CYBER WARFARE – THE GAME CHANGER IN THE BATTLESPACE

A recent development in warfare has been the integration of Electronic Warfare (EW), Information Warfare (IW) and Cyber Warfare (CW) systems designed to generate non-kinetic effects in battle space together with the traditional use of kinetic weapons. These new capacities of armed forces create new possibilities to achieve the goals of war. These advanced and new capabilities form a whole new non-kinetic environment in which they have become a game changer in battle space. This article focuses on describing cyber warfare and the first experiences of the war in Ukraine.

// Martti Lehto

1. Introduction

In the traditional warfare model, nation states fight each other for reasons as varied as the full array of their national interests. Military operations in traditional warfare normally focus on an adversary's armed forces to ultimately influence the adversary's government.

The difference between traditional kinetic warfare and cyber warfare is that kinetic warfare exists only in the physical world whereas cyber warfare exists in both a physical world and a cyber one. Conventional military operations have generally been a mandate of legitimate state military organizations. The vast interconnectivity and interdependence of cyber infrastructure provide a wide range of both independent and state-sponsored cyber criminals with almost the same opportunities to execute malicious attacks in the cyber world. Today, governments and states use cyber criminals as proxies in military cyber missions.

It was discovered in the early 1990s that information infrastructures are vulnerable to attacks. At that time, information infrastructure in particular was the focal point, and this in turn depends on other infrastructures such as electrical power and other forms of energy.

Arquilla and Ronfeldt published in 1993 in an article titled "*Cyberwar is Coming!*" where they described Netwar and Cyberwar. They explained that Netwar refers to information-related conflict on a grand level between nations or societies. It refers to the process of trying to disrupt, damage or modify what a target population "knows" or thinks it knows about itself and the world around it. On the other hand, Cyberwar refers to the conducting, and preparations to conduct military operations according to information-related principles. In their definition, Netwar can also be considered as Information Warfare.

Martin Libicki published an essay titled "What is information Warfare?" in the National Defence University in August 1995. His taxonomy included seven forms of Information Warfare. According to his classification, IW is the top form that includes Electronic Warfare and Cyber Warfare among others.

The term cyberspace was not officially designated by the Department of Defense (DoD) as a warfighting domain until 2006. Prior to 2006, the term cyberspace was perhaps understood as a commercial realm in which the military sent and received data packets but had no real need to do more than to worry about the DoD's own networks. The USA has been a forerunner in the development of cyber warfare capability. Other Western countries have since been making progress as well.

2 Cyberspace

The Internet forms the basic structure of cyberspace. Still, there is no widely accepted definition of cyberspace. Cyberspace is a man-made environment and is therefore unlike the natural domains of air, land, maritime, and space. Hence, cyberspace is a military medium subject to the tenets of warfare that exist in the other physical media. Cyberspace is its own medium with its own rules. Cyberspace has its own unique characteristics in that it is not spatially distinct from the other domains, but rather it pervades all the other domains.

Some definitions divide it into constituent parts or different levels. Some focus more on information flows or processes from a holistic point of view. Yet, others concentrate more on the administrational, governmental, and legal side of this new, artificial, and continuously changing space.

In the US military context, cyberspace is "A global domain within the information environment consisting of an interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

Cyberspace is one of NATO's five operational domains. It was recognized as such in 2016 as the fourth domain after land, sea, and air. Space was then added to the list in 2019.

So, cyberspace is one of the military domains. It requires continuous attention from people to persist and encompass the features of specificity, global scope, and emphasis on the electromagnetic spectrum. Cyberspace nodes physically reside in all domains. Activities in cyberspace can enable the freedom of action for activities in the other domains, and activities in the other domains can create an impact in and through cyberspace.

3. Cyber Warfare (War in bits and bytes)

Cyber Warfare involves non-kinetic attacks on information data and its collection process aimed at damaging, disrupting, or destroying decision-making processes. It is both offensive and defensive, ranging from methods that prohibit the enemy from exploiting information to corresponding measures to guarantee the availability, reliability, and interoperability of friendly information assets. Thus, CW encompasses the use of all digital system "tools" available to paralyze or even destroy the enemy's ICT-technology based systems while keeping one's own systems operational. Cyber warfare is an outcome of information age components like satellites, electronic mailing system, internet, computers, and micro-chips.

Where does one draw the line between cyber warfare and traditional warfare? Definitions matter when implementing policy, and in developing CW a variety of factors must be considered. In essence, this question focuses on the role of information technology as an enabler of warfare and therefore, as a viable target from both attack and defense viewpoints. Cyber warfare will have kinetic effects, meaning it will cause real, direct and indirect damage to physical infrastructure.

Cyber warfare involves the actions by a nation state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. Cyber warfare refers to a country's use of digital attacks such as computer viruses and hacking to disrupt the vital computer systems of another, with the aim of causing damage, death, and destruction.

The effects of cyber-attack may be categorized as either desired or undesired, as well as direct and indirect. These include but are not limited to securing, isolation, containment, neutralization, recovery, manipulation, exfiltration, degradation, disruption, or destruction. In the effects-based cyber operations, digital systems can be targets that are either concrete (physical) or abstract (mental).

Martin C. Libicki's structure for the cyber world uses a four-layer cyber world model: physical, syntactic, semantic, and cognitive. Using Libicki's structure and adding service as a fifth layer, we have a five-layer cyber world model: physical, syntactic, semantic, service, and cognitive.

The physical layer contains the physical elements of the military communication and information network. **The syntactic layer** is composed of various military system control and management programs and features which facilitate interaction between the devices connected to the network. **The semantic layer** is the heart of the entire network. It contains the information and datasets in the armed forces data warehouses and computer terminals, different large-scale information systems, as well as different user-administered functions. **The service layer** contains all the IT-based digital military services for users in the network. **The cognitive layer** provides the decision makers and warfighters with an information-awareness environment i.e., a world in which information is being interpreted and where one's contextual understanding of information is created. The cognitive layer can be seen as the mental layer from a larger perspective; it includes the user's cognitive and emotional awareness.

Cognitive layer

- Decision makers and warfighters information-awareness environment
- Contextual understanding of information

Service layer

- The digital services for Army, Navy, Air ja Space Force and Cyber Force
- The Common core services

Semantic layer

- Information and datasets in the Armed Forces in the data warehouses, and computer terminals,
- Different large-scale information systems, as well as different user-administered functions

Syntactic layer

- Military system control and management programs and features
- Protocols and software: send, receive, store, format, and present data

Physical layer

- Physical military communication and information networks, cellular technologies
- Network devices, switches and routers, fiber-optic cables

The enemy should be considered a complex system during execution of effects-based cyber operations. This means that the attacker can exploit different cyberspace attack vectors to impact the target. Target analysis involves the systematic discovery of enemy system components and especially the vulnerabilities of systems. Systematically and consistently planned and executed effects-based cyber operations have the potential to create a strategic impact on a national/state level. In practice, the target is the civilian and military physical cyber-infrastructure, so the destruction or disruption will cause collateral damage to the whole society, which in many cases is the intention of the attacker.

Cyber infrastructures can be used by cyber criminals with almost the same possibilities to execute malicious attacks in the cyber domain, which can help military operations. For example, Russia's cyber group known as Sandworm Team, often implements cyber operations as a proxy for GRU (foreign military intelligence agency of the General Staff of the Armed Forces of the Russian Federation). Sandworm attacked Ukraine's energy facility in February 2022. Attackers succeeded in planting a new version of the Industroyer malware to disrupt ICS infrastructure at different levels. The cyber-attack was detected and prevented by the Ukrainian team.

Russia vs. Ukraine in Cyber Warfare

The Armed Forces of the Russian Federation define information warfare as "confrontation in the information space with the goal of causing damage to critical information systems, undermining political, economic, and social systems, psychologically manipulating the public to destabilize the state and coerce the state to make decisions to benefit the adversary party", according to public Defense Ministry documents.

Russia launched its war on Ukraine on 24 February 2022, but Russian cyber-attacks against Ukraine have persisted ever since Russia's illegal annexation of Crimea in 2014, and they have intensified just before the 2022 invasion. After 2014, hundreds and even thousands of cyber-attacks occur each month, making Ukraine the perfect place for Russia to test new cyber-weapons, tactics, attack vectors and tools.

ATTACKS DURING 2014-2022

In March 2014, Russia launched a DDoS cyber-attack aimed to paralyze Ukrainian computer networks and communications to divert public attention from the presence of Russian troops in Crimea.

In May 2014, prior to the Ukrainian presidential elections, a pro-Russian hacktivist group carried out a series of cyber-attacks to manipulate votes. The attack failed, as the malware was removed 40 minutes before the election. However, the hackers managed to delay the election count.

In the following couple of years 2015 and 2016, there were two cyber-attacks on power grids. In 2015, the Russian state-sponsored Sandworm Team succeeded in paralyzing the systems of 16 electrical substations, such that over 230 000 consumers in western Ukraine experienced power outages ranging from one to six hours. A similar cyber-attack occurred in 2016.

The NotPetya attack in June 2017 hit the Chernobyl nuclear power plant radiation monitoring system and close to 13 000 devices used by public institutions, banks, postal services, newspapers, transport infrastructure and businesses. The malware had a global impact, affecting 65 countries and about 50 000 systems, and inflicted a loss of over 10 billion USD.

The cyber weapon production for the war had already begun at the latest in the fall of 2021. According to the code's timestamp, hackers created different malwares for attacks on critical infrastructure and several malwares for phishing attacks.

In addition, in December 2021, there was a phishing attack on the State Migration Service of Ukraine and a group compromised the network of a nuclear safety organization. Later on in March 2022, they also stole data from this organization.

ATTACKS AFTER FEBRUARY 2022

This analysis of cyber operations in the Ukraine war is based on publicly available information from Microsoft, the Center for Strategic & International Studies, and the European Parliamentary Research Service.

According to Microsoft analysis, a day before the military invasion on February 24, 2022, six separate

Russia-aligned, nation-state actors launched more than 237 operations against Ukraine. These included destructive WhisperGate malware attacks masquerading as ransomware on hundreds of systems in Ukrainian government, IT, energy, and financial organizations. The destructive attacks have also been accompanied by broad espionage and intelligence activities. Since then, attacks have included attempts to destroy, disrupt, or infiltrate networks of government agencies, and a wide range of critical infrastructure organizations. These cyber-attacks have at times not only degraded the functions of the targeted organizations but also sought to disrupt the citizens' access to reliable information and critical life services, and to shake their confidence in the country's leadership.

Also, hackers have targeted a Western government agency operating in Ukraine with a phishing attack at the same time.

CYBER-ATTACKS AFTER 24.2.2022 TO JUNE 2022

Attacks on critical infrastructure tried to disrupt, paralyze, or destroy the systems. The following is a list of targets affected by these operations:

- A destructive malware (HermeticWiper) targeting 300 systems such as dozens of financial, government, energy, information technology, and agricultural organizations.
- The network of an agricultural grain production company.
- A destructive malware (IsaacWiper) targeting the Ukrainian government network.
- A destructive malware targeting satellite communications company, Viasat.
- A destructive malware targeting Ukrainian border control.
- At least 30 Ukrainian university websites.
- Telecom provider, Triolan.
- A destructive malware (DesertBlade) targeting a major broadcasting company.
- A disruptive attack on charities, non-governmental organizations, and other aid organizations.
- A Ukrainian research institution.
- A disruptive attack on the Vinasterisk network in western Ukraine.
- A destructive malware (CaddyWiper) targeting many Ukrainian organizations.
- A destructive malware (DoubleZero) targeting Ukrainian enterprises.
- A transportation and logistics provider.
- Attack on Ukrtelecom reduced connectivity in the country to 13 percent of pre-war levels.
- A Ukrainian energy facility trying to shut down electrical substations in Ukraine.

Phishing attacks were used to gain access to sensitive data and user identification information, and to steal this sensitive information. The targets were included the organizations such as the following: Ukrainian state bodies, Ukrainian government, the Ukrainian energy company and media. In addition, phishing attacks were targeted at different personnel groups, in particular high-profile Ukrainians. Also, attackers deployed malware that compromised user data, uploaded backdoors, and stole Telegram accounts.

Several DDoS attacks focused on the Ukrainian banking sector and government websites, Kyiv Post, WordPress websites, Ukrainian government agencies, and financial sites.

Alongside cyber operations, Russia also executes several information operations, such as disseminating fake news via the media company Ukraine 24 that President Zelensky announced a surrender to Russia. One of the targets included the platforms of several Ukrainian news outlets defaced with symbols banned in Ukraine, and hackers created a fake Ukraine 24 Facebook page, prompting users to enter their personal data and payment information.

In the initial phase, the focus was on attacking critical infrastructure. At the beginning of April, phishing attacks targeting Ukrainian government officials also increased.

It seems that Russia has also received external help. The Times reported in February 2022 that Chinese hackers targeted vulnerabilities in over 600 critical infrastructure institutions and the Defense Ministry in Ukraine to compromise data and disrupt services.

> **Cyber Warfare (CW) goes beyond the boundaries of traditional Information Warfare (IW).**

Summary

Cyber Warfare (CW) goes beyond the boundaries of traditional Information Warfare (IW). In CW the battle is in bits and bytes while in IW the battle takes place in the human mind. The integrated employment of the core capabilities of CW in tandem with specified supporting and related capabilities to influence, disrupt, corrupt, usurp, paralyze, or even destroy adversarial human and automated decision-making while protecting our own and finally, the adversary's ability to wage war.

The structural reorganization is now underway. For example, the mission statement of the U.S. Army Cyber Command now reads that it "integrates and conducts full-spectrum cyberspace operations, electronic warfare, and information operations, ensuring freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries."

There is no 100% foolproof cyber defense, but Ukraine's efforts have so far mitigated the Russian cyber-attacks. It seems that for offensive operations, planning for cyber operations must be integrated into broader campaign planning and there is a need to gauge where and when their use is beneficial. Cyber missions must integrate other offensive capabilities. Cyber-attacks alone are not an option for kinetic action.

Cyber-attacks already perform well in terms of speed, range, and precision and may offer greater possibilities for surprise, but their destructive capabilities are still limited. Use of offensive cyber-attacks require precision analyses on how much of it is necessary to achieve a strategic effect.

The offensive cyber campaign plan needs to include a realistic and specific assessment of the benefits and costs of cyber operations, including the efforts needed for intelligence collection. Planning must be realistic because a cyber operation will require an analysis of the specific target and intended effect. Cyber weapon design (code-writing) and testing are also needed well in advance prior to the cyber-attack reconnaissance of the target network.

Planning for offensive cyber operations must take into account the politics of cyberattacks in connected civilian networks. The cyberattacks harm civilians, including degrading their access to online services and social media, with which the attacker aims to paralyze the vital functions of society and weaken the citizens' will to defend themselves.

It seems that Russian cyber operations failed to advance its goals - the occupation of Ukraine and the replacement of its government. The lesson learned for cyber warfare in Ukraine is that effective preparation and planning are needed to integrate cyber operations with kinetic attacks to achieve maximum effect.

This also means that the integration of all operations in the electromagnetic spectrum and digital environment, i.e., the realm of digital and electronic communication systems and the information conveyed through them, becomes increasingly necessary. ■

DR. MARTTI LEHTO

Dr. Martti Lehto, (Military Sciences), Col (GS) (ret.) works as a Cyber security professor in the University of Jyväskylä in the Faculty of Information Technology. He has over 30 years' experience as developer and leader of C4ISR Systems in Finnish Defence Forces. Now he is a Cyber security and Cyber defence researcher and teacher and the pedagogical director of the Cyber Security MSc. program. He is also Adjunct professor in National Defence University in Air and Cyber Warfare. He has over 100 publications, research reports and articles on the areas of C4ISR systems, cyber security and defence, information warfare, air power and defence policy. Since 2001 he has been the Editor-in-Chief of the Military Magazine

"The development of strategic cyber situational awareness requires the ability to produce analyzed information about the events in cyberspace and thus create the required situational awareness."