/there-is-no-cyberspace/

PBS. (2022, February 15). *Cyberattacks take down Ukrainian government and bank websites*. PBS NewsHour. https://www.pbs.org/newshour/world/cyberattacks-take-down-ukrainian-government-and-bank-websites

Peters, G., Portman, R., Klobuchar, A., & Blunt, R. (2021). *Examining the U.S. Capitol attack.* United States Senate. https://www.rules.senate.gov/download/hsgac-rules-jan-6-report

Peterson, A., & Cimpanu, C. (2022, February 25). *Russia appears to deploy digital defenses after DDoS attacks.* The Record by Recorded Future. https://therecord.media/russia-appears-to-deploy-digital-defenses-after-ddos-attacks/

Pitrelli, M. B. (2022, March 16). *Anonymous declared a "cyber war" against Russia. Here are the results.* CNBC. https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html

Polityuk, P. (2022, April 22). Ukraine's postal service hit by cyberattack after sales of warship stamp go online. *Reuters*. https://www.reuters.com/world/europe/ukraines-postal-service-hit-by-cyberattack-after-sales-warship-stamp-go-online-2022-04-22/

Pomerleau, M. (2021, April 14). *US military to blend electronic warfare with cyber capabilities.* C4ISRNET. https://www.c4isrnet.com/electronic-warfare/2021/04/14/us-military-to-blend-electronic-warfare-with-cyber-capabilities/

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks* [Briefing]. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Prunckun, H. (2018). Weaponization of Computers. In Prunckun, H. (Ed.), *Cyber weaponry: Issues and implications of digital arms* (pp. 1–12). Sydney: Springer.

Psaki, J., Neuberger, A., & Singh, D. (2022, February 19). *Press briefing by press secretary Jen Psaki, deputy national security advisor for cyber and emerging technology Anne Neuberger, and deputy national security advisor for international economics and deputy NEC director Daleep Singh, February 18, 2022.* The White House. https://www.whitehouse.gov/briefing-room/press-briefings/2022/02/18/press-briefing-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-and-deputy-national-security-advisor-for-international-economics-and-dep/

Puolustusministeriö. (2010). *Yhteiskunnan turvallisuusstrategia* [The security strategy for society]. https://turvallisuuskomitea.fi/wp-content/uploads/2015/10/yts_2010_fi_nettiin.pdf

Quinlan, M. (2007). Just intelligence: Prolegomena to an ethical theory. *Intelligence and National Security, 22*(1), 1–13. https://doi.org/10.1080/02684520701200715

Raggi, M., & Cass, Z. (2022, March 1). *Asylum ambuscade: State actor uses compromised private Ukrainian military emails to target European governments and refugee movement*. Proofpoint. https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

Revay, G. (2022, April 28). An Overview of the Increasing Wiper Malware Threat | FortiGuard Labs. *Fortinet*. https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

Romanosky, S., & Boudreaux, B. (2019). *Private sector attribution of cyber incidents: Benefits and risks to the U.S. government* [Working paper]. RAND Corporation. https://doi.org/10.7249/WR1267

Rousku, K., Härkönen, J., Cederberg, A., & Hartikainen, J. (2022, May 3–5). *Venäjän hyökkäys Ukrainaan – miten digitaalinen maailma on muuttunut? Miten tilanteeseen tulisi varautua? Miltä tulevaisuus näyttää?* [Russia's attack to Ukraine – How is the digital world changed? How should we prepare for the situation? How does the future look like?] [Panel discussion]. Teknologia 22, Helsinki, Finland.

Russian Federation presidential edict. (2010). *The Military Doctrine of the Russian Federation* [Translated]. The Russian Federation. http://carnegieendowment.org/files/2010russia_military_doctrine.pdf

Sambaluk, N. M. (2020). *Myths and realities of cyber warfare: conflict in the digital realm.* Santa Barbara: ABC-CLIO.

Sander, B. (2019). *The sound of silence: International law and the governance of peacetime cyber operations.* 2019 11th International Conference on Cyber Conflict (CyCon). https://doi.org/10.23919/CYCON.2019.8756882

Satter, R. (2022a, March 3). Ukrainians say hackers used local government sites to spread fake "capitulation" news. *Reuters*. https://www.reuters.com/world/europe/ukrainians-say-hackers-used-local-government-sites-spread-fake-capitulation-news-2022-03-03/

Satter, R. (2022b, March 5). Ukrainian websites under "nonstop" attack—Cyber watchdog agency. *Reuters*. https://www.reuters.com/world/europe/ukrainian-websites-under-nonstop-attack-cyber-watchdog-agency-2022-03-05/

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

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations.* New York: Cambridge University Press.

Schultz, J. (2022, July 21). Attackers target Ukraine using GoMet backdoor. *Talos Intelligence.* http://blog.talosintelligence.com/2022/07/attackers-target-ukraine-using-gomet.html

Schwarz, D. (2022, March 2). DanaBot Launches DDoS Attack Against the Ukrainian Ministry of Defense. *Security Boulevard*. https://securityboulevard.com/2022/03/danabot-launches-ddos-attack-against-the-ukrainian-ministry-of-defense/

Security Service of Ukraine. (2021). *Gamaredon/Armageddon group: FSB cyber attacks against ukraine.* https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf

Security Service of Ukraine. (n.d.-a). *Mission and values*. Retrieved June 30, 2022, from https://ssu.gov.ua/en/misia-ta-tsinnosti

Security Service of Ukraine. (n.d.-b). *Cyber Security Situation Centre*. Retrieved June 30, 2022, from https://ssu.gov.ua/en/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky

Security Service of Ukraine. (2022c, March 28). *З початку війни СБУ ліквідувала 5 ворожих ботоферм потужністю понад 100 тис. Фейкових акаунтів* [Since the beginning of the war, the SBU has liquidated 5 enemy bot farms with a capacity of more than 100 thousand fake accounts]. https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv

Seedyk, C. (2018). Characterizing cyber intelligence as an all-source intelligence product. *DSIAC Journal, 5*(3), 4–10. https://dsiac.org/wp-content/uploads/2020/05/dsiac-summer-2018-vol-5-no-3.pdf

Shchepanskaya, M. (2022, May 15). *Consequences of a cyber attack on Lviv: Part of the data was stolenl*. Lviv City Council. https://city-adm.lviv.ua/news/government/291555-naslidky-kiberataky-na-lviv-vykradeno-chastynu-danykh

Shore, J. (2022, June 8). *Don’t Underestimate Ukraine’s Volunteer Hackers.* Foreign Policy. https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/

Sinovets, P., Renz, B. (2015). Russia's 2014 military doctrine and beyond: Threat perceptions, capabilities and ambitions. NATO Defense College. http://www.ndc.nato.int/download/downloads.php?icode=457

Slaney, R. (2022, March 10). SecurityScorecard Discovers new botnet, ‘Zhadnost,’ responsible for Ukraine DDoS attacks. *SecurityScorecard*. https://securityscorecard.com/blog/securityscorecard-discovers-new-botnet-zhadnost-responsible-for-ukraine-ddos-attacks

Slovo i Dilo. (2022, March 17). *СБУ повідомила про масову хакерську атаку на сайти популярних онлайн-видань в Україні* [The SBU reported a massive hacker attack on the sites of popular online publications in Ukraine]. https://www.slovoidilo.ua/2022/03/17/novyna/suspilstvo/sbu-povidomyla-pro-masovu-xakersku-ataku-sajty-populyarnyx-onlajn-vydanukrayini

Sly, L. (2022, April 23). *The Belarusian railway workers who helped thwart Russia's attack on Kyiv.* Washington Post. https://www.washingtonpost.com/world/2022/04/23/ukraine-belarus-railway-saboteurs-russia/

Smith, T. E. (2013). Cyber Warfare: A Misrepresentation of the True Cyber Threat. *American Intelligence Journal, 31*(1), 82–85. http://www.jstor.org/stable/26202046

SOCRadar. (2021, September 22). Dark web threat profile: Conti ransomware group. *SOCRadar® Cyber Intelligence Inc.* https://socradar.io/dark-web-threat-profile-conti-ransomware-group/

SOCRadar. (2022, May 20). Conti ransomware ended: They operate with other groups now. *SOCRadar® Cyber Intelligence Inc.* https://socradar.io/conti-ransomware-ended-they-operate-with-other-groups-now/

Soesanto, S. (2022). *The IT Army of Ukraine: Structure, Tasking, and Ecosystem*. Center for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf

SSSCIP. (2022a, May 10). *Russian hackers have landed a massive DDoS attack on Ukrainian telecom operators' websites*. State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/en/news/rosiiski-khakeri-zdiisnili-masshtabnu-ddos-ataku-na-saiti-ukrayinskikh-telekom-operatoriv

SSSCIP. (2022b, June 6). *Russian cyberattack on the OLL.TV service*. State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/en/news/kiberataka-rosiyi-na-servis-oll-tv

SSSCIP. (2022c, June 30). *Чотири місяці війни: Статистика кібератак* [Four months of war: Statistics of cyberattacks]. https://cip.gov.ua/ua/news/chotiri-misyaci-viini-statistika-kiberatak

SSSCIP. (2022d, July 12). *The malware-spreading activity of hacker groups has increased*. https://cip.gov.ua/en/news/zrosla-aktivnist-khakerskikh-grup-shodo-rozpovsyudzhennya-shkidlivogo-programnogo-zabezpechennya

SSSCIP. (2022e, July 12). *Russian hackers keep attacking the Ukrainian infrastructure and descending to civilian targets*. https://cip.gov.ua/en/news/rosiiski-khakeri-prodovzhuyut-atakuvati-ukrayinsku-infrastrukturu-ne-grebuyuchi-civilnimi-cilyami

SSSCIP. (n.d.-c). *About the SSSCIP.* State Service of Special Communications and Information Protection of Ukraine. Retrieved June 30, 2022, from https://cip.gov.ua/en/statics/veterani-derzh-speczv-yazku-organizuvali-volonterskii-khab-dlya-civilnikh-ta-viiskovikh

Stanton, A. (2022, April 3). Anonymous apparently behind doxing of 120K Russian soldiers in Ukraine war. Newsweek. https://www.newsweek.com/anonymous-leaks-personal-data-120k-russian-soldiers-fighting-ukraine-1694555

Stech, F. J., & Heckman, K. E. (2018). Human nature and cyber weaponry: use of denial and deception in cyber counterintelligence. In Prunckun, H. (Ed.). *Cyber weaponry: Issues and implications of digital arms.* Sydney: Springer.

Stokel-Walker, C., & Milmo, D. (2022, March 15). ‘It’s the right thing to do’: The 300,000 volunteer hackers coming together to fight Russia. *The Guardian*. https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia

Springer, P. J. (2015). *Cyber warfare: A reference handbook.* Santa Barbara: ABC-CLIO.

Springer, P. J. (2020). *Cyber warfare: A documentary and reference guide.* Santa Barbara: Greenwood.

Swed, O., & Crosbie, T. (2019, March 14). *Who are the private contractors in Iraq and Afghanistan?* Military Times. https://www.militarytimes.com/news/your-navy/2019/03/14/who-are-the-private-contractors-in-iraq-and-afghanistan/

Tarabay, J. (2022, April 20). *An underwater hack and the digital ripple effects*. Bloomberg. https://www.bloomberg.com/news/newsletters/2022-04-20/an-underwater-hack-and-the-digital-ripple-effects

TAVR Media. (2022, July 21). *Увага, важлива інформація! Сьогодні було здійснено кібератаку на сервери та мережі радіостанцій TAVR Media. В даний момент відповідні служби працюють* [Attention, important information! Today, a cyber attack was carried out on the servers and networks of TAVR Media radio stations. At the moment, the relevant services are working] [Status update]. Facebook. https://www.facebook.com/tavrmedia/posts/pfbid0voE4Ft6pfrDKKQ5iyrkk11ydPtBYcZJsMAW3VW27HQQy3nn6cRyLUSLZysqsSNyHl

The Embassy of the Russian Federation to United Kingdom of Great Britain and Northern Ireland. (2015). *The Military Doctrine of the Russian Federation* [Translated]. The Russian Federation. https://rusemb.org.uk/press/2029

Thomson, I. (2017, June 28). *Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide*. https://www.theregister.com/2017/06/28/petya_notpetya_ransomware/

Threat Intelligence Team. (2022, March 9). FormBook spam campaign targets citizens of Ukraine. *Malwarebytes Labs*. https://blog.malwarebytes.com/threat-intelligence/2022/03/formbook-spam-campaign-targets-citizens-of-ukraine/

Toffler, A. & Toffler, H. (1993). *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little Brown & Co.

Treisman, R. (2022, May 9). Patron the bomb-sniffing dog cements his hero status with a presidential medal. *NPR*. https://www.npr.org/2022/05/09/1097585032/patron-dog-ukraine-zelenskyy-medal

Trellix. (2022, June 6). *Growling bears make thunderous noise*. https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/growling-bears-make-thunderous-noise.html

Tucker, M. (2022a, April 1). *China accused of hacking Ukraine days before Russian invasion*. The Times. https://www.thetimes.co.uk/article/china-cyberattack-ukraine-z9gfkbmgf

Tucker, M. (2022b, April 11). *Video of Ukrainian soldiers with pets shows their softer side*. https://www.thetimes.co.uk/article/video-of-ukrainian-soldiers-with-pets-shows-their-softer-side-dd82d6lpg

Ukraine Center for Strategic Communications. (2022, January 14). *Атака на урядові сайти: Новий розділ кібервійни проти України* [Attack on government sites: A new chapter in the cyber war against Ukraine]. https://spravdi.gov.ua/ataka-na-uryadovi-sajty-novyj-rozdil-kibervijny-proty-ukrayiny/

Ukrainian Red Cross [@RedCrossUkraine]. (2022, March 16). *The official website of the Ukrainian Red Cross is hacked! No personal data of beneficiaries was stored on the website* [Image attached] [Tweet]. Twitter. https://twitter.com/RedCrossUkraine/status/1504123401941790720

Unit 42. (2022, February 25). *OutSteel, SaintBot delivered by spear phishing attacks targeting Ukraine*. Palo Alto Networks. https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

United Nations. (1977). *Protocol additional to the Geneva conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol 1)*. OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and

United States district court western district of Pennsylvania. (2020, October 15). *United States of America V. Yuriy Sergeyev Ich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevichfrolov,* *Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin, defendants* [Press Release]. U.S. Department of Justice. https://www.justice.gov/opa/press-release/file/1328521/download

U.S. Air Force. (2011). *Cyberspace operations* (AFDP 3-12). https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

U.S. Air Force. (2020). *A doctrine primer (2nd ed.)*. https://www.doctrine.af.mil/Portals/61/documents/Doctrine_Primer/A%20Primer%20on%20Doctrine%208%20Oct%2020%20v2.pdf

van Niekerk, B., & Maharaj, M. (2010). *Mobile Security from an Information Warfare Perspective.* https://digifors.cs.up.ac.za/issa/2010/Proceedings/Full/06_Paper.pdf

Vavra, S. (2019, May 6). *It was “inevitable” that bombs would fall in response to a cyberattack*. CyberScoop. https://www.cyberscoop.com/hamas-cyberattack-israel-air-strikes/

Viasat. (2022, March 30). *KA-SAT Network cyber attack overview*. Viasat Corporate. https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

Volz, D. (2022, February 23). Some Ukrainian government, banking websites disrupted again. *The Wall Street Journal.* https://www.wsj.com/livecoverage/russia-ukraine-latest-news/card/some-ukrainian-government-banking-websites-disrupted-again-HnTGLkoVmpezDz8UBdPY

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., & Schwarzenbach, A. (2020). National cyber power index 2020: Methodology and analytical considerations. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage*. Minnesota Journal of International Law, 22*(347). https://scholarship.law.umn.edu/faculty_articles/223

Welch, L. D. (2011). *Cyberspace - The fifth operational domain.* IDA. https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx

Williams, R. (2022, March 7). *Anonymous hacking group troll Russia with meme on military radio broadcast.* Inews.Co.Uk. https://inews.co.uk/news/anonymous-hacking-group-troll-russia-with-meme-on-military-radio-broadcast-1501848

YLE. (2014, July 2). *Secret services: Cyber spies twice penetrated Foreign Ministry*. https://yle.fi/news/3-7334589

YLE. (2017, January 13). *Russian group behind 2013 Foreign Ministry hack.* https://yle.fi/news/3-8591548

Zhadan, A. (2022a, May 12). *Starlink: Fighting for Ukraine on the cyber front*. CyberNews. https://cybernews.com/cyber-war/starlink-fighting-for-ukraine-on-the-cyber-front/

Zhadan, A. (2022b, May 17). *Key highlights of Russia's cyber aggression against Ukraine: Has Russia exhausted its digital arsenal?* CyberNews. https://cybernews.com/cyber-war/key-highlights-of-russias-cyber-aggression-against-ukraine-has-russia-exhausted-its-digital-arsenal/

Appendices

Appendix 1. APT Actors and Hacktivists Affiliated to Russia

Name	Organization	Aliases
Fancy Bear	GRU, 85th Main Special Service Centre, military unit 26165	APT28, Pawn Storm, STRONTIUM, Threat Group-4127, TG-4127, SNAKEMACKEREL, Swallowtail, IRON TWILIGHT, Sofacy, SIG40, Tsar Team, Group 74, Unit 26165, UAC-0028, Frozen Lake, Zebrocy, Sednit, AKT 5, T-APT-12, TAG-0700
Voodoo Bear	GRU, Main Centre of Special Technologies, military unit 74455	Sandworm, BlackEnergy, Unit 74455, GTsST, Telebots, Iron Viking, Quedagh, ELECTRUM, UAC-0082, IRIDIUM, TEMP.Noble, ATK 14, DEV-0665
Ember Bear	[Suspected GRU]	Lorec53, LoriBear, UAC-0056, TA471, SaintBear, BleedingBear, UNC-2589, DEV-0586
Cozy Bear	SVR	APT29, CozyCar, CozyDuke, Dark Halo, The Dukes, NOBELIUM, Office Monkeys, StellarParticle, UNC2452, YTTRIUM, UAC-0029, IRON HEMLOCK, IRON RITUAL, NobleBaron
Primitive Bear	FSB	Gamaredon, Shuckworm, ACTINIUM, UAC-0010, Armageddon, IRON TILDEN, DEV-0157, Winterflouder, BlueAlpha, BlueOtso, SectorC08, Calisto, APT-C-53, COLDRIVER
Venomous Bear	FSB	Turla, KRYPTON, Uroboros, Snake, Waterbug, IRON HUNTER, Group 88, WRAITH, Hippo Team, Popeye, SIG23, MAKERSMARK, WhiteBear, Belugasturgeon, Popeye, TAG_0530, Pfinet
Berserk Bear	FSB	Energetic Bear, DragonFly, Crouching Yeti, TEMP.Isotope, BROMINE IRON LIBERTY, DYMALLOY, TG-4192
GRIZZLY STEPPE	GRU & SVR	[*Joint operations of Fancy Bear & Cozy Bear*]
XENOTIME	TsNIIKhM	Temp.Veles
Wizard Spider	Organized crime	Conti, Trickbot, UNC1878, TEMP.MixMaster, Grim Spider, UAC-0098, Gold Ulrick, Gold Blackburn, ITG23
InvisiMole	Organized crime	UAC-0035, LoadEdge, TunnelMole [*Linked to Gamaredon*]

The Red Bandits	Organized crime	TheRedBanditsRU
CyberGhost	Organized crime	
Mummy Spider	Organized crime	TA542, TEMP.Mixmaster, UNC3443, Gold Crestwood
Salty Spider	Organized crime	Sality
Scully Spider	Organized crime	Gold Opera
Smokey Spider	Organized crime	
Wizard Spider	Organized crime	Gold Ulrick, UNC2727
The Xaknet Team	Organized crime	[*Linked to Killnet group*]
The CoomingProject	Organized crime	
Vermin	“Security Agency for Luhansk People’s Republic”	SPECTR, UAC-0020
NEARMISS	Unknown	SunFlowerSeed, UAC-3715
AcidRain	Unknown	[*Linked to Voodoo Bear*]
SunSeed	Unknown	Asylum Ambuscade, UAC-0064 [*Similar to Belarusian Ghostwriter*]
KillNet	Unknown	UAC-0108 [*Linked to The XakNet Team*]
TA416	Unknown	UAC-0086
Stormous Ransomware	Unknown	
Hydra	Unknown	
RaHDit	Unknown	
404 Cyber Defence	Unknown	
WereTheGoons	Unknown	
punisher_346	Unknown	
DDoS Hacktivist Team	Unknown	
cyberwar_world	Unknown	

Zsecnet NEW	Unknown	

Texts written in [ ] are editorial notes.

Appendix 2. APT Actors Affiliated to Belarus

Name	Organization	Aliases
Ghostwriter	Ministry of Defence	TA445, UNC-1151, UNC1151

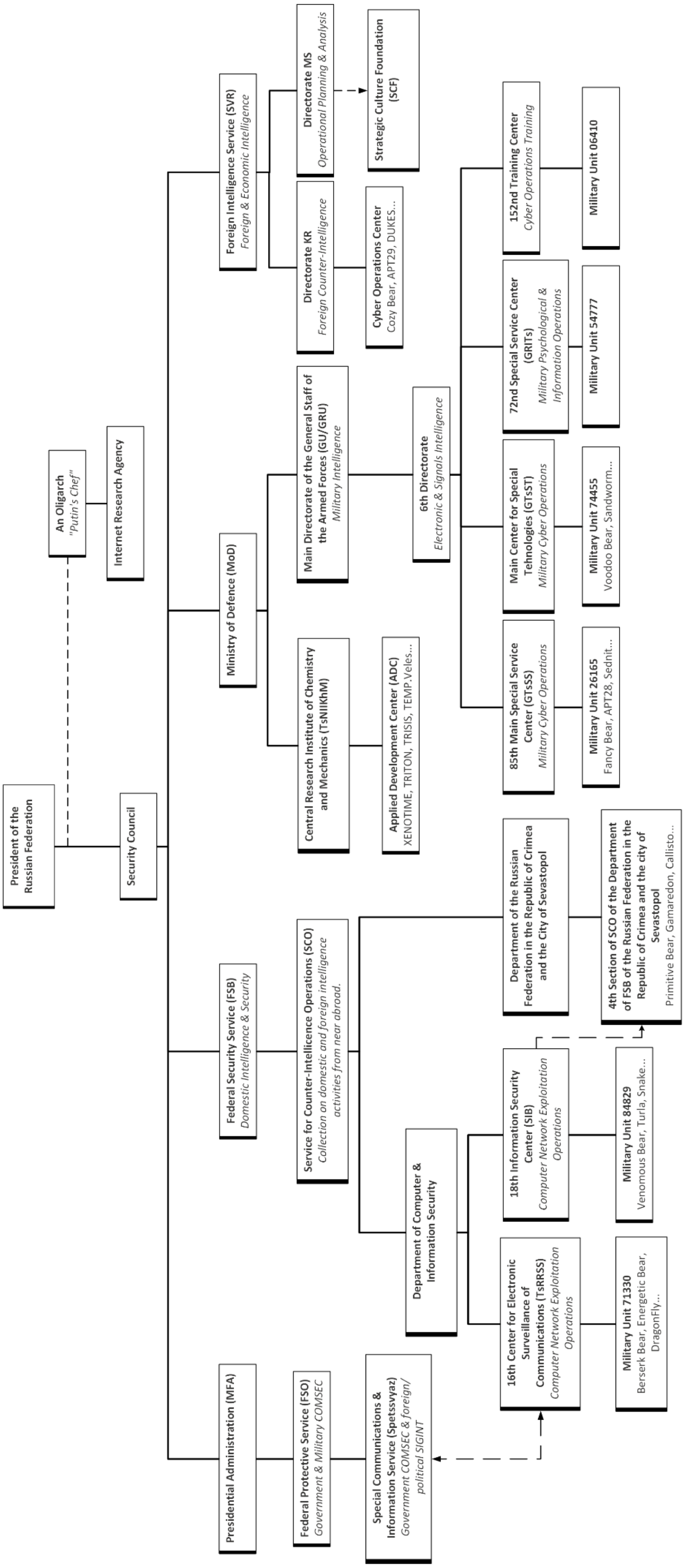
Appendix 3. APT Actors and Hacktivists Affiliated to be Pro-Ukraine

Name	Aliases
IT Army of Ukraine	[*Volunteer hackers for Ukraine Ministry of Defence*]
Anonymous	Anon
Network Battalion 65	NB65, National Battalion 65, Battalion-65, Battalion65
AgainstTheWest	
Anonymous Liberland & PWN-Bär Hack Team	
Bandera Hackers	
barbby	
BeeHive Security	
Belarusian Cyber Partisans	Cpartisans, Cyber-Partisans
BlackHawk	
BlueHornetAPT 49	
BrazenEagle	
Burkeluke	
ContiLeaks	
Cyber Defence	
Cyber_legion_hackers	
ECO	
Eye of the Storm	
GhostClan	
GhostSec	
GNG	
GNG	
HackenClub	
Hackers-Arise	
Hydra UG	
KelvinSecurity Hacking Team	

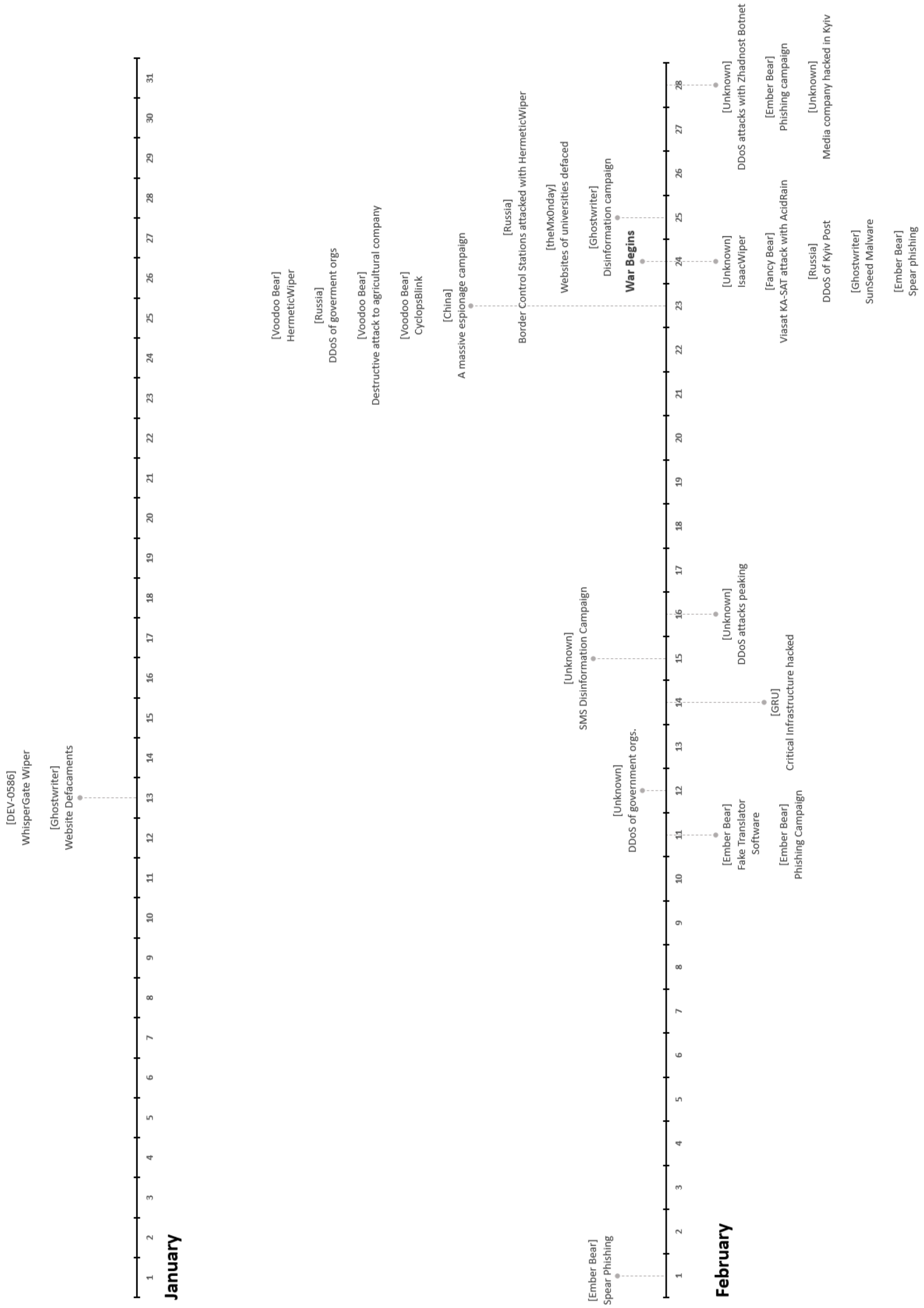
LevelCrew	
Monarch Turkish Hacktivists	
NetSec	
Rabbit Two	
Raidforum Admins	
Raidforums2	
Ring3API	
SecDet	
SecJuice	
Spot	
Squad303	Squad3o3
StandForUkraine	
The Connections	

Texts written in [ ] are editorial notes.

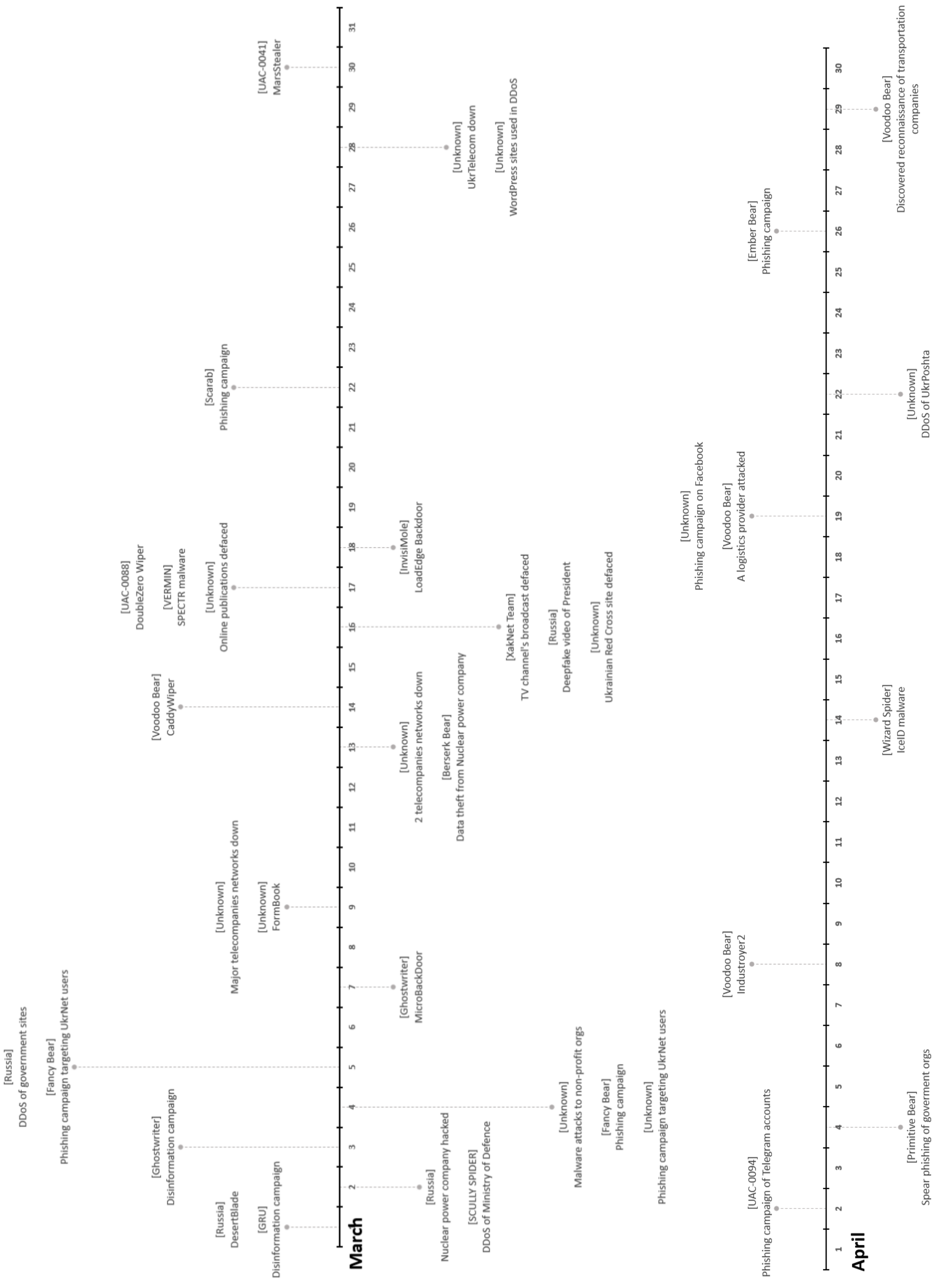
Appendix 4. Russian Cyber Units Organization Chart


President of the Russian Federation
An Oligarch "Putin's Chef"
Internet Research Agency
Security Council
Foreign Intelligence Service (SVR) Foreign & Economic Intelligence
Directorate MS Operational Planning & Analysis
Strategic Culture Foundation (SCF)
Directorate KR Foreign Counter-Intelligence
Cyber Operations Center Cozy Bear, APT29, DUKES...
Ministry of Defence (MoD)
Main Directorate of the General Staff of the Armed Forces (GU/GRU) Military Intelligence
6th Directorate Electronic & Signals Intelligence
152nd Training Center Cyber Operations Training
Military Unit 06410
72nd Special Service Center (GRITs) Military Psychological & Information Operations
Military Unit 54777
Main Center for Special Tehnologies (GTsST) Military Cyber Operations
Military Unit 74455 Voodoo Bear, Sandworm...
85th Main Special Service Center (GTsSS) Military Cyber Operations
Military Unit 26165 Fancy Bear, APT28, Sednit...
Central Research Institute of Chemistry and Mechanics (TsNIIKhM)
Applied Development Center (ADC) XENOTIME, TRITON, TRISIS, TEMP.Veles...
Federal Security Service (FSB) Domestic Intelligence & Security
Service for Counter-Intellicence Operations (SCO) Collection on domestic and foreign intelligence activities from near abroad.
Department of the Russian Federation in the Republic of Crimea and the City of Sevastopol
4th Section of SCO of the Department of FSB of the Russian Federation in the Republic of Crimea and the city of Sevastopol Primitive Bear, Gamaredon, Callisto...
Department of Computer & Information Security
18th Information Security Center (SIB) Computer Network Exploitation Operations
Military Unit 84829 Venomous Bear, Turla, Snake...
16th Center for Electronic Surveillance of Communications (TsRRSS) Computer Network Exploitation Operations
Military Unit 71330 Berserk Bear, Energetic Bear, DragonFly...
Presidential Administration (MFA)
Federal Protective Service (FSO) Government & Military COMSEC
Special Communications & Information Service (Spetssvyaz) Government COMSEC & foreign/ political SIGINT

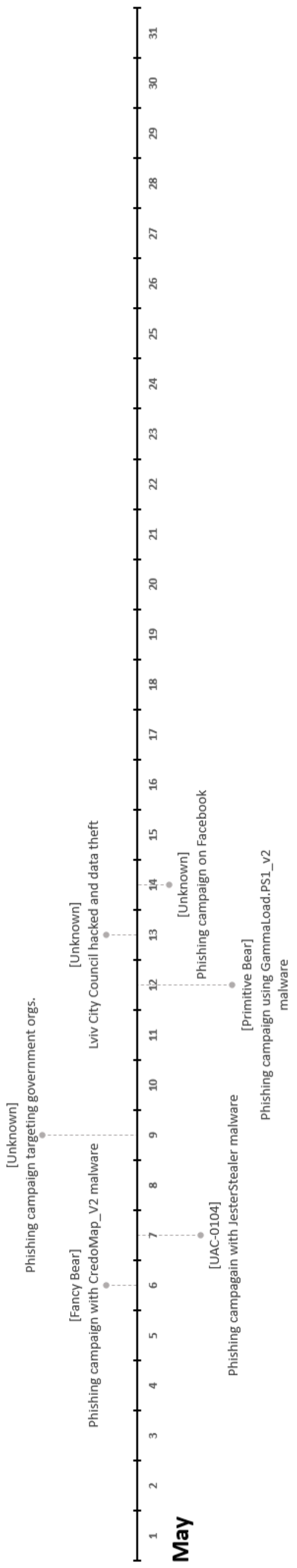
Appendix 5. Timeline: January - February 2022

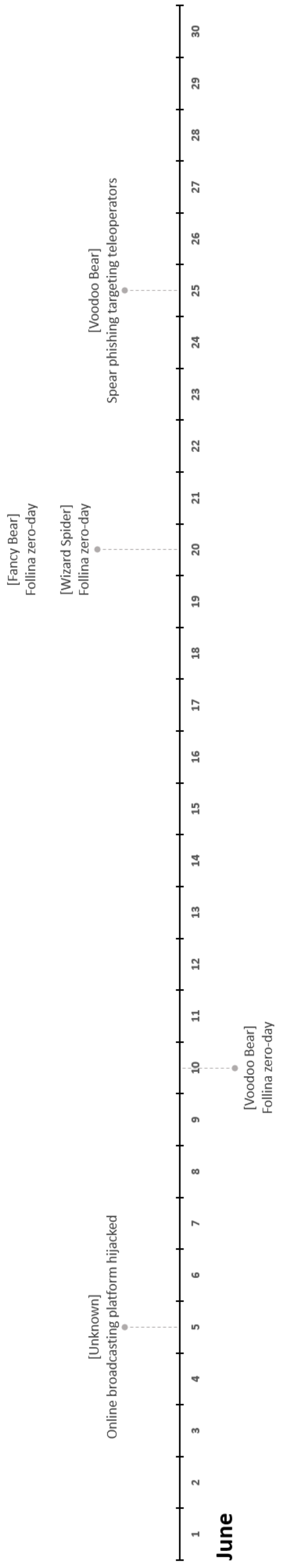


Appendix 6. Timeline: March - April 2022

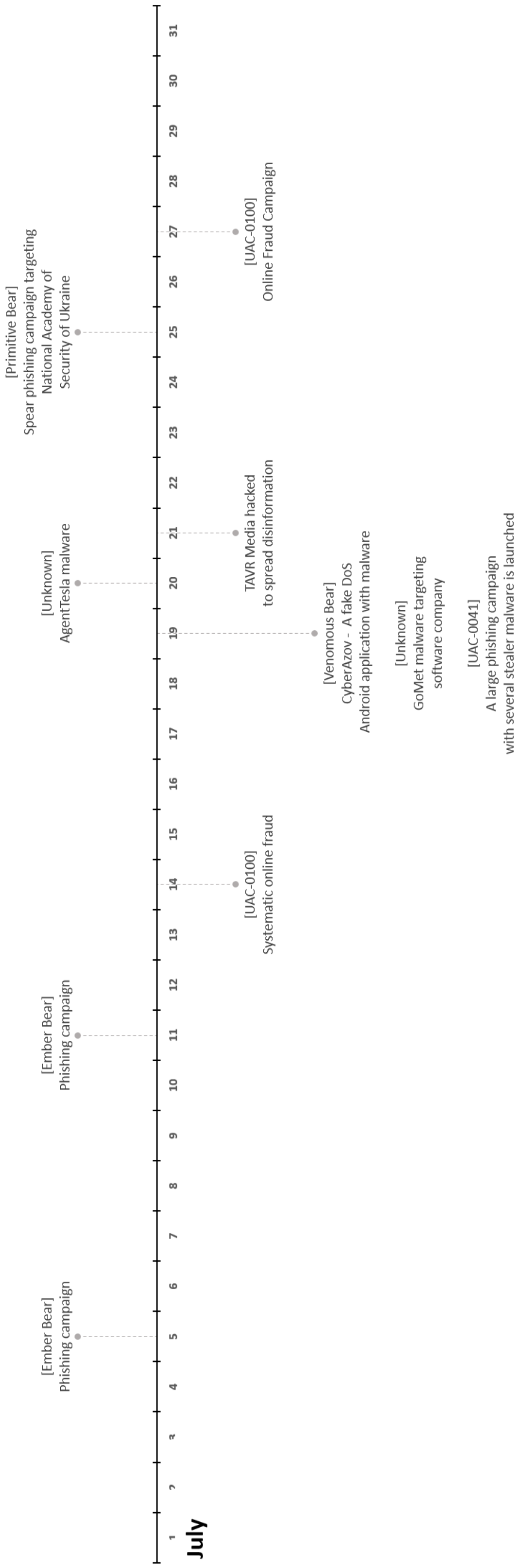

March
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
[Russia] DesertBlade
[GRU] Disinformation campaign
[Russia] Nuclear power company hacked
[SCULLY SPIDER] DDoS of Ministry of Defence
[Ghostwriter] Disinformation campaign
[Unknown] Malware attacks to non-profit orgs
[Fancy Bear] Phishing campaign
[Unknown] Phishing campaign targeting UkrNet users
[Russia] DDoS of government sites
[Fancy Bear] Phishing campaign targeting UkrNet users
[Ghostwriter] MicroBackDoor
[Unknown] Major telecompanies networks down
[Unknown] FormBook
[Unknown] 2 telecompanies networks down
[Berserk Bear] Data theft from Nuclear power company
[Voodoo Bear] CaddyWiper
[XakNet Team] TV channel's broadcast defaced
[Russia] Deepfake video of President
[Unknown] Ukrainian Red Cross site defaced
[UAC-0088] DoubleZero Wiper
[VERMIN] SPECTR malware
[Unknown] Online publications defaced
[InvisiMole] LoadEdge Backdoor
[Scarab] Phishing campaign
[Unknown] UkrTelecom down
[Unknown] WordPress sites used in DDoS
[UAC-0041] MarsStealer
April
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
[UAC-0094] Phishing campaign of Telegram accounts
[Primitive Bear] Spear phishing of goverment orgs
[Voodoo Bear] Industroyer2
[Wizard Spider] IcelD malware
[Unknown] Phishing campaign on Facebook
[Voodoo Bear] A logistics provider attacked
[Unknown] DDoS of UkrPoshta
[Ember Bear] Phishing campaign
[Voodoo Bear] Discovered reconnaissance of transportation companies

Appendix 7. Timeline: May - June 2022


May
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
[Fancy Bear]
Phishing campaign with CredoMap_V2 malware
[UAC-0104]
Phishing campagain with JesterStealer malware
[Unknown]
Phishing campaign targeting government orgs.
[Primitive Bear]
Phishing campaign using GammaLoad.PS1_v2 malware
[Unknown]
Lviv City Council hacked and data theft
[Unknown]
Phishing campaign on Facebook



Appendix 8. Timeline: July 2022



Appendix 9. Observed Major Attacks on Ukraine (From January to July)

JANUARY 13, 2022

WhisperGate and WhisperKill Wiper Malware

Targets: Public Sector, NonProfit, ICT

Attribution: Ember Bear (GRU)

Destructive wiper malware known as WhisperGate was used to attack against several organizations. WhisperGate was made to look like ransomware, but according to Microsoft Security's (2022) examination of malware revealed it was lacking any recovery mechanisms, making it a wiper malware. WhisperGate malware overwrites master boot record of the system and creates a fake ransom note. Additionally, it downloads from a Discord server another malware known as WhisperKill to corrupt local files. Digital Security Unit (2022) of Microsoft suggests Ember Bear being linked possibly to GRU.

Defacing Government Websites

Targets: Public Sector

Attribution: Ghostwriter (Belarusian MoD)

Between January 13th and 14th more than 70 websites of the Ukrainian government were defaced with political propaganda. The attack affected government's public-facing services, but the effects of the attack were reversed in a couple of hours. Defacement messages included threats like "Fear..." and "Wait for the worst" (Ukraine Center for Strategic Communications, 2022).

FEBRUARY 1, 2022

Spear Phishing Campaign

Targets: Energy Sector

Attribution: Ember Bear (GRU)

According Palo Alto Networks' Unit 42 (2022), a Ukrainian energy company was targeted with email spear phishing attack with social engineering aspect claiming the receiver from committing a criminal activity. The emailed attachment Microsoft Word file pretending to be the National Police of Ukraine's investigation report included JavaScript used to download and install two payloads known as SaintBot and OutSteel. OutSteel is a primitive document stealer malware which searches for various types of documents and database files to be uploaded to a remote server. SaintBot is malware loader with ability to execute downloaded payloads with different ways (e.g., load to local memory or inject to a process) and remove itself (Unit 42, 2022).

FEBRUARY 11, 2022

Fake Dictionary-Translator Software

Targets: Multiple

Attribution: Ember Bear (GRU)

SentinelOne's Ehrlich (2022) examined phishing campaign disguised as messages from Ukrainian government agencies. Receivers were tricked to use fake Ukrainian dictionary-translator that downloaded two different malware, GrimPlant and GraphSteel. GraphSteel is malware used for stealing and harvesting user credentials. According to Ehrlich's analysis, building the attack infrastructure was started in early December 2021.

Phishing Campaign

Targets: Public Sector

Attribution: Ember Bear (GRU)

Another attack was launched with email. At least two different messages are reported. One containing Microsoft Excel file with a VisualBasic script. The script was used to download Cobalt Strike Beacon from Discord server along with GrimPlant and GraphSteel malware. Another reported lure-message was an advice to improve information security by installing suggested critical updates (CERT-UA, 2022ab).

FEBRUARY 12, 2022:

DDoS attacks

Targets: Public Sector

Attribution: Unknown

On February 12th, a small-scale DDoS attack was launched against the websites of Ukrainian government, at least five different ministries were targeted (360 Netlab, 2022).

FEBRUARY 14, 2022

Critical Infrastructure Compromised

Targets: Unknown

Attribution: GRU

On 14th of February critical infrastructure in Odessa was compromised by a cyber-attack (Microsoft, 2022). This has not been able to be verified from other sources, but because of Microsoft's reputation as a cyber security vendor the claim has been included here.

FEBRUARY 15, 2022

SMS Disinformation Campaign

Targets: Civilians

Attribution: Unknown

Text message disinformation campaign started claiming ATM machines of Ukrainian state-owned bank being out-of-order because of technical malfunctions. The Cyber police of Ukraine did not find reasons to believe that this was a phishing campaign (Cyber police of Ukraine, 2022b).

FEBRUARY 16, 2022

DDoS Attacks Peaking

Targets: Public Sector, Financial

Attribution: GRU

DDoS attacks started on 12th of February kept intensifying and peaked on 16th of February. The attacks used different kind of OVH, STD and UDP floods and NTP amplification (360 Netlab, 2022). These attacks were confirmed by Ukraine's State Service of Special Communications and Information Protection of Ukraine and targeted websites were Ukraine's Ministry of Defence, armed forces and two Ukrainian banks (PBS, 2022). The United States' government has publicly attributed these DDoS attacks to Russian GRU (Psaki et al., 2022).

FEBRUARY 23, 2022

Websites of Government and Institutions Attacked with Exploits

Targets: Military, Financial, Healthcare, Energy, Education, Transportation

Attribution: China

The attack using at least 20 different vulnerabilities targeted more than 600 websites, including Ministry of Defence, border protection and control, the National Bank and railway authority. The attacks were possibly a part of cyber espionage campaign designed to steal information and seek attack-methods against critical infrastructure (Tucker, 2022a).

DDoS Attacks

Targets: Public Sector, Financial

Attribution: Russia

A large scale DDoS attack shutdown access to the websites of Ukrainian government and several banks. At least websites of Cabinet of Ministers, Ministry of Internal Affairs, Security Service of Ukraine and Ministry of Defence were run inaccessible among other services of Ukrainian government (Volz, 2022).

HermeticWiper Malware

Targets: Public Sector, Financial, Energy, ICT

Attribution: Voodoo Bear (GRU)

Hundreds of computers in at least five different organizations were infected by a new destructive wiper malware, known as HermeticWiper or FoxBlade, only a few hours after the DDoS attacks were launched against the websites of the Ukrainian government. According to ESET's (2022a; 2022b) examination of malware, the malicious wiper misuses drivers of EaseUS Partition Master software. Another interesting feature pointed out by ESET (2022a) is the use of genuine code-signing certificate from Hermetica Digital Ltd. located in Cyprus. The malware is made from three different components (HermeticWiper used to corrupt data, HermeticWizard worm used to spread wiper with lateral movement via WMI and SMB and HermeticRansom used as ransomware). The evidence reviewed by ESET (2022b) suggests the attacker already had a foothold on the infected systems Active Directory. Malware's attribution to the GRU's APT actor Voodoo Bear was claimed by Microsoft (Digital Security Unit, 2022).

Destructive Malware Attack to the Ukrainian Agriculture Company

Targets: Agriculture

Attribution: Voodoo Bear (GRU)

A file encryptor malware attributed to Voodoo Bear was found from the network of a Ukrainian agricultural firm, suggested by Microsoft to be a major exporter of Ukrainian grain (Digital Security Unit, 2022).

CyclopsBlink Malware

Targets: Civilians

Attribution: Voodoo Bear (GRU)

Some models of consumer routers of ASUS were hit by Voodoo Bear attributed CyclopsBlink malware. The infected routers are used as part of a botnet to attack different organizations (Chirgwin, 2022). This kind compromised devices can also be used as proxies to hide the attacker's identity or even as attack vectors if located inside targeted organizations.

FEBRUARY 24, 2022 – The War Begins

IsaacWiper Malware

Targets: Public Sector

Attribution: Unknown

New destructive wiper malware, known as IsaacWiper or Lasainraw was found in Ukraine. The malware is less sophisticated than previous wiper malware, HermeticWiper (Microsoft, 2022). The malware deployed as a Windows executable wipes infected systems disks and partitions by overwriting them using Mersenne Twister pseudo-random number generator. Interestingly, ESET (2022b), found on following day an IsaacWiper variant with debug logs enabled, suggesting that attack did not work in all intended targets and the attacker was trying to solve the issue. Some of the detected variants also tried to reboot the infected machines after the attack. According to Dwyer and Henson (2022) of IBM's Security Intelligence, if malware was not able to overwrite data on the disk, it created a temporary file with generated random data to fill disk out of space.

DDoS Attack Against the Kyiv Post

Targets: Media

Attribution: Russia

One of the leading media's The Kyiv Post was targeted with a DDoS attack to prevent information coverage of the start of the Russian invasion (Darcy, 2022).

SunSeed Malware

Targets: Public Sector, Military

Attribution: Ghostwriter (Belarus)

A mass phishing email campaign targeting Ukrainian military personnel and European governmental entities was detected luring victims with subject "IN ACCORDANCE WITH THE DECISION OF THE EMERGENCY MEETING OF THE SECURITY COUNCIL OF UKRAINE DATED 24.02.2022" (Raggi & Cass, 2022) and including a Microsoft Excel file “list of persons.xlsx”. The attached file contained a simple malicious VisualBasic macro used to create a Windows installer. The created installer sets UILevel as “2” which allows the program to do a silent install feature indented to be used with MSI install packages. This MSI package is used to install Lua-based SunSeed malware from the attacker’s determined IP address (Raggi & Cass, 2022). The phishing campaign is attributed to Ghostwriter as its TTPs resembles the Asylum Ambuscade campaign, even matching to WiX 3.11.0.1528 version used to create the MSI installer (Raggi & Cass, 2022).

AcidRain Malware Attacks Viasat’s KA-SAT

Targets: Communications

Attribution: Fancy Bear (GRU)

A cyber-attack impacting to tens of thousands of customers across the Europe and thousands of customers in Ukraine was launched one hour before the military invasion. The attack supposedly was targeting the internet communications used by the Ukrainian military with destroying over thirty thousand of satellite terminals. Among the affected customers were multiple European companies including 5,800 wind turbines in Germany (Martin, 2022; Viasat, 2022).

The attack started with massive volume of malicious traffic created by some satellite modem models physically located in the Ukraine. The malicious traffic caused DDoS affecting to other satellite modems’ ability to stay on the network. About one hour later satellite modems all over the Europe started to exit from the network without re-entering (Viasat, 2022).

According to Viasat’s (2022) investigation, the intruder was able to gain access to the management segment of the KA-SAT’s network by exploiting misconfigured VPN appliance. From the trusted management segment, the intruder was able to move laterally to another management segment where the attacker could legitimately operate private customers’ satellite modems. This access was used to overwrite data on the modems’ flash memory with destructive commands (Viasat, 2022).

Sentinel Lab’s Guerrero-Saade and van Amerongen (2022) suggests that modem targeting Acid-Rain wiper malware used in the attack share similarities with VPNFilter campaign attributed to Fancy Bear. According to Sentinel Lab’s examination the malware itself is pretty simple and basically brute-forces different options and file identifiers to be overwritten or erased.

Spear Phishing Attacks with XFILES Malware

Targets: Media

Attribution: UNC3691, linked to Ember Bear (GRU)

Spear phishing attack targeting Ukrainian journalists was discovered by Mandiant Threat Intelligence (2022). The phishing campaign used a Microsoft Word document with malicious macro. The macro downloads XFILES stealer malware from a Discord channel used previously by Ember Bear and UNC3691 with GOOSECHASE malware.

FEBRUARY 25, 2022

Border Control Station Attacked with HermeticWiper

Targets: Public Sector

Attribution: Russia

While the Ukrainian refugees were trying to flee the country, the border control station locating between Ukraine and Romania was hit with a wiper malware, most likely HermeticWiper. According to a cyber security expert interviewed by The Washington Post, the damage caused by the malware was massive. As the cyber-attack took down computer systems of the State Border Guard Service of Ukraine, slow but working solution was to start to keep notes of crossing refugees with a pen and paper (Berger, 2022; Alspach, 2022).

Universities’ Websites Defaced

Targets: Education

Attribution: theMx0nday (Brazil)

A pro-Russian APT actor, theMx0nday, from Brazil attacked and successfully compromised with defacements at least 30 websites of Ukrainian universities. The attack peaked on 26th of February and stopped just after three days, according the company Wordfence who is the cyber security provider of those websites. WordFence recognized 209624 sophisticated exploit attempts against 376 university websites during those three days (Maunder, 2022).

Disinformation Campaign Launched on Social Media Platforms

Targets: Media, Civilians, Military

Attribution: Ghostwriter (Belarus)

A small disinformation campaign against Ukrainian citizens, military personnel and public figures was launched on Facebook, Instagram, Twitter and a few other social media platforms. According to Meta's Gleicher and Agranovich (2022) the company removed approximately 40 accounts from Facebook and Instagram that were part of the network spreading disinformation on multiple platforms. The disinformation campaign tried to spread images and videos portraying Ukrainian soldiers to be appearing weak and surrendering to Russian troops.

FEBRUARY 28, 2022

DDoS Attacks Continues with Zhadnost Botnet

Targets: Public Sector, Financial

Attribution: Unknown

SecurityScorecard's Slaney (2022) revealed Zhadnost botnet, mainly created from infected MikroTik's router devices, were discovered with more than 3,000 IP addresses launching DDoS attack against websites of Ukrainian government (e.g., Ministry of Foreign Affairs, Ministry of Defence, Security Service of Ukraine etc.) and financial websites (at least Oschadbank and Privatbank). The attack used mainly HTTP floods and DNS amplification methods. According to Slaney's research, the same botnet was behind the DDoS attacks witnessed on the 23th of February.

Phishing Campaign

Targets: Industrial Production

Attribution: Ember Bear (GRU)

A new phishing campaign was launched sending emails portraying coming from the SSU and luring victims with topic of SSU approved evacuation plans. The email allegedly contained malicious RAR file which used RemoteUtils to download stealer malware (Censor.net, 2022).

A Media Company Attacked

Targets: Media

Attribution: Unknown

An unnamed media company located in Kyiv was compromised in cyber-attack according to Micosoft (2022). This has not been able to be verified from other sources though because of Microsoft's reputation as a cyber security vendor the claim has been included here.

MARCH 1, 2022

DesertBlade Malware

Targets: Media

Attribution: Russia

Microsoft's Digital Security Unit (2022) detected an attack launched with a new wiper malware known as DesertBlade against an unnamed media company on Ukraine. Later on, Russian missiles targeted a TV tower located in Kyiv. According to Microsoft's Digital Security Unit this was part of Russia's agenda to control information environment by using destructive cyber operations and kinetic strikes.

Disinformation Campaign on Telegram

Targets: Media

Attribution: GRU

The SSU issued a warning of disinformation messages spread on Telegram channels linked to GRU (Gatlan, 2022).

MARCH 2, 2022

APT Advances in Network of Ukrainian Nuclear Power Company

Targets: Energy

Attribution: Russia

Russian based APT group was able to advance laterally on Ukrainian nuclear power company's network (Micosoft, 2022). Ukraine claimed two days later the attacks against nuclear power systems were under control (Nakashima, 2022).

DDoS Attack Against Ministry of Defence

Targets: Military

Attribution: SCULLY SPIDER

A DDoS attack against Ukraine’s Ministry of Defence’s webmail server was launched with SCULLY SPIDER criminal group operated DanaBot botnet. The attack was classified as HTTP-based type of DDoS attacks. The DDoS was actually used as a delivery mechanism for malware payload (Schwarz, 2022).

MARCH 3, 2022

Disinformation Campaign

Targets: Public Sector

Attribution: Ghostwriter (Belarus)

Ukraine's SSSCIP warned about new disinformation campaign targeting Ukrainian citizens. Multiple websites belonging to the local governments and regional authorities had been compromised and defaced with disinformation. The spread message claimed that Ukraine had surrendered and signed a peace treaty with Moscow. The attack is attributed to Ghostwriter APT group (Satter, 2022a).

MARCH 4, 2022

Malware Attacks Targeting Charities

Targets: Non-profit

Attribution: Russia

Amazon has released statement regarding witnessing Russian nation-state linked actors targeting several different non-government organizations, including charities helping Ukrainian refugees. These cyber-attacks have used different malware specifically targeting aid organizations. This includes disrupting food, medical supplies and other similar essential supplies (Amazon, 2022).

Phishing Campaign Targeting Government

Targets: Public Sector

Attribution: Fancy Bear (GRU)

An undisclosed Ukrainian government's network in Vinnytsia was attacked by Fancy Bear (Microsoft, 2022).

Phishing Campaign Against UkrNet's Users

Targets: Civilians

Attribution: Unknown

CERT-UA issued a warning regarding an ongoing phishing campaign using compromised Indian email addresses for sending messages made to look like sent by the ukr.net. At least 20 different compromised email addresses were detected sending messages with topic "Увага" [Attention] (Lakshmanan, 2022). The message itself was a classical phishing attempt with warning users from unauthorized access attempts to their account and requesting to change their password immediately (Lakshmanan, 2022).

MARCH 5, 2022

DDoS Attacks Against Government websites

Targets: Public Sector

Attribution: Russia

SSSCIP issued information regarding ongoing DDoS attacks against websites of Ukrainian government, including Ministry of Defence, Internal Affairs Ministry, Cabinet of Ministers, etc. The attack was not attributed to any specific actor (Satter, 2022b).

Phishing Campaign Against UkrNet's Users

Targets: Media

Attribution: Fancy Bear (GRU)

According to Google's Threat Analysis Group (Huntley, 2022) Fancy Bear has launched a phishing campaign targeting UkrNet's users. The email contained link to the websites used in previous Fancy Bear's phishing campaigns and newly created Blogspot domains.

MARCH 7, 2022

MicroBackDoor Malware

Targets: Military, Public Sector

Attribution: GhostWriter (Belarus)

CERT-UA (2022aa) released warning of MicroBackDoor malware spread by Ghostwriter. According to CERT-UA the email contained "help.zip" file containing "dovidka.chm" a Microsoft HTML help document. The help document contained a malicious file with VBScript used to decode .NET loader which was used to decode and execute the actual MicroBackDoor malware. According to Cluster25's (2022) examination of the malware, the DLL file used in .NET code was compiled on 31st of January, 2022.

MARCH 9, 2022

Cyber-Attacks Against Two Major Telecommunications Providers

Targets: Communications

Attribution: Unknown

A major Ukrainian telecommunications provider, Triolan was hacked. According to Triolan, the attack vector is still unknown while its network's several key nodes were compromised and run inoperable. Besides this, some of the company's internal computers were reset to default settings. Triolan's network was down over 12 hours. The company was told to be hacked also on 24th of February when the Russian invasion began (Brewster, 2022).

Ukrtelecom's network was down for approximately 40 minutes nationwide. Ukrtelecom is the largest internet service provider in Ukraine (Moss, 2022a).

FormBook Malware Spam Campaign

Targets: Civilians

Attribution: Unknown

Malwarebytes Labs' Threat Intelligence Team (2022) reported witnessing FormBook stealer malware targeting Ukrainian citizens. The lure in the attack was attached to a message promising funds from the Ukrainian government. Attached malicious Microsoft Excel file was used to download FormBook malware from attacker's remote server.

MARCH 13, 2022

Attacks to the Telecommunications

Targets: Communications

Attribution: Unknown

In two different regions of Ukraine cyber-attacks against internet service providers were launched. Network disruptions were affecting the city of Summy and the Vinnytsia Oblast. No further information regarding the attacks have been shared (Moss, 2022b).

Data Theft from A Nuclear Safety Organization

Targets: Energy

Attribution: Berserk Bear (FSB)

According to Microsoft (Digital Security Unit, 2022) Berserk Bear was able to again compromise a nuclear safety organization and stole data. As claimed by Digital Security Unit the organization was initially compromised in December 2021.

MARCH 14, 2022

CaddyWipper Malware

Targets: Unknown

Attribution: Voodoo Bear (GRU)

ESET’s (2022c) researchers found CaddyWiper malware from a limited number of undisclosed Ukrainian organizations. Even though CaddyWiper does not have much code similarities with earlier wipers, it suggests similar TTPs of attacker. For Caddywiper, just like HermeticWiper, it is reasonable to assume that attacker had already gained a foothold on the attacked networks. The malware’s destructive nature renders compromised systems unbootable after overwriting the files and the disks.

MARCH 16, 2022

Hacked TV-Station Spreads Disinformation

Targets: Media

Attribution: The XakNet Team

According to the Atlantic Council’s Digital Forensics Lab (2022) a national news channel Ukraine 24 was hacked allegedly by the hacktivist group known as The XakNet Team. The news broadcast's banner was defaced to show disinformation messages looking like they would be coming from the President of Ukraine. The messages were similar to earlier disinformation campaigns telling Ukrainians to stop fighting and to lay down their weapons.

Deepfake video of Ukrainian President

Targets: Civilians

Attribution: Unknown

Later on, a Pro-Russian Telegram channel started to distribute a deepfake video of the President of Ukraine repeating similar false messages (Digital Forensics Lab, 2022).

The Website of Ukrainian Red Cross Defaced

Targets: Non-Profit

Attribution: Unknown

The Ukrainian Red Cross tweeted to inform cyber-attack targeted their website resulting with defacing of the site. It was restored a few hours later (Ukrainian Red Cross, 2022).

MARCH 17, 2022

SPECTR Malware

Targets: Military, Public Sector

Attribution: VERMIN

CERT-UA (2022ac) states Ukrainian government and Ministry of Defence being targeted by emails containing SPECTR malware. The emails included "ДВТПРОВТ.rar" [DVTPPROVT.rar] (CERT-UA, 2022ac) named RAR archive containing two files as an attachment. The attack was using same infrastructure as witnessed before on the cyber-attacks carried out by VERMIN.

Popular Online Publications Defaced

Targets: Media

Attribution: Unknown

The SSU released statement regarding a cyber-attack targeting several popular online publications. At least Slovo i Dilo's website was compromised and defaced with symbols banned in Ukraine (Slovo i Dilo, 2022).

DoubleZero Wiper Malware

Targets: Unknown

Attribution: UAC-0088

Discovery of a new destructive wiper malware was announced by CERT-UA (2022ae). The malware is known as DoubleZero or FiberLake. DoubleZero is a bit different kind of wiper when compared to earlier discoveries done from Ukraine. It uses a .NET capability for destroying files in compromised systems (Microsoft, 2022). Another distinguishing feature was discovered by Cisco Talos. DoubleZero has a hardcoded list of system folders that it preserves to be deleted after all the other files on the system have been destroyed and overwritten. This way it can maximise the destruction without danger of crashing the system (Malhotra, 2022).

MARCH 18, 2022

Phishing Campaigns Launched Using LoadEdge Backdoor

Targets: Public Sector

Attribution: InvisiMole

Warning of government targeting phishing email campaign was issued by CERT-UA (2022ad). The campaign was attributed to InvisiMole group, linked to FSB's Primitive Bear. The emails contained a ZIP archive "501_25_103.zip" which included LNK shortcut file with the same name pointing to an HTA file. When opened, the file used VBScript for downloading and decoding LoadEdge Backdoor.

MARCH 22, 2022

Scarab Targets Ukraine with Russian War Crimes Lure

Targets: Unknown

Attribution: Scarab (China)

CERT-UA (2022af) released information regarding phishing emails containing malicious RAR archive. The email's attachment "Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.rar" [On the preservation of video recordings with the recording of criminal actions of the army of the Russian Federation.rar] (CERT-UA, 2022af) includes an EXE file with the same filename. Executing the file generates a decoy document and drops malicious DLL file now known as HeaderTip.

MARCH 28, 2022

UkrTelecom Targeted with a Major Cyber-Attack

Targets: Communications

Attribution: Unknown

IT-infrastructure of Ukrtelecom was targeted with a major cyber-attack causing nationwide disruption to the communications services. The affected services were down for over 15 hours until Ukrtelecom was able to restore them (Bing & Satter, 2022).

WordPress Websites Used in DDoS Attacks

Targets: Financial, Public Sector, Non-Profit

Attribution: Unknown

Hackers targeted multiple WordPress websites infecting them with malicious JavaScript code. When the code is executed in a visiting web browser, the browser performs multiple HTTP GET requests to the sites targeted in a DDoS attack. This makes the visitors of compromised sites non-volunteering participants of a cyber-attack (Abrams, 2022).

MARCH 30, 2022

MarsStealer Malware

Targets: Civilians

Attribution: UAC-0041

Information from a new APT group's phishing attack was reported by CERT-UA (2022ag). Threat actor currently known as UAC-0041 was detected mass sending emails with topic "Нова програма для запису в журналі." [New program for journal entry.] (CERT-UA, 2022ag). It was pretending to be a message from Ministry of Education and Science of Ukraine. The email included a malicious password protected archive as an attachment and password to open it. The EXE file inside the archive infected system with MarsStealer malware.

APRIL 2, 2022

Phishing Campaign Targeting Telegram Accounts

Targets: Civilians

Attribution: UAC-0094

Ukrainian CERT-UA (2022ai) issued a warning regarding ongoing phishing campaign targeting Telegram accounts. The phishing was done by sending a malicious link where the victim was asked to provide their phone number and one-time-password sent via SMS. The attacker then used these to obtain access to the victims Telegram account.

APRIL 4, 2022

Spear Phishing Campaign Targeting Government Agencies
Targets: Public Sector
Attribution: Primitive Bear (FSB)
According to CERT-UA (2022ah) FSB's Primitive Bear was targeting Ukrainian government agencies using theme of Russian war criminals as a lure. The email contained an attached HTML file "Військові злочинці РФ.htm" [War criminals of the Russian Federation.htm] (CERT-UA, 2022ah). When the HTML file was opened, it created RAR archive to the system with filename "Viyskovi_zlochinci_RU.rar" (CERT-UA, 2022ah). The archive had only one LNK shortcut file inside "Військові-злочинці що знищують Україну (домашні адреси, фото, номера телефонів, сторінки у соціальних сетях).lnk" [War criminals destroying Ukraine (home addresses, photos, phone numbers, pages in social networks).lnk] (CERT-UA, 2022ah) which was used to download HTA file from attacker's remote server. The downloaded HTA file used VBScript to download and execute malicious PowerShell script on victims' machine. The script sent unique identifier of the compromised system to the attacker's management server which was then used to control exploiting of the payload.

Influence Operation Targeting Mariupol
Targets: Civilians
Attribution: Ember Bear (GRU)
Microsoft's Digital Security Unit (2022) suggested Russian influence operation targeting Mariupol. The messages were sent by using the name of Ukrainian government official and asking to stop fighting and start to resist Ukrainian government.

APRIL 8, 2022

Industroyer2 Malware Used to Attack Critical Infrastructure

Targets: Energy

Attribution: Voodoo Bear (GRU)

According to CERT-UA (2022aj) Voodoo Bear launched a cyber-attack against Ukrainian high-voltage electrical substations with a new variant of Industroyer malware, named as Industroyer2 along side with several other destructive malware. The Industroyer2's destructive data-wiping features were notably improved from the last variant. The CERT-UA claims that each malicious executable was uniquely created to target a specific substation. The incident was investigated in co-operation with Ukrainian authorities and private vendors ESET and Microsoft. ESET (2022d) clarifies used malware by suggesting that Industroyer2 and a new version of CaddyWiper was used against network partition of ICS based on Windows operation system used to control the targeted substations. The other destructive malware used against the network containing machines with Linux and Solaris operation systems were AWFULSHRED, SOLOSHRED and ORCSHRED.

CERT-UA (2022aj) suggests that targeted the energy company was prefatory compromised on February to create a foothold for launching the actual destructive cyber-attack against critical infrastructure. As claimed by the CERT-UA the attack was successfully thwarted with the help of the private vendors mentioned earlier.

APRIL 14, 2022

Phishing Campaign with IceID Trojan

Targets: Civilians, Public Sector

Attribution: Wizard Spider

Another phishing email campaign was launched as suggested by CERT-UA (2022ak) warning. The email included a Microsoft Excel file “Мобілізаційний реєстр.xls” [Mobilization Register.xls] (CERT-UA, 2022ak) with malicious macro. When opened, the macro was used to download and execute GzipLoader malware which was used to download and execute IceID trojan used in the attack. Even when the IceID is classified as banking trojan it includes multiple features for data theft and loading further malware.

APRIL 19, 2022

Phishing Campaign on Facebook with Financial Aid Lure

Targets: Civilians

Attribution: Unknown

An unknown threat actor, as claimed by CERT-UA (2022al) was using a page on Facebook pretending to be page of Ukrainian TV channel Ukraine 24 for its phishing campaign. The malicious fake page lured victims with providing a link to an external survey. Participants were promised to receive financial aid from EU countries.

Logistics Provider Targeted with Destructive Attack

Targets: Logistics

Attribution: Voodoo Bear (GRU)

A logistics provider on Kyiv was targeted with destructive cyber-attack according to Microsoft (2022). No further details were released.

APRIL 22, 2022

DDoS Attack Against Ukrposhta

Targets: Postal Services

Attribution: Unknown

According to Reuters (Polityuk, 2022) Ukrainian Postal Service Ukrposhta was hit by a DDoS attack that took down Postal Service’s systems and online store. The attack was launched when sales of the famous Ukrainian propaganda postage stamp started. The stamp was referencing to the incident between Ukrainian soldiers and the warship Moskva on Snake Islands.

APRIL 26, 2022

Phishing Campaign Using Compromised Email Account

Targets: Public Sector

Attribution: Ember Bear (GRU)

A compromised email account of the Ukrainian government employee was used in a phishing campaign, according to CERT-UA (2022am). The lure used in this campaign was COVID-19 theme with a Microsoft Excel file “Aid request COVID-19-04_5_22.xls” (CERT-UA, 2022am) as an attachment.

The malicious XLS file contained a macro which is used to create a Cobalt Strike Beacon and dropper malware to the host. Then the dropper downloaded and ran GraphSteel and GrimPlant backdoors on infected system.

APRIL 29, 2022

Identified Cyber Reconnaissance to Transportation Sector's Company

Targets: Transportation

Attribution: Voodoo Bear (GRU)

Cyber reconnaissance of Voodoo Bear was identified to target a Lviv based transportation company (Microsoft, 2022).

MAY 6, 2022

Possible Phishing Campaign Using CredoMap_V2 Malware

Targets: Unknown

Attribution: Fancy Bear (GRU)

Ukrainian CERT-UA (2022an) states it was provided malware sample for further examination. Provided file was a RAR archive "UkrScanner.rar" containing similarly named a SFX file. The file contained a CredoMap_v2 malware's new variant. The New variant sent stolen data back to the attacker with HTTP POST requests.

MAY 7, 2022

Massive Phishing Campaign Using JesterStealer Malware

Targets: Unknown

Attribution: UAC-0104

A massive phishing campaign spreading JesterStealer malware was detected according to CERT-UA (2022ao). The campaign used a war related lure since the topic of emails was "хімічної атаки" [Chemical attack]. The message had a Microsoft Excel file attached with a malicious macro. The macro downloads and executes an EXE file used for downloading and running JesterStealer malware on the host. Jester Stealer was used steal information from internet browsers and other web related clients (e.g., mail clients, FTP-clients, password managers, crypto wallets, etc.). Stolen data was transmitted to the attacker's Telegram channel through proxy and TOR network. CERT-UA also noted that the malware contained anti-forensics features and removed itself after the data theft.

MAY 9, 2022

Spear Phishing Targeting a Government Employee

Targets: Public Sector

Attribution: Unknown

According Trellix (2022) a Ukrainian government employee was targeted in a spear phishing campaign. The attack followed familiar path by having a password protected ZIP archive “Необхідні частини.zip" [Required parts.zip] (Trellix, 2022) as an attachment and the email message’s body included the password. The LNK shortcut file inside the archive executed PowerShell script to create a webclient used to download malicious “helper.exe” executable file. The malicious file was a stealer malware and it transmited stolen information back to the attacker with HTTP POST requests.

Websites of Teleoperators Targeted with DDoS

Targets: Communications

Attribution: Unknown

The SSSCIP (2022a) released information regarding a massive DDoS attack as claimed by SSSCIP. The attack was told to be targeting websites of Ukrainian telecommunications companies. According to the statement, the targeted websites were only partially affected.

MAY 12, 2022

Phishing Campaign Using GammaLoad.PS1_v2 Malware

Targets: Unknown

Attribution: Primitive Bear (FSB)

CERT-UA (2022ap) released information from Primitive Bear’s phishing campaign. Topics of the emails continued to follow current occasions of the war as the used lure was “Щодо проведення акції помсти у Херсоні!” [On revenge in Kherson!] (CERT-UA, 2022ap). The attached RAR archive “Herson.rar” included a LNK shortcut file “План підходу та закладання вибухівки на об'єктах критичної інфростурктури Херсона.lnk” [Plan of approach and laying of explosives on objects of critical infrastructure of Kherson.lnk] (CERT-UA, 2022ap) used to load and execute an HTA file which created two malicious files to the host and ran them. This led to downloading of GammaLoad.PS1_v2 malware.

MAY 13, 2022

Cyber-Attack Targeting Lviv City Council
Targets: Public Sector
Attribution: Unknown
The city of Lviv's online services went down for less than a day as a result of cyber-attack. Also, some of the city council employees' computers were compromised during the attack. The unknown attacker was claimed to have released at least part of the city's stolen data on Telegram (LMR press service, 2022; Shchepanskaya, 2022).

MAY 14, 2022

Phishing Campaign on Facebook
Targets: Civilians
Attribution: Unknown
Similar phishing campaign on Facebook was found when compared to the one discovered on 19th of April. This time the phishing page on Facebook imitated Ukrainian TC channel TSN. The lure continued same financial theme providing a link to a survey and with a promise of "грошову допомогу в рамках соціальної програми ООН" [financial assistance under the UN social program] (CERT-UA, 2022aq).

JUNE 2, 2022

Government Agencies Attacked with Cobalt Strike Beacon and Follina Zero-Day Vulnerability
Targets: Public Sector
Attribution: Unknown
CERT-UA (2022ar) published cyber-attack targeting Ukrainian government agencies with a malicious email. The organizations were targeted with messages with an attached Microsoft Word document "зміни оплата праці з нарахуваннями.docx" [changes in payroll with accruals.docx] (CERT-UA, 2022ar). The document contained a link to a malicious HTML where JavaScript was used

to exploit two different remote code execution vulnerabilities (CVE-2021-40444 and zero-day vulnerability CVE-2022-30190, now known as Follina). These vulnerabilities were used to execute PowerShell script used to download an EXE file containing Cobalt Strike Beacon.

JUNE 5, 2022

Soccer Broadcast Hijacked with Cyber-Attack
Targets: Media
Attribution: Unknown
According to OLL.TV (2022), and later on confirmed by SSSCIP (2022b), the TV broadcasts of qualifier game of the Football World Cup 2022 were interrupted on Ukraine when OLL.TV (the Ukrainian platform for online broadcasting) was compromised in a cyber-attack (State Service of Special Communications and Information Protection of Ukraine. According the SSSCIP the game broadcast between Wales and Ukraine was replaced with a Russian propaganda channel Izvestia. At least five different TV channels were mentioned affected to spread disinformation on Ukraine.

JUNE 10, 2022

Massive Cyber-Attack Targeting Media Organizations with CrestentImp Malware
Targets: Media
Attribution: Voodoo Bear (GRU)
Over 500 email addresses of media organizations were targeted with malicious emails according to CERT-UA (2022as). The attack was very similar with attack occurred on June 2, 2022, only the lure was changed to “СПИСОК_посилань_на_інтерактивні_карти.docx” [LIST_of_interactive_maps.docx] (CERT-UA, 2022as) and different malware payload was used. The attack continued to exploit same CVE-2022-30190 (Follina) vulnerability.

JUNE 20, 2022

Targets: Unknown
Attribution: Fancy Bear (GRU)
Fancy Bear launched its own cyber-attack campaign using Follina (CVE-2022-30190) vulnerability, according to CERT-UA (2022at). The lure used in the attack was “Nuclear Terrorism A Very Real

Threat.rtf” (CERT-UA, 2022at) and the chosen malware used to exploit victim’s host was CredoMap malware. CERT-UA notes that the document used in the attack was modified on June 9, 2022 according the metadata. This opens up the possibility that the document file was the same one used by Voodoo Bear on June 10, 2022.

Targets: Critical Infrastructure
Attribution: Wizard Spider
Wizard Spider was discovered launching own campaign using the same Follina (CVE-2022-30190) vulnerability, according to CERT-UA (2022au). The difference to the GRU’s hacker units’ methods was attach emails with a password protected ZIP archive “НакладенняШтрафнихСанкцій.zip” [Imposition of Penalty Sanctions.zip] (CERT-UA, 2022au) containing a malicious Microsoft Word file “Накладення штрафних санкцій.docx” [Imposition of penalties.docx] (CERT-UA, 2022au). The messages were sent pretending to be coming from the State Tax Service of Ukraine.

JUNE 25, 2022

Spear Phishing Campaign Targeting Teleoperators
Targets: Communications
Attribution: Voodoo Bear (GRU)
The CERT-UA (2022av) released information of Voodoo Bear’s spear phishing campaign targeting Ukrainian telecommunication operators. Email messages were discovered with topic “Безоплатна первинна правова допомога” [Free primary legal assistance] (CERT-UA, 2022av) and it contained a password protected RAR archive “Алгоритм дій членів сім’ї безвісти відсутнього військовослужбовця LegalAid.rar” [Algorithm of actions of family members of a missing serviceman LegalAid.rar] (CERT-UA, 2022av). The archive included a single Microsoft Excel file “Алгоритм_LegalAid.xlsm” [Algorithm_LegalAid.xlsm] (CERT-UA, 2022av). Malicious macro on the excel file run a PowerShell script to load an EXE file which was used to download and execute a DarkCrystal remote access trojan.

JULY 5, 2022

Phishing Campaign Targeting Government Agencies
Targets: Public Sector

Attribution: Ember Bear (GRU)

A new phishing campaign was targeting Ukraine’s government agencies with Cobalt Strike Beacon, according to CERT-UA (2022aw). The lure used in the campaign was open vacancies on defense sector, “Спеціалізованої прокуратури увійськовій та оборонній сфері. Інформація щодо наявності вакансій та їх укомплектування” [Specialized prosecutor's office in the military and defense sphere. Information regarding the availability of vacancies and their staffing] (CERT-UA, 2022aw). The attack followed the same basic path with having a malicious Microsoft Excel file as attachment “Інформація щодо наявності вакансій та їх укомплектування.xls” [Information regarding availability of vacancies and their staffing.xls] (CERT-UA, 2022aw). The file contains macro that was used to create and execute an executable file named as “write.exe”. As a next step, it checked if a specific file was successfully written and then launched a PowerShell script. The script disabled PowerShell’s logging and bypassed Microsoft’s antimalware scan interface, also known as AMSI. If successful, the script decoded and decompressed its contents as a new PowerShell script used to run Cobalt Strike Beacon.

JULY 11, 2022

Phishing Campaign Targeting Government Agencies

Targets: Public Sector

Attribution: Ember Bear (GRU)

Ember Bear’s phishing campaign using Cobalt Strike Beacon continued with a new lure as suggested by CERT-UA (2022ax). “Об'єднаний офіційний звіт про гуманітарну ситуацію. Україна” [Joint official report on the humanitarian situation. Ukraine] (CERT-UA, 2022ax). The email contained, like in previous campaign on July 5, a malicious Microsoft Excel file “Гуманітарна катастрофа України з 24 лютого 2022 року.xls” [Humanitarian catastrophe of Ukraine since February 24, 2022.xls] (CERT-UA, 2022ax). The macro created this time “baseupd.exe” executable file for dropper which led ultimately to running Cobalt Strike Beacon on victim’s machine.

JULY 14, 2022

Online Fraud on Facebook

Targets: Civilians

Attribution: UAC-0100

CERT-UA (2022ay) issued a warning regarding new phishing campaign spreading on Facebook. The links on social media led to website “Єдиний Компенсаційний Центр Повернення Невиплачених Грошових Коштів” [Unified Compensation Center for the Return of Unpaid Funds] (CERT-UA, 2022ay) which looked like it would be collecting financial aid for Ukraine. The malicious website asked the victim to provide personal information and credit card information. CERT-UA suggested fraud being a part of series of systematic and ongoing campaigns.

JULY 19, 2022

CyberAzov - A Fake DoS Android Application

Targets: Civilians

Attribution: Venomous Bear (FSB)

According to Leonard (2022) of Google’s Threat Analysis Group, Venomous Bear launched its first malware campaign targeting Android based devices. The malicious application named as CyberAzov was hosted on website tricking visitors with Azov Regiment theme and claims of being an application used to do denial of service (DoS) attacks against Russian targets. As suggested by Leonard, the fake application is inspired by similar StopWar application used by IT Army of Ukraine.

GoMet Backdoor Targeting Software Company

Targets: Software, Public Sector

Attribution: Russia

As claimed by Cisco Talos’s Schultz (2022) a large Ukrainian software company was targeted by a cyber-attack using modified version of GoMet backdoor malware. Several Ukrainian government agencies are known to be clients of the company. As suggested by Schultz, the attack was most likely trying to create initial attack vectors as a supply-chain attack. GoMet backdoor is pretty simply malware, but it contains a noteworthy feature for daisy chaining its access on a victim machine or a network, being especially effective on segmented networks.

Massive Phishing Campaign with Stealer Malware

Targets: Civilians

Attribution: UAC-0041

A large phishing campaign using several different stealer malware was launched according to CERT-UA (2022ba). The emails used topic “Остаточний платіж” [Final payment] (CERT-UA, 2022ba) and included a similarly named TGZ archive file as an attachment. In the archive was an executable file that was used to download and execute malicious RelicSource from the attacker's OneDrive. This .NET program was used as an installer and it was having several sophisticated features. It could decrypt at least five different cyphers and it contained multiple methods for establishing persistence on the victim machine. It also contained features to detect if it is being run in a virtual machine to protect itself from analysis. As claimed by CERT-UA, the used stealer malware were Snake keylogger and Formbook, both using Telegram for transmitting stolen data.

JULY 20, 2022

Phishing Campaign Using AgentTesla Stealer Malware

Targets: Public Sector

Attribution: Unknown

A new phishing campaign targeting Ukraine's government agencies was discovered by CERT-UA (2022az). The email contained a Microsoft PowerPoint presentation "Доповідь_050722_4.ppt" [Report _050722_4.ppt] (CERT-UA, 2022az) with a thumbnail image referring to the South (Code name for operational command of Ukraine's army). According to CERT-UA, the malicious macro executed when the document was opened. It executed a sophisticated attack utilizing multiple obfuscation methods (e.g., XOR, base64, Gzip, AES, etc.) and steganography applications. The installed and executed malicious payload to the system was stealer malware known as AgentTesla.

JULY 21, 2022

TAVR Media Hacked to Spread Disinformation

Targets: Media, Civilians

Attribution: Unknown

According to Ukrainian TAVR Media (2022) its servers used as a broadcasting platform was hacked. The platform was used by nine major Ukrainian radio channels which were now exploited to spread Pro-Russian disinformation with false claims regarding President Zelensky's health and him being in a critical condition.

JULY 25, 2022

Spear Phishing Campaign to Ukraine’s Military Academy

Targets: Military, Academic

Attribution: Primitive Bear (FSB)

The national academy of security of Ukraine was targeted with a sophisticated spear phishing campaign according to CERT-UA (2022bb). A vast number of emails was sent to private email addresses of the targeted victims with topics “Інформаційний бюлетень” [Information bulletin] (CERT-UA, 2022bb) and “Бойове розпорядження” [Combat order] (CERT-UA, 2022bb) spoofed to look like coming from the academy. The emails contained attached letter with a malicious HTM dropper used to create a RAR archive to the victim machine using filenames like “22_07_2022.rar” (CERT-UA, 2022bb). Inside the RAR archive was a LNK shortcut file named with highly targeted lure for the victim (e.g., “Інформаційний бюлетень Департаменту контрозвідки Служби безпеки України від 22 липня 2022 року.lnk” [Information bulletin of the Counterintelligence Department of the Security Service of Ukraine dated July 22, 2022.lnk] (CERT-UA, 2022bb)). When the file was opened it downloaded and ran an HTA file containing a VBScript. The script used PowerShell to decode and execute the GammaLoad.PS1_v2 malware. This attack also used Cloudflare DNS services and other similar third-party services to mask IP addresses of attacker’s command and control servers.

JULY 27, 2022

Online Fraud Campaign

Targets: Civilians, Financial

Attribution: UAC-0100

A criminal organization continued to use war and humanitarian related lures in their online fraud campaigns, according to CERT-UA (2022bc). The messages spread on several popular messaging applications were using “допомоги від Червоного Хреста” [aid from the Red Cross] (CERT-UA, 2022bc) as their topic. The messages contained links to fraudulent websites made to look like popular Ukrainian banks. The fake banks asked the victims to provide their banking information which led to compromising their accounts.