HADMÉRNÖK

XIII. Évfolyam „KÖFOP" szám – 2018. január

CAPABILITIES OF COMPUTER NETWORK OPERATIONS IN THE WORLD

SZÁMÍTÓGÉP-HÁLÓZATI MŰVELETI KÉPESSÉGEK A VILÁGBAN

BERKI Gábor

(ORCID: 0000-0002-9531-4074)

berki.gabor@uni-nke.hu

Abstract

At the 2016 NATO Summit in Warsaw, special attention was paid to cyber security. Heads of State and Government recognized cyberspace as a new operational environment in which NATO has the same defence functions as in the air on land, and sea. The aim was set at enhancing the protection of the networks of the Alliance and, after the 2014 Wales Summit, the extension of the collective protection to cyberspace was repeatedly declared. This means that if a coordinated cyberattack is launched against one of its member states, NATO will consider it as an attack against the Alliance as a whole. However, the question arises: what states or organizations are capable of preparing and executing such an attack. The following study presents what are the computer network operations which comprise the basis for such an attack, what conflicts have taken place in this area in recent years, and what potentials the world's leading powers have in terms of computer network warfare. The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in Győző Concha Doctoral Program.

Keywords: *computer network warfare, cyber defence, cyberattack*

Absztrakt

A NATO varsói csúcstalálkozóján 2016-ban kiemelt figyelmet kapott a kiberbiztonság. Az állam- és kormányfők a kiberteret új műveleti környezetként ismerték el, melyben a NATO-nak ugyanúgy védelemi feladatai vannak, mint a szárazföldön, a tengeren vagy a levegőben. Célul tűzték ki a szövetséges hálózatok fokozott védelmét, valamint a 2014-es walesi csúcstalálkozó után újból deklarálták a kollektív védelem kibertérre történő kiterjesztését. Ez azt jelenti, hogyha az egyik tagállama ellen koordinált kibertámadás történik, azt a NATO a szövetség egésze elleni támadásnak fogja tekinteni. Felmerül azonban a kérdés, hogy kik azok az államok vagy szervezetek, akik képesek ilyen támadást előkészíteni, megvalósítani. Az alábbi tanulmány bemutatja, hogy mik is azok a számítógép-hálózati műveletek, amelyek egy ilyen támadás alapjait képezik, milyen konfliktusok voltak az elmúlt időben ezen a területen és hogy a világ vezető hatalmai milyen potenciállal rendelkeznek a számítógép-hálózati hadviselés tekintetében. A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Concha Győző Doktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *számítógép-hálózati hadviselés, kibervédelem, kibertámadás*

A kézirat benyújtásának dátuma (Date of the submission): 2017.08.30.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.01.09.

INTRODUCTION

By the present information technology has penetrated societies to such an extent that not only industrial, financial, or governmental work but also the daily life of people could be possible to envisage without computers. This fact is proven by the data stating that in March 2017 49.7% of the total population of the World – more than 3.7 billion people – used the internet (77.4% of the population of Europe, and 88.1% of North America). [1] It does not seem to be an exaggeration to state that modern people are significantly addicted to information technology systems.

However, the IT devices and services making daily life easier have significant security risks as well. An increasing amount of information is available about various computer attacks committed and damage made. Reference can be made to ransomware recently paralysing even hospitals, which encrypted the data on computers and demanded money for them, or to attacks launched against banks and their clients, aimed at getting sensitive customers' information. A large number of malicious hackers may be met on the internet. Simple criminals who want your money, spies who want to get our secrets, fanatics who want to grab our attention because of their political views or religious convictions. Such people or groups carry out their attacks with the use of various IT methodology which ranges from hacking web sites to sending letters with malicious codes and to hacking into computer networks. The methods are similar, the goals make the difference.

The rapid development of information technology also affected military organisations and law enforcement agencies because the devices they operate and the collected, processed and stored data are of national security significance therefore their protection is top priority. It was quickly realised how great significance it would be in the course of a potential conflict if similar systems of the adversary party could be successfully attacked, the stored data could be obtained, altered, or destroyed. Therefore, besides making the protection as efficient as possible, the elaboration of the ways of attacks also began.

In this article I wish to present the computer network warfare, the results achieved in this field by the leading powers of the World, and their relating capabilities.

COMPUTER NETWORK OPERATIONS

Before a detailed description of the computer network warfare, its position within military operations should be introduced. An activity defined as computer network operations comprises an organic part of information operations. In NATO information operations are detailed in doctrine AJP 3.10 while in the Hungarian Defence Forces it is the Information Operations Doctrine, issued in 2014, which deals with the question. In the framework of information operations closely related activities are integrated in order to achieve information superiority in military operations, in order to have information domination and leading superiority through achieving time reduction for friendly forces and time expansion for the opposing party. In practice, more reliable information can be obtained by friendly parties in shorter time than by the opposing party, which allows making conclusions for good decisions to be made. All this may provide operational superiority as well. Such activities have their impact in the physical, information, and conscious dimensions. Apart from computer network warfare, these activities are also part of electronic warfare, psychological operations, operational security, military deception, and physical destruction, and even civil-military cooperation and mass communication can also fall into this category. [2, p185]

The figure below illustrates the position of computer network operations within information operations.

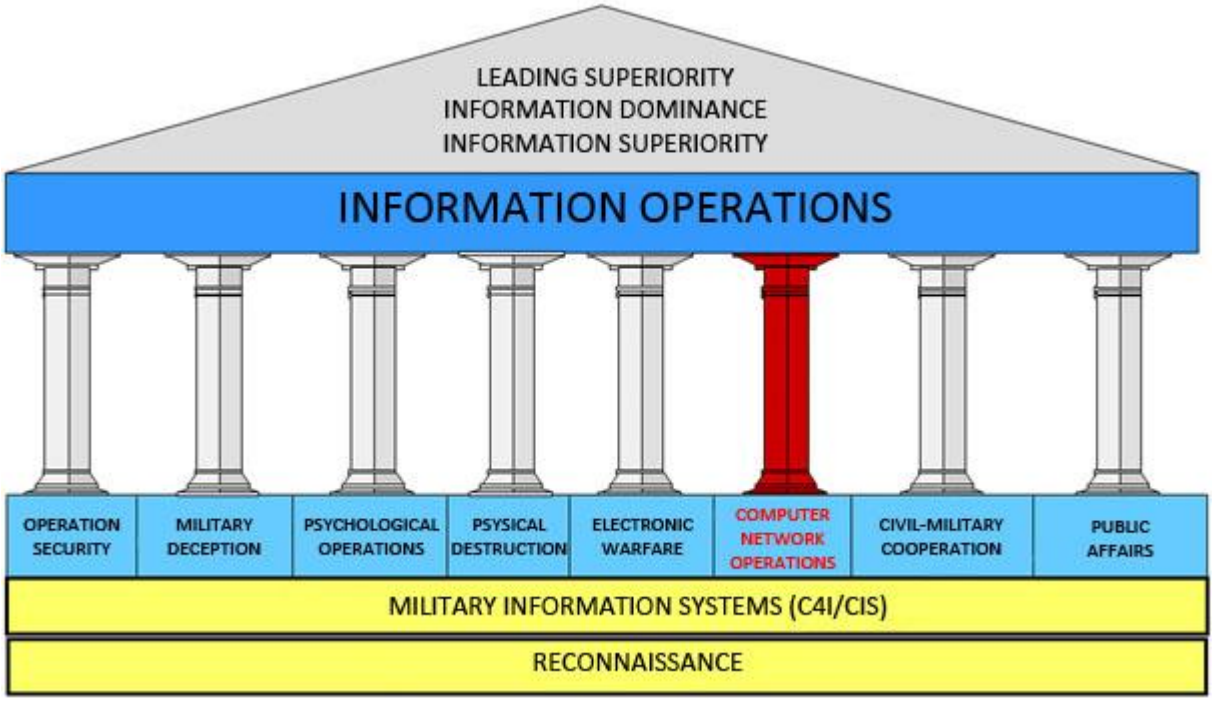

Fig. 1. Computer Network Operations in the Information Operations
(drawn by the author based on reference No. 2, p 198)

Military experts in the United States use a somewhat different approach. A new concept of operation was elaborated, which was published in doctrine FM 3-38, entitled Cyber Electromagnetic Activities. It means that electronic warfare, cyber operations, and frequency-management operations are integrated and synchronised in order to have mutually complementing and reinforcing effects. It is easy to understand that the lack of cooperation among the above activities would reduce the efficiency of operations, and generate undesirable clashes and interferences among devices and systems used in the electromagnetic spectrum. [3, p122] The name of computer network operations was also changed and the term Cyberspace Operations[1] was introduced. Cyberspace is recognised as a domain of warfare which is equal in significance with land, air, sea, and space dimensions of operations. Cyberspace operations are divided into offensive and defensive operations and are complemented with a third element: the military information network operations.

In accordance with the definition of the doctrine: „*Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system."* [4]

This concept is illustrated with the figure below:

[1] Abbreviated: CO

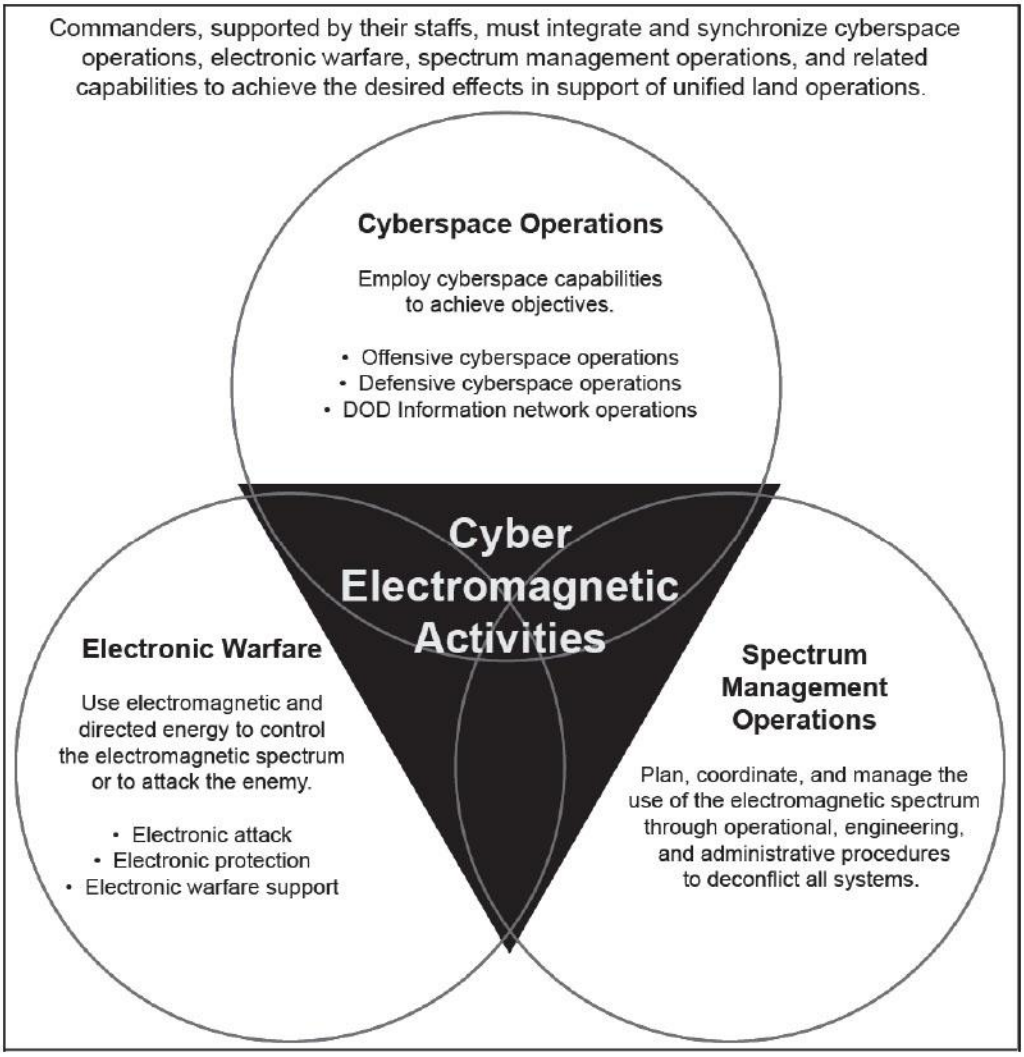

Fig. 2. Cyber electromagnetic activities
(source: [4 p1-2])

Computer network operations may be divided into two major groups. Offensive operations are aimed at mapping adversary IT systems in a network, influencing, degrading, and paralysing their operation, while defensive activities mean the protection of friendly computer networks from the information attacks of adversaries.

A computer network attack is a software- or hardware-based penetration into the information system of the attacked party with the aim to destroy, modify, or make inaccessible data stored there, or to make the operation of the system impossible in itself. Such attacks are executed by well-prepared IT experts, so called hackers, who know information systems better than anybody else at a standard or user level, are able to illegally enter the networks at their weak points, gain right of access and make various operations there. [2, p228] It is important to note that such experts do not always use their knowledge only for harmful purposes as they may work on eliminating the weak points of a system as well. In this case such activities are labelled as ethical hacking.

Malicious software and its large number of sub-types must be highlighted among the means of computer attacks. The well known viruses are programs which add their own program codes to another program and this way they multiply and spread. Usually they have two main parts; one is responsible for the spread while the other is the core which contains the activity to execute. Computer worms are standalone programs which are capable of multiplication, and spreading themselves. Their structure is similar to that of viruses but usually they have an additional part of program responsible for disguise making more difficult to disclose and

identify them. Trojan programs are seemingly useful applications with useful functions, however, besides their original functions they execute unwanted operations too. There are also various types of spyware, keyboard tracers, and their countless combinations. [3, p131]

Another frequently used method is the use of botnets or zombie networks. A zombie computer is a computer under the control of a malicious hacker through Trojan software. Afterwards the capacities of the computer are used for the attacker's purposes, often for launching DDoS[2] attacks. Botnets are the networks of such zombie computers. If attackers have an appropriate amount of zombie computers, they may be able to overload the selected target thus making it inoperable. Computers controlled such way are also used for sending masses of spams – unwanted letters. It is important to note here that such devices are used not just in the field of computer network operations but also by criminals and other malicious attackers.

Obviously, operations of defensive nature are aimed at protecting friendly information systems against adversaries' offensive activities. The tools of defensive operations are firewalls which filter illegal network traffics, and various types of antivirus software which recognise and destroy malicious codes.

It is very important to underline that computer network operations takes place only when a country launches an attack against the computer networks and critical infrastructures of another state with the use of information technology and physical means on its own account or with the involvement of a third party. Such a third party may be a state, an organisation, or a group. However, this has been impossible to prove in relation to the attacks of the past years because all suspected countries categorically denied the accusations.

MAJOR ATTACKS TO DATE

According to special literature the very first documented cyberattack was launched by a Sri Lanka terrorist organisation, the Tamil Tigers, in 1997. [5] Their method would seem fanciful nowadays – they flooded governmental sites with unwanted e-mails.

In 1999 Serbian hackers – in response to the NATO air campaign over Serbia – attacked the servers of the Alliance and made some of them inaccessible for a while with the use of DDoS method, and also broke in some web sites and placed there propaganda messages.

The first cyberattack launched against a country happened in 2007. In Estonia, which has highly developed IT culture, riots broke out due to the removal of a Soviet war monument from downtown Tallinn on 27th April 2007. The first signs of DDoS attacks appeared a few days after the first protest demonstrations, and were targeting the servers of Parliament, government offices, ministries, banks, telephone companies, and media companies. The selection of targets, the coordination, precise execution, and efficiency of attacks clearly indicated that there were organised forces in the background of the attacks. In a few cases it was established that the attacks had been launched from Russian servers, which was denied by Russian authorities, of course. At the same time the nature of the attacked servers indicates that the clear objective of the attacks was to paralyse the critical information infrastructure of the Baltic state. The key servers, responsible for the on-line data traffic of the country collapsed on a daily basis, and the networks of many state institutions had to be temporarily disconnected from the internet. Electronic banking and trade either ceased or significantly stalled. According to some experts the cyberattack inflicted much more significant economic damage to Estonia than the trade sanctions could have which Russia threatened the country with in the first weeks of the crisis.

[2] Distributed Denial of Service

Although NATO experts were also involved in the initial phase of the investigation, due to the nature of the attacks it was nearly impossible to identify the attackers. Although many of them could be identified in Russia, it was impossible to clearly prove that governmental servers were involved in the action. According to generally accepted views Russian hackers with patriotic emotions established a botnet in which apart from Russian computers hardware in another 178 countries were also involved without their knowledge (zombie computers) and the attacks were executed through them. [5]

The Russo-Georgian war in August 2008 also had a cyber aspect. As it is well known, the president of Georgia tried to resolve the long-lasting Georgian-Ossetian and Georgian-Abkhazian conflict through attacking the mentioned territories with the use of military force on 8th August 2008. However, he had miscalculated the situation when had not taken into account that Russia would not tolerate the attack inter alia because it had troops stationed in South Ossetia involved in a peacekeeping mission under UN mandate. The Russian troops delivered powerful counterstrikes at the Georgian forces and after five days of heavy fighting Georgia was forced to request a ceasefire. [6]

During the armed conflict a cyber campaign was also launched against Georgia. Russia– or at least somebody in Russia – took control of internet traffic, according to the Georgian government, which was virtually forced into a cyber emigration and besides the war reports a large number of reports were also issued about virtual attacks. [7]

The most spectacular hacker actions were launched against the country's governmental web sites which were paralysed from outside and their contents were changed.[3] The hackers from Russia vandalised the portraits of president Saakashvili. Hitler-moustaches were drawn on the images of the head of Georgian government and a number of pictures of him were published depicting him posing as the Nazi dictator or copied his portrait among the greatest thugs of human history.

At the same time web sites aimed at discrediting the country were also established for disinformation purposes – the blog continuously reporting about the conflict listed the credible sources among the links. In the Caucasian country web sites with domain extension .ru also became inaccessible. According to some sources, they were blocked by the Georgian government itself in order to halt Russian propaganda and the workers of the Russian embassy in Tbilisi claimed that there had been problems with mobile phone and landline telephone services too (although that must have been because of the military offensive). [8]

In my opinion the Georgian government clearly exaggerated the cyberattacks launched against it since Georgia did not have such highly developed infrastructure as, for example, Estonia therefore the cyberattacks did not have such a serious impact: neither the banking system nor public administration got paralysed. Large scale attacks on the internet are particularly effective if they are launched against a country which strongly relies on information technology and on its infrastructure. In the case of Georgia this was not the case: through the internet the attackers were not able to inflict more damage than the Russian soldiers stepping on the soil of the country. It is not easy to understand why the government focused on the cyberattacks while Georgian towns and infrastructure were bombarded by Russian forces. Nevertheless, this was the conflict where cyber operations were also used for supporting conventional military operations.

It can be stated both in connection with the Russian-Estonian and Russian-Georgian conflicts that Russian official authorities categorically denied their involvement in the attacks. The post-

[3] In internet jargon: defacement.

conflict analyses could only establish that the attackers were motivated by Russian nationalistic emotions, however, it was impossible to prove the participation of any Russian state agencies.

Attacks targeting some critical infrastructures should not be ignored either. These facilities may comprise part of electric works, power stations, or other vital systems. There have been several attacks in the World (Brazil, Turkey) resulting in the breakdown of electric supply caused by a cyberattack. In December 2015 an attack of such type was also registered in Ukraine, which resulted in a several-hour-long blackout affecting 1.4 million people. [9]

Malicious codes used for attacking critical infrastructure and industrial process control systems have become increasingly developed and sophisticated in recent years. The creators of such codes put great emphasis on the development of the hiding capabilities of their programs, thus making them more difficult to detect. A typical and notorious example of these programs is the new malicious code, named Stuxnet, discovered by the Belarusian VirusBlockAda in June 2010.

The new worm spread on Microsoft operating systems and was developed exclusively against industrial process control systems. The exceptional nature and specialization of Stuxnet is highlighted by the fact that these industrial surveillance, control and data collection systems are manufactured by a single company, German Siemens (SIMATIC WinCC HMI and WIMATIC STEP 7) and are basically used in heavy industry, energy production, and transportation. This means, the threat is presented basically for facilities only, some of which are classified as critical infrastructures. [10]

Stuxnet's ultimate goal was to reprogram the automatic processes of industrial control systems. It primarily attacked PLC[4] software. Software WinCC / Step 7 was the primary of all Stuxnet targets. This software connects to the PLC via a data cable, reaches memory content, is capable of re-configuring processes and uploading programs, and performs some tracking functions during the execution phase. If the PLC has already been programmed, it can be switched off and the PLC is able to operate on its own. Stuxnet used this software to enter its code blocks into the PLC and then hid them.

Stuxnet searched the PLCs for specific industrial devices, namely frequency converters of high-speed motors, and only entered into action when it found the Finnish Vacon or Iranian Fararo Paya devices, and if the monitored device operated between 807 and 1210 Hz. Such frequency converters and motors are used almost exclusively in Iranian uranium enrichment facilities. [11]

The clear purpose of the virus was the undetectable destruction of uranium enrichment centrifuges and the degradation of the enrichment process. This goal was successfully achieved since at least 1,000 centrifuges were made unusable in the Natanz enrichment facility and, according to many experts' opinions, disrupted the Iranian nuclear program for at least two years.

It is a proof for the professionalism of the writing of the attack code that it exploited four zero-day[5] threats simultaneously, and certified its legitimacy with two stolen digital signatures.

[4] PLC - Programmable Logic Controller, used in large numbers in industrial regulation technology, various electric processes, and procedures operated this way.

[5] Term *zero-day/zero-hour* is used for describing computer security threats which exploit a undisclosed, unpublished vulnerability of a given IT application. Having disclosed a vulnerability the attacker makes a so called *zero-day exploit* which is a computer code capable of exploiting the particular vulnerability. However, because of the difficult detectability of vulnerabilities the makers of malware a disclosed vulnerability is of significant significance and value therefore one program is usually based only for the exploitation of one vulnerability. During such attacks the developer of the attacked application is usually unaware of the vulnerability or has not been able to make corrections.

There were no accurate data about its origins for a long time, but everyone thought of the United States and Israel as of the two countries which were capable of and interested in launching an action against the Iranian nuclear program. In his blog Ralph Langner, a Hamburg virus security expert, was deeply involved with Stuxnet and in his post on 31st December 2010 he wrote:

„The forces behind such a high-profile attack can be traced easily. Stuxnet required an extreme amount of intelligence about the Natanz plant layout, a full understanding of the IR-1[6] *operation (presumably with a mockup test system available), and an extreme amount of insider knowledge of the Siemens products involved. This limits the search for the originators to very few organizations in the world."* [12]

In February 2016, Alex Gibney's documentary Zero Days was presented at the Berlin International Film Festival, which deals with this topic. The film also features General Michael Hayden, who was also head of the CIA[7] and the NSA[8]. In the documentary he acknowledges that Stuxnet was developed in cooperation with Israel, and targeted specifically Iran's nuclear program. [13]

But Stuxnet was just the beginning of a new generation of malware. In 2011 and 2012 the staff at CrySyS Data and System Security Laboratory at the Budapest University of Technology discovered Duqu, and sKyWiper codes respectively, which were also very sophisticated and state-of-the-art tools and some state involvement in their development could be almost taken for granted. In early 2015, Kaspersky Lab found a new malicious code labelled as Duqu 2. The new code is the most sophisticated the Lab's workers have ever met, and its creators' mindset and philosophy are completely new. According to the company's senior researcher, that spyware had been used for attacking around 100 targets, including luxury hotels in which Great Power negotiations aimed at curbing the Iranian nuclear weapons program were conducted. [14]

At the same time the quantity of attacks and ransomware keeps rising continuously. In May 2017, for example, a large-scale ransomware campaign was launched worldwide. The ransomware cryptoworm, named WannaCry, infected tens of thousands of computers in a few hours' time and encrypted their files. The global cyberattacks generated significant interruptions and delays all over the world, for example, in the affected British hospitals a large number of operations had to be postponed due to the unserviceability of their IT hardware. A few weeks before the attack, hacker group The Shadow Brokers had leaked a tool EternalBlue, allegedly used by the NSA for breaking in distant computers with the use of a security breach of the Windows operating system. [15] WannaCry usually got in the computer of a victim wrapped in an e-mail, however, through a generally used network protocol (SMB) it easily propagated onto other workstations of the network. Although Microsoft had completed the correction of the mistake, at the time of the attack many users still failed to install that on their computers. The further destruction caused by the ransomware was prevented by a British IT expert who discovered a switch in the software disallowing its further propagation.

A few weeks later another ransomware appeared which also encrypted the files on the attacked and infected computer. The malware named Petya began attacking Ukrainian targets and very soon appeared in other countries as well. The propagation of the worm started through a seemingly entirely innocent accounting software upgrade widely used in Ukraine, coming from a completely secure source. For further propagation in networks this ransomware also

[6] The name of the Iranian variant of Pakistani P-1 uranium-enrichment centrifuge, given by the outside world.
[7] Central Intelligence Agency
[8] National Security Agency

used EthernalBlue. According to experts both its operation and settings indicated that the hackers' objective was not financial profit making but rather destruction and panic-mongering. [16]

These data also underpin the fact that a lot of military organisations and government bodies in the world are seeking to gain decisive influence in cyberspace, not only to strive for capabilities to fend off attacks, but also to have an attack capability.

Fending off IT attacks has now become a top priority in the World. Everywhere it has been realized that cyber security is essential and key information systems need to be protected against cyberattacks. In May 2008, the Cooperative Cyber-defence Centre of Excellence (CCDCoE) was established. On 14th May, the Memorandum of Understanding was signed by the founding countries, the Baltic States, Germany, Spain, Italy and Slovakia. On 28th October 2008, by the decision of the North Atlantic Council, the Centre was legally declared an international military organization. The fact that the Centre was established in Tallinn, Estonia's capital is a significant indication. The Centre's tasks include, inter alia, support to the development of member state cyber capabilities, that of national doctrines, concepts and strategies, training in the field of information security, conduct of continuous training programs and exercises, and the analysis of the legal aspects of cyber-warfare. That is, the organization does not represent NATO's offensive cyberattack capabilities, but functions as a research and education centre. Hungary joined the work of the Centre on 23rd June 2010.

A publication, issued in 2013, was compiled by internationally renowned lawyers, technical specialists and researchers and was titled "Tallinn Handbook on the International Law Applicable to Cyber Warfare". This manual covers the regulation of cyber warfare, detailing them in 95 major rules in 2 parts, on more than 300 pages. The title of the first part is "International Cyber Security Law" and that of the second is "The Law of Cyber Armed Conflict". It is stated that a cyberattack can be classified as an armed attack, so that the attacked state can legitimately use even conventional weapons for self-defence. However, cyber-espionage, cyber-bullying or cyber-harassment, and hacking websites are not considered as armed attacks. It is pointed out that civilian casualties must be avoided, that is civilian targets, hospitals, nuclear power plants, hydroelectric power stations or dams must not be attacked – as is the case with traditional armed conflicts – which is now prohibited for the belligerents by the Geneva Conventions. The principle of proportionality should also apply to cyber warfare, on the basis of which the attacked party cannot inflict much greater losses to the attacker than it has suffered before.

It can be stated that outstanding work has been compiled in the field of regulating cyber-warfare, which does not have compulsory recommendations, nevertheless the preliminary wide-range consultations resulted in establishing principles which may be well used in the legislation of individual countries. [17] 2017 saw the publication of version 2.0 of the manual, extended with legal analyses and case studies.

NATO regards attacks in cyberspace as a significant threat. At the Summit Meeting held in Warsaw on 8th and 9th July 2016 the objective was set to develop cyber defence, to integrate it into planning processes at a larger extent, and to increase the protection of national and allied networks with the use of the most up-to-date technologies. After the 2014 Wales Summit Meeting the extension of collective defence on cyberspace was declared again. [18]

As it has been mentioned above the Tallinn centre does not develop NATO's offensive cyber capabilities – the organisation does not even have a program of such type – however, certain member states deal with developing offensive capabilities although this process is not open to public scrutiny. In many countries of the World research programs were launched besides increasing their cyber-defence capabilities to the highest possible level to enhance their offensive capabilities as well.

CNO CAPABILITIES IN THE WORLD

The United States, both as the country of origin of internet and the leading power of the World, makes extremely huge efforts to preserve its positions in cyberspace. Taking this into account the Department of Defence approved a resolution on the establishment of a military Command which would coordinate cyber-defence at national level. The USCYBERCOM[9] started its operation in subordination to the Strategic Command of the United States, in Fort Mead, Maryland, in 2010. According to its mission statement:

„*USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."* [19]

All cyber operations military units of every service were subordinated to the new Command. This means: U.S Army Forces Cyber Command, 24th USAF, Fleet Cyber Command and Marine Forces Cyber Command. Its full operational capacity is expected to be reached in 2018, when 6,200 personnel will serve there. Its activity is coordinated with the NSA, responsible for electronic intelligence. The commander of the unit is also the director general of the NSA. [20] The proper reason for the development of operational capabilities was the growing threat that the US military and civil IT networks were facing. The Command has to be capable of delivering an appropriate counterstrike in cyberspace in the case of a traditional or an IT attack targeting the country. A cyberattack can be ordered by the President of the United States of America either as a response to an attack against the military or civil computer networks of the country, or in order to prevent such an attack. The methodology of defence from cyberattacks against the US, and that of counterstrikes were laid down in the International Cyber-security Strategy, issued in 2011.

In accordance with the strategy, American cyber defence is based on prevention and deterrence. The basis of prevention is international cooperation. The establishment of international law enforcement cooperation is encouraged, which would allow further enhancement of countering crime and terrorism. In accordance with the Strategy, as the legal grounds of a counterstrike following a cyberattack launched against the US by a nation state, activities conducted in cyberspace also belong to the responsibilities of sovereign nation states, comprising the international community. In accordance with the Strategy, in the case of a cyberattack launched against either the US or its allies the US may take any necessary diplomatic, economic, and military measures. On the basis of the Strategy, the US may respond to a cyberattack with a traditional military strike as well. [21]

The role of the NSA must also be mentioned in connection with American cyber activities. This organisation functions in subordination to the Department of Defence and was established primarily for signals intelligence on 4th November 1952. Its scope covers foreign signals intelligence, cryptography – that is deciphering foreign codes and the protection of the security of American codes – and all types of electronic intelligence. [22]

The NSA was one of the protagonists of Operation ECHELON, which was launched as early as the Cold War but continued afterwards for decades, involving the United States, Great Britain, Australia, Canada, and New Zealand. Its main field of activities was the control of data traffic of telecommunication satellites. This close cooperation of the five countries (or the Big Five, as special literature labelled them) still exists. Former contract worker of the NSA Edward

[9] United States Cyber Command

Snowden disclosed a number of documents which shed some light on the magnitude of the global listening activities of the NSA. The publicised materials generated a tremendous uproar all over the World.

It was disclosed that more than one billion people's telephone and internet communication is tracked by the NSA, collecting information not only about terrorism but foreign policy, economy, particular trade issues as well. In mid-2012 the Agency recorded more than 20 billion communication events – so called metadata (internet and telephone) – every day.

The NSA conducted large-scale espionage against the European Union, the United Nations Organisation, and a large number of governments which are otherwise close allies of the United States. In order to illustrate the capabilities of the organisation it needs mentioning that it has access to the servers of major on-line service providers, is capable of switching on the cameras and microphones of remote mobile telephones, tapping the traffic of undersea cables, and listening to remote Wi-Fi traffic. One of the most important units of the Organisation is TAO[10], whose members are well trained hackers. They are tasked with the identification and monitoring of computer networks operated by foreign organisations, with hacking into them and gathering information from them. TAO cooperates with other intelligence organisations, such as the FBI and the CIA, and even assists them if necessary. They even deliver hackers to particular sites in order to allow them to have access to local networks or non-internet-based networks. [23]

Therefore, as it can be seen, the United States is declaredly capable of conducting offensive operations in cyberspace.

After the tremendous development phase of the past decades, China grew into the second largest economy of the World. Although the economic crisis of 2008 did not leave it unaffected, the growth of the Chinese economy did not stall. Naturally, the development of military capabilities is also constant. In 2016 defence spending grew faster than the GDP, as the increase was 7.6%, which is equal to USD 135bn. Computer network operations capabilities are also in the phase of permanent development. China regards the internet as a potential tool of war, and stimulates the training and equipping of experts and hackers, in order to penetrate adversary information networks. University courses are organised which are aimed at the preparation for launching and fending off attacks, at studying hackers' methods, designing and applying computer viruses, and the problems of network security. [24]

Reports made by leading network security companies of the World indicate that most of the IT attacks may be tracked back to Chinese perpetrators. Several reports mention Shanghai-based military unit 61398, whose activities were classified as state secret by the Chinese government. The unit's Headquarters is in Pudong, the financial centre of Shanghai, and it may have several thousand personnel, who speak very good English and possess excellent IT skills and knowledge. According to reports they have stolen hundreds of terabytes of data from the computers of 141 organisations since 2006. [25, p3] Of course, the Chinese defence ministry categorically denied any involvement of Beijing in any type of hacker activity. However, it is more than puzzling what simple hackers or criminals would have done with such an amount of data of such type.

Russia is the third great player in cyberspace and it also claims not to have a cyber army. Nevertheless, it was Russia, which was suspect number one of the Estonian incident and of the attacks against Georgia. According to certain experts, the basis of Russia's cyber-operations capabilities is comprised by cyber-criminal groups. Such groups conduct their activities with the tacit permission of the Russian government and get their incomes through classic cyber-crime. Their capabilities are used – if necessary – against targets designated by the Russian

[10] Tailored Access Operations.

leadership. According to experts Russian cyber-capabilities are based on botnets[11], and apart from that Russian hackers have leading role in hacking computer programs as well. The best-known Russian group of cyber-criminals is the Russian Business Network (RBN), whose botnets were also involved in the DDoS attacks launched against Estonia in 2007. According to some sources personal connections can be detected among the leaders of the RBN, those of Russian state administration, and of secret services. [26] According to computer security experts, the Russian secret services participating in cyber-operations – primarily the Federal Security Service and the Federal Protective Service – cover up their information operations activities with establishing phantom firms or imitating the operations of the RBN and other cyber-criminal groups.

Russia – similarly to China – regularly attacks the computer systems of the United States and other NATO member states. However, due to the nature of botnets it is impossible to prove that such activities are orchestrated by the Russian government. [27] Social networks are also frequently used for propaganda purposes. According to the accounts of two former workers of a Sankt Petersburg-headquartered company, hundreds of commenters working in shifts do their jobs in strictly regulated frameworks in order to share anti-western, pro-Kremlin news in domestic and foreign portals. The topics are identified in the beginning of every working day and a specific number of comments must be posted under certain profiles. However, conducting such activity is typical not only for Russia as other countries also use social networks for spreading propaganda. In Great Britain a unit, Brigade 77, was established within the army, and was tasked with conducting psychological operations in social networks. [28]

Smaller states also develop their cyber-capabilities. Iran, for example, began to develop its military unit within the structure of the Revolutionary Guard after the cyberattacks in 2010. Merely one year later the unit successfully seized the control of an American unmanned aerial stealth vehicle – RQ-170 – and landed it unharmed. [29]

North Korea also established its cyber warfare unit, squad 121, within the intelligence service. According to experts, the strength of the unit has grown to 6,000 personnel and several hundred of them work abroad. Their primary target is South Korea but this unit is held responsible also for the attack against Sony in 2014, which was allegedly motivated by a revenge for film "The Interview". [30]

Israel should also be mentioned as it has always been a pioneer in electronic development programs – it was the Israeli forces, for example, that used frequency hopping radios first time – and currently it has 10 percent of the World's cyber security market, experts say. Besides the United States, Israel also took part in the development and deployment of Stuxnet against the Iranian Uranium enrichment facilities, although officially such an action has never been admitted. In early 2016 the establishment of a technological park in Beér-Seva was declared; its purpose is to found a cyber-security centre there with the involvement of private companies. According to the plans 15,000 people will work on IT-security there. The cyber-defence units of the armed forces will also be transferred there and the cyber warfare unit of the army – currently being in a nascent state – will also be located there. [31]

In Germany CIR[12], which will be the cyber warfare unit of the German military in subordination to the Bundeswehr, was established in 2017. The Bonn-headquartered Command had 260 personnel in the beginning but in accordance with the plans the number of military and civil employees will have grown to 13,500 by 2021. According to General Ludwig Leinhos

[11] A large number of computers infected with malware and controlled through a central computer. They are typically used for DDoS attacks.
[12] Cyber- und Informationsraum.

there was no time to waste after the series of computer attacks, and the unit had to be established. [32]

In my opinion, apart from the above mentioned countries there are a lot of other states trying to develop their cyberattack capabilities. By now every involved party has realised the high significance of cyber defence. Several countries – including Hungary – established that legal background which supports the organisation of the defence. Most NATO member states have already elaborated their cyber-security strategies and shared them with each other. The strategies are public and may be accessed on the home page of the Cyber Centre of Excellence, together with similar documents of other, non-NATO countries. Among others the national cyber-security materials of Russia, China, Japan, Saudi Arabia, New Zealand, and South Africa may also be found there. However, international cooperation is indispensable as this is the only way of suppressing cyber-crime and cyber-terrorism. In this spirit two highly significant bilateral agreements have recently been signed, one between Russia and China and the other between the United States and China.

The agreement between Russia and China was signed on 8th May 2015, expressing the resolute intent of the signatory parties to prevent unlawful activities in cyberspace, and the necessity of joint efforts in order to take actions against any types of cyber-crime and terrorism. A consensus was also achieved on not attacking each other's systems and not providing any support to such intentions. The two countries will regularly inform each other on cyber threats and launch joint scientific and educational projects in the field of research and development.

After the signing of the agreement some analysts had concerns about the opportunity that the two signatory states wanted to coordinate their cyber activities targeting the United States. Hopefully, this agreement is not about this. The fact that on 25th September 2015 US President Barack Obama and the President of China Xi Jinping also signed a bilateral agreement in the White House on the acceleration of information flow and provision of assistance in the case of malicious attacks underpins this opinion. The parties will not conduct or support deliberate cyberspace actions aimed at the stealth of intellectual property with the purpose to obtain business secrets or other confidential information appropriate for gaining business advantages, and they will improve their cooperation in countering cyber-crime.

Another example of the bilateral cooperation is the agreement signed by Canada and China in June 2017. In it the two countries agree on not committing state-sponsored cyberattacks for obtaining business secrets or any other confidential business information from the other. [33]

CONCLUSIONS

In conclusion it can be stated that the rapid development of technologies made the issue of cyber security a top priority. By now this fact has been recognised by every country and measures have also been made in this field. International cooperation is paramount for the containment of cyber-crimes and terrorism. IT systems appear to have increasingly encompassed not just everyday life but also military forces. Military Command and Control systems (C2) and smart weapon systems will all work on network basis which will expose them to security risks. It has to be understood that in the conflicts of the years to come attacks launched against both military and civil networked electronic information management systems and critical IT system elements will play an increasingly significant role. All countries that will fail to establish capabilities in this field may be placed at a tremendous disadvantage because the establishment of cyber defence may not be sufficient in a conflict. This is why the countries in the World should be expected to spend an increasing amount of energy on the increase of their cyberattack potentials in the future.

In my opinion Hungary should also establish a unit which would be capable of executing offensive operations in cyberspace. As it is demonstrated above, other states established such

units under military command and control within the structure of their armed forces. This arrangement may ensure an optimum exploitation of cyber warfare capabilities in military operations, and their coordination with other operations. To this end such a capability should be integrated in the structure of the Hungarian Defence Forces, and a close cooperation is needed with other domestic organisations responsible for cyber defence.

FELHASZNÁLT IRODALOM

[1] Internet World Stats http://www.internetworldstats.com/stats.htm (downloaded: 12.06.2017.)

[2] HAIG Zs., VÁRHEGYI I.: *Hadviselés az információs hadszíntéren,* Zrínyi Kiadó, Budapest, 2005.

[3] HAIG Zs.: *Információ – társadalom – biztonság;* NKE Szolgáltató Kft., Budapest, 2015.

[4] FM 3-38: Cyber Electromagnetic Activities. Headquarters Department of Army, 2014. https://fas.org/irp/doddir/army/fm3-38.pdf (downloaded: 05.06.2017.)

[5] HAIG ZS., KOVÁCS L.: *Fenyegetések a cybertérből;* Nemzet és biztonság I. évfolyam, 5. szám. Budapest, 2008. pp.: 61-69

[6] NÉMETH J., HAJZER T. : *Az orosz-grúz háború néhány jellemző vonása;* http://old.biztonsagpolitika.hu/?id=16&aid=709&title=az-orosz-gruz-haboru-nehany-jellemz337-vonasa (downloaded: 16.06.2017.)

[7] Ministry of Foreign Affairs of Georgia: Cyber Attacks Disable Georgian Websites http://georgiamfa.blogspot.hu/2008/08/cyber-attacks-disable-georgian-websites.html (downloaded: 16.06.2017.)

[8] VÁMOSI G., SZEDLÁK Á. : *Az Interneten is zajlik az orosz-grúz összecsapás;* http://www.origo.hu/techbazis/internet/20080811-az-interneten-is-zajlik-az-oroszgruz-osszecsapas.html (downloaded: 20.06.2017.)

[9] LIPOVSZKI R, CHEREPANOV A. *: BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry;* https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/ (downloaded: 20.06.2017.)

[10] BERZSENYI D., SZENTGÁLI G. : *STUXNET: a virtuális háború hajnala;* http://old.biztonsagpolitika.hu/?id=16&aid=932&title=stuxnet-a-virtualis-haboru-hajnala (downloaded: 20.06.2017.)

[11] CSERHÁTI A.: *A Stuxnet vírus és az iráni atomprogram;* Nukleon IV. évfolyam 1. szám Budapest 2011. p.:85

[12] Langner R. hamburgi vírusbiztonsági szakértő blogja 2010. december 31. https://www.langner.com/2010/12/year-end-roundup / (downloaded: 20.06.2017.)

[13] Magyar Nemzet Online: *Visszafelé sült el Izrael fegyvere;* http://mno.hu/film/visszafele-sult-el-izrael-fegyvere-1329288 (downloaded: 20.06.2017.)

[14] SG.HU: *Izrael tagadja, hogy köze lenne a Duqu 2 kémprogramhoz;* https://sg.hu/cikkek/112940/izrael-tagadja-hogy-koze-lenne-a-duqu-2-kemprogramhoz (downloaded: 20.07.2017.)

[15] GIBBS, S: *Shadow Brokers threaten to unleash more hacking tools;* https://www.theguardian.com/technology/2017/may/17/hackers-shadow-brokers-threatens-issue-more-leaks-hacking-tools-ransomware (downloaded: 29.12.2017.)

[16] GÁLLFY CS.: *Petya: minden, amit tudunk a támadásról;* https://www.hwsw.hu/hirek/57452/microsoft-windows-ransomware-kriptovirus-petya.html (downloaded: 29.12.2017.)

[17] GYEBROVSZKI T.: *Stuxnet – mint az első alkalmazott kiberfegyver – a Tallini Kézikönyv szabályrendszere szempontjából;* Hadmérnök IX. évfolyam 1. szám Budapest, 2014. pp.: 164-174

[18] Warsaw Summit Communiqué; http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (downloaded: 18.07.2017.)

[19] U.S. Cyber Command; http://www.arcyber.army.mil/Pages/USCyberCommand.aspx (downloaded: 18.07.2017.)

[20] NSA: Leadership; https://www.nsa.gov/about/leadership/ (downloaded: 18.07.2017.)

[21] International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World; https://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf (downloaded: 18.07.2017.)

[22] NSA: About NSA; https://www.nsa.gov/about/faqs/about-nsa-faqs.shtm (downloaded: 18.07.2017.)

[23] GREENWALD G. *: A Snowden-ügy;* HVG Kiadó, Budapest 2014.

[24] JORDÁN GY: *A kínai katonai modernizáció;* Nemzet és biztonság IV. évfolyam 2. szám. Budapest, 2011. pp.: 32-49

[25] Mandiant : *APT1 Exposing One of China's Cyber Espionage Units;* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (downloaded: 18.07.2017.)

[26] FLOOK. K,: *Russia and the Cyber Threat;* http://www.criticalthreats.org/russia/russia-and-cyber-threat (downloaded: 24.07.2017.)

[27] NAGY V.: *The geostrategic struggle in cyberspace between the United States, China and Russia*; AARMS Vol. 11, No. 1 Budapest 2012. pp.:13-26

[28] BÁNYÁSZ P.: *A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében*; Szakmai Szemle 2016. I. szám, Budapest pp.:61-81

[29] Israeli Intelligence Report: *US Drone downed by Iran Cyber Attack* http://www.globalresearch.ca/israeli-intelligence-report-us-drone-downed-by-iran-cyber-attack/28114 (downloaded: 24.07.2017.)

[30] PARK J., PEARSON J. : *Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West;* http://www.reuters.com/article/us-cyber-northkorea-exclusive-idUSKCN18H020 (downloaded: 22.07.2017.)

[31] BERTA S.: *A Negev-sivatagban lesz Izrael kibervédelmi központja;* https://sg.hu/cikkek/117093/a-negev-sivatagba-lesz-izrael-kibervedelmi-kozpontja (downloaded: 22.07.2017.)

[32] SCHIMMECK, T.: *Militärs mit Computermaus und Laptop;* http://www.deutschlandfunk.de/das-neue-cyber-kommando-der-bundeswehr-militaers-mit.724.de.html?dram:article_id=382767 (downloaded: 24.07.2017.)

[33] CRAWLEY, K.: *China Agrees to Cease Cyber-Attacks on Canadian Private Sector;* https://www.infosecurity-magazine.com/news/china-canada-cyber-espionage/ (downloaded: 20.07.2017.)