WELCOME TO CYBERWAR

WARSAW INSTITUTE

— SPECIAL REPORT —

WIKTOR SĘDKOWSKI

2020/12/17

- Sponsored by the KGB, the world's first ever cyber operation Cuckoo's Egg took place in 1986 – as commissioned by the Soviet services. Two decades later, hacks became an inherent tool in a repertoire used by the conflicting states. While writing his famous phrase „Welcome to cyberwar" in September 2010, Ralph Langner began a brand-new era of armed conflict.

- Espionage activities are the core cyberspace tasks that many countries tend to carry out. It is not always necessary to gain physical access to devices to intercept data sent through the network.

- The U.S.-Iran cyberwar is considered the world's first known cyber conflict that broke out when the computer worm Stuxnet caused severe damage to Iran's nuclear facilities. Iran responded by taking aim at the private sector in both the United States and Washington's allied countries. On August 15, 2012, as most Saudi Aramco employees were on holidays, the computer virus Shamoon began wiping data from the company's hard drives.

- The Ukraine-Russia conflict began in February 2014. Simultaneously with the war, analysts at F-Secure came upon a new version of the BlackEnergy malware. The Ukraine-Russia war is a classic example of hybrid warfare – a military strategy blending conventional warfare and cyber operations.

- In 2017, the United States reported $6.7 billion in funding on cyberspace operations while this spending grew to $8.5 billion in the 2019 budget scheme. According to some estimates, there are as many as 3.5 million unfilled positions in the cybersecurity industry across the globe.

Introduction

In the last century, Albert Einstein refused to predict what arms the warring parties of World War III would use on a battlefield. Nonetheless, as the scientist was aware of both the potential and destructive force of nuclear weapons, he believed those used in World War IV be sticks and stones. Over half a century has passed since then yet it is still challenging to firmly state what stockpile will be mobilized in a plausible global conflict. However, we know that those areas of the battlefield that nobody took into account a couple of decades ago will occupy a vital – if not a key – role in a possible clash.

In late December 2019, the United States officially launched the United States Space Force, a new service branch of the U.S. military that just a few decades earlier had been nothing but a reverie of science-fiction novels and films. It is the newest military service that so far – and for obvious reasons – has had no opportunity to prove itself in battle. Thus, it is not fully predictable to assess what role it would serve in the future. A typical division into traditional spheres of warfare – on land, at sea, and in the air – got cyberspace as a new addition. Here, unlike in space, operations have seen efficient outcomes on many occasions while parties have been involved in large-scale operations for many years now.

Here, unlike in space, operations have seen efficient outcomes on many occasions while parties have been involved in large-scale operations for many years now.

NATO countries officially recognized cyberspace as a military operational domain at the Warsaw summit in July 2016. It was then that NATO states vowed to implement what they referred to as the Cyber Defence Pledge, considering it a vital step to boost cybersecurity of national networks and critical infrastructure. Members of the military bloc made this decision as there emerged the need for regular cyberspace operations. These have been carried out on a full scale for a couple of years, with their outcomes taking the toll on people in many countries formally not entangled in any armed conflict.

SOURCE: NATO.INT

New battlefield

In September 2010, thus six years before the NATO declaration was signed, Ralph Langner, a control system security specialist, concluded his analysis of the virus[1]– a document well known to all cybersecurity enthusiasts – with the famous words: „Welcome to cyberwar.“ The computer worm Stuxnet that Langner meant in his paper was not the first-ever case of a cyber operation, but it is certainly the most famous one, mainly due to keywords such as virus, computer, and nuclear power plant that featured all papers on that matter.

To date, researchers argue over an exact definition of cyberwar while the line between information warfare and cyber warfare remains very vague and imprecise. The thing was simple with old-fashioned disinformation activities as those carried out in some past conflicts. Distributing fake content leaflets is undeniably an element of information warfare. The same is with stealing research plans from a foreign-based facility, a classic example of information warfare. But what if the intruder uses cutting-edge tools to slip through a set of security measures in a F-22 fighter factory to pilfer technological details and gain an advantage on the battlefield? Is this still an example of information warfare? And what if while breaking into the company‘s systems, the attackers imperceptibly add modifications to the fighter software to be able to ground the jet at any moment? Can this be already labeled as

To date, researchers argue over an exact definition of cyberwar while the line between information warfare and cyber warfare remains very vague and imprecise.

1. www.langner.com/2010/09/stuxnet-logbook-sep-16-2010-1200-hours-mesz/

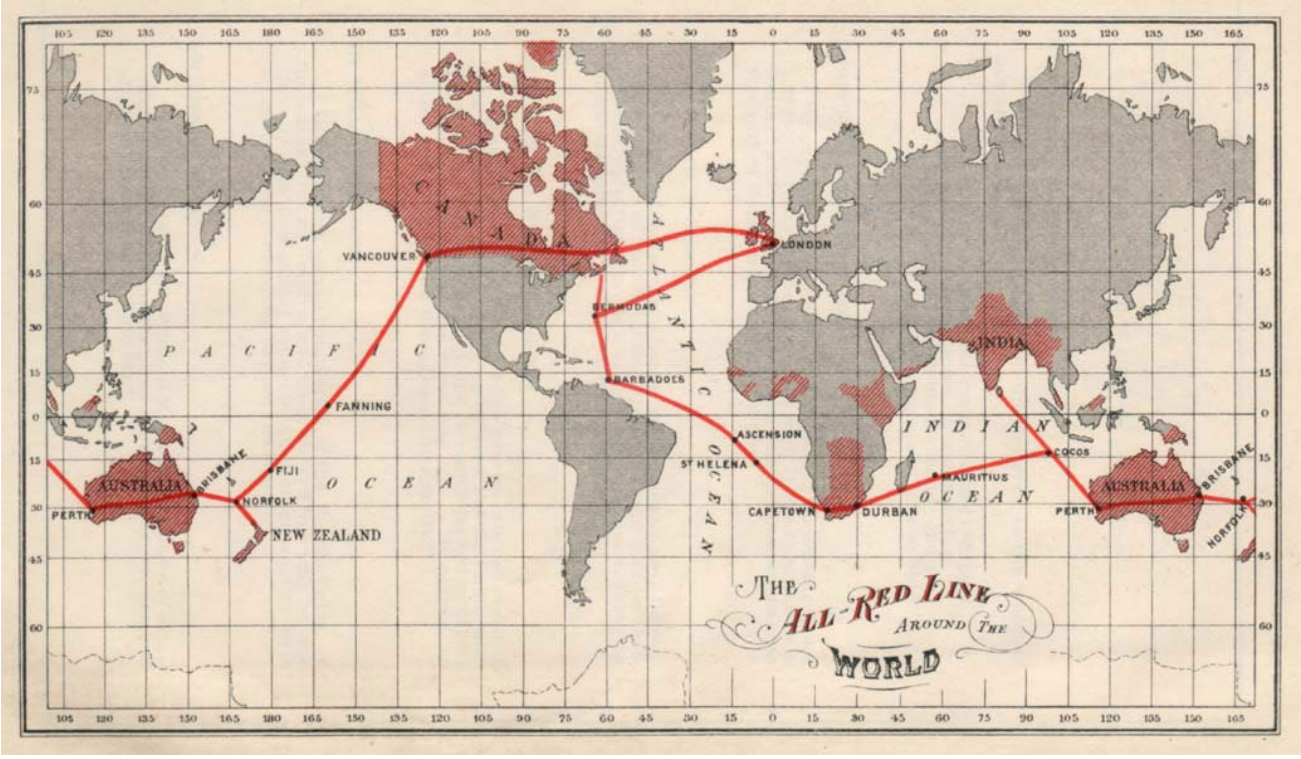
cyberwar? The boundary between these two is certainly artificial and redundant in the current world that is almost fully reliant on information systems.

Using telecommunications systems for espionage purposes has a very long history. In 1858, the first telegraph message was sent between Ireland and Newfoundland, and by 1902, telegraph systems spread across the globe. The main cable office – the heart of the communications system – was located in Porthcurno, Cornwall. The museum--turned-station for decades served as the top hub where British intelligence services collected information. In January 1917, also in the Porthcurno cable station, spies intercepted the Zimmermann telegram[2], a secret diplomatic note, the disclosure of which undeniably contributed to the U.S. Congress's decision to join World War I.

The telegraph system was not a computer system so the incident was far from being dubbed a cyber operation. It is yet worth remembering as this maneuver is still the basis for collecting data off modern telecommunications systems that have undergone major technological updates over the past century. The United States created the Advanced Research Project Agency Network, in short ARPANET, that merged a bunch of local networks into the global internet. It has been in commercial use since 1991 and is an integral part of almost everyone's life. But before this happened, it is worth taking a look on what many specialists recognized as the world's first known case of an attack on a computer system. The KGB-orchestrated Cuckoo's Egg operation began in 1986. A German hacker working in the service of Soviet intelligence services broke into U.S. government computers stealing software source code subject to export restrictions,

The KGB-orchestrated Cuckoo's Egg operation began in 1986.

SOURCE: PUBLIC DOMAIN



2. www.langner.com/2010/09/stuxnet-logbook-sep-16-2010-1200-hours-mesz/

military plans, and system passwords. By penetrating computer systems of universities, labs, and the military network MILNET, the intruder acquired access to a slew of files, including information on nuclear weapons ready to be used in case of a conflict in Europe. As later found out, the schemes were available to the public and were not secret. That who deduced that the system got hacked was Clifford Stoll, an astronomer-turned-systems manager at Lawrence Berkeley Lab. He even stalked the hacker based in West Germany. With some help from a German telecoms operator, authorities arrested the man in his Hanover apartment and brought him to trial[3]. His intrusions were based mainly on guessing passwords to computer systems. In most cases, it was possible to conduct an attack as administrators paid little attention to security issues and often did not change default passwords.

It was only a decade later that U.S. government agencies again fell victim to infiltration practices. In July 1998, the FBI opened an investigation into a suspicious activity that had been accidentally discovered in the computer network at the Wright-Patterson Air Force Base. The inquiry revealed that more institutions were targeted, including U.S. Navy research labs, Air Force Institute of Technology (AFIT), U.S. Department of Energy, and Los Alamos Base[4]. From there and elsewhere, hackers stole data inaccessible to the public. Sometime later, investigators discovered that the same group had hit institutions in the United Kingdom, Canada, Germany, and Brazil. Hackers broke into the systems while using known and sometimes publicly available exploits, or pieces of software that take advantage of systém vulnerabilities, thus yet again benefitting from the carelessness of system administrators who did not shield themselves against a threat they could easily counteract.

Home advantage

The nineteenth-century telegraph tapping continues till now. Telecommunications systems serve as an excellent source of data for intelligence services and other agencies tasked with state security. It is therefore little surprising that they seek to intercept as much data sent over the network. Enjoying the world's leading position among global tech companies, the United States undoubtedly holds an advantage over other countries in this respect. Files obtained from Edward Snowden in 2013 revealed the National Security Agency and Britain's GCHQ tapped on Google and Yahoo, two of the world's biggest tech companies. Under a project codenamed Muscular, these two intelligence agencies bugged on the cables connecting the internet giants' data centers[5]. As people around the globe use both Google and Yahoo, it is fairly easy to state that the operation sought to win what is known as „home advantage." With technological capabilities, both NSA and GCHQ intended to seize as much data as possible on what people in other countries did online. Another such example was when hackers infiltrated the United Nations video-conferencing network[6], a feat also made public in 2013. Besides, according to media reports, at least two countries could have spied on the United Nations. The espionage attack was

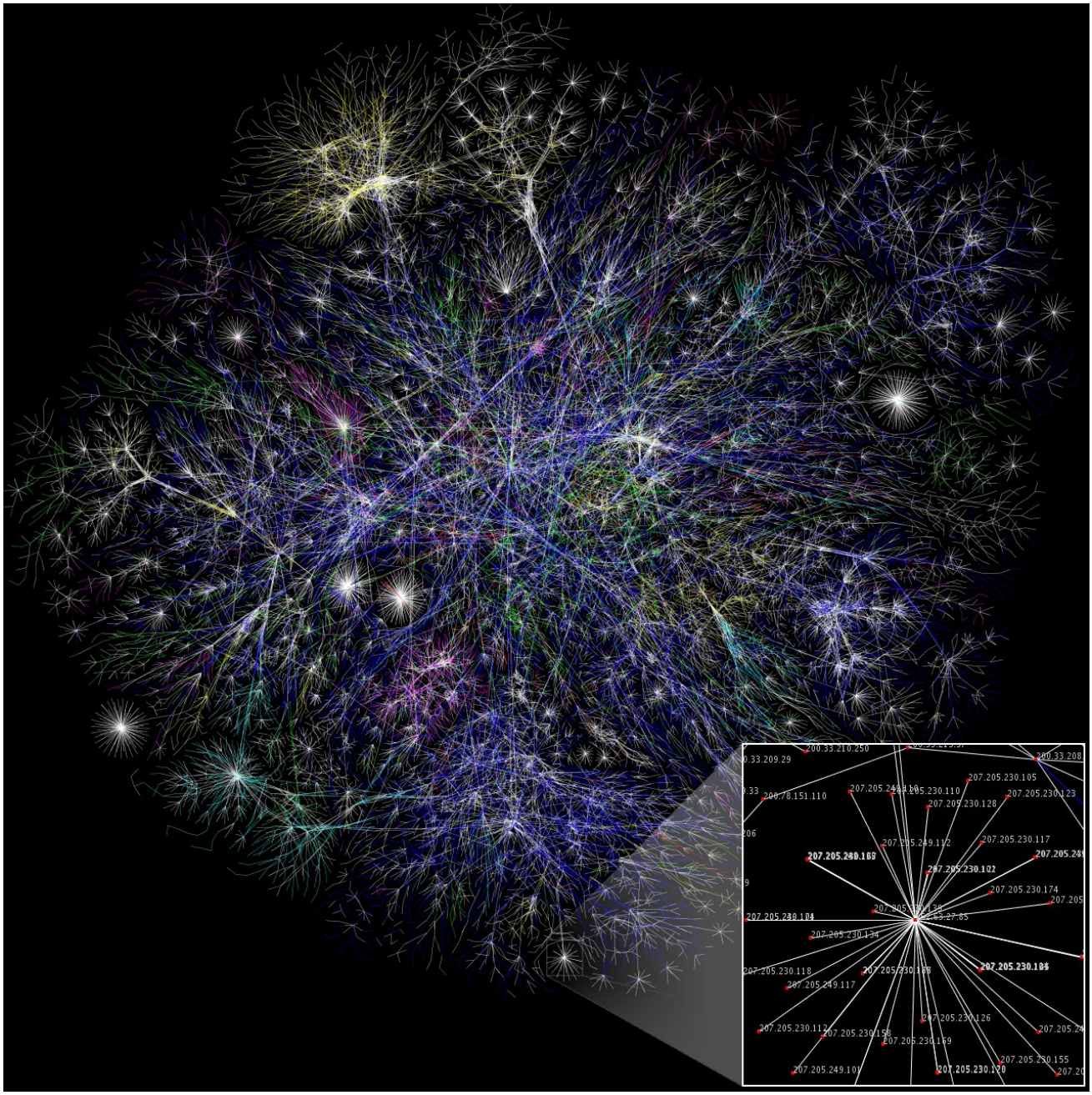
3. Stoll, C. (2005), The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.
4. PENGUIN'S MOONLIT MAZE: The Dawn of Nation-State Digital Espionage, 2017, J.G.-S., C.R., D.M., T.R.
5. www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links
6. www.latimes.com/world/worldnow/la-fg-wn-nsa-leaks-spying-un-20130826-story.html

conducted by both the Americans and Chinese hackers[7].

Sometimes intelligence services try to gain this advantage outside their country. In 2015, after a ten-year investigation, the Greek government identified an NSA operative as responsible for illegal wiretapping and compromising devices of the mobile operator Vodafone. Calls from over a hundred users – mostly government officials, including the then-prime minister of Greece – were wiretapped with illegal software performed at the switch that is normály a legal solution used by telecoms operator to monitor data transmission. This yet first needs adequate permits from dedicated government agencies[8].

It is not always necessary to gain physical access to devices to intercept data sent through the network. Border Gateway Protocol, or BGP, is

SOURCE: WIKIMEDIA COMMONS



7. www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html
8. en.wikipedia.org/wiki/Greek_wiretapping_case_2004-05

the basis for the modern internet. It routes the transfer of data between locations – those of the sender and the recipient – over the internet.

The route should be as short as possible. Nonetheless, it is possible to provoke what is known as a deliberate BGP route leak. One such example was in 2015 when China Telecom diverted internet traffic between South Korea and Canada by shunting it through its network. The same happened in 2017 when traffic was rerouted between Sweden and a branch of a U.S. news agency in Japan. The last time this took place was in June 2019 after traffic meant for European mobile networks in France, the Netherlands, and Switzerland was rerouted through China Telecom's network for more than two hours[9].

Files obtained from Edward Snowden in 2013 revealed the National Security Agency and Britain's GCHQ tapped on Google and Yahoo, two of the world's biggest tech companies.

USA vs Iran

Cyberintelligence operations are just one kind of cyber activities. A wide variety of such attacks was employed by both parties to the U.S.-Iran conflict. The most notorious case was the computer virus Stuxnet that sought to bar Iran from developing its nuclear program. Stuxnet exploited both publicly known vulnerabilities in the operating system, as well as targeted those in programmable logic controllers (PLCs), an inherent part of the systems used at Iran's Natanz nuclear facility. As a result, the computer worm ruined roughly 1,000 centrifuges at the uranium enrichment plant in a move that compromised Iran's nuclear program for over five years[10]. Those who developed the virus paid big to attain the goal, pouring at least several tens of millions of dollars into devising such a complex solution. To conduct a precise strike it was necessary to employ both programmers and specialists fluent in systems like ICS, SCADA, and Simatic PLCs. The worm must have undergone thorough trials before it hit Iran's nuclear facility thus the purchase of P1-type centrifuges used at the Natanz plant had to come from the cyberweapon budget[11].

As a result, the computer virus Stuxnet destroyed roughly 1,000 centrifuges at the uranium enrichmnent plant in a move that sabotaged Iran's nuclear program for over five years.

Iran responded by taking aim at the U.S. private sector, mainly banks, in 2012. The Distributed Denial of Service (DDoS) attack is an unsophisticated tool that made U.S.-based financial institutions unreachable for their customers. The six-month-long assault affected forty-six financial institutions such as Bank of America, JPMorgan, or NASDAQ. Although rudimentary, it caused

9. www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/
10. Zetter, K. (2015), Countdown To Zero Day
11. ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

damage that cost tens of millions of dollars. The Islamist group Izz ad-Din al-Qassam Cyber Fighters publicly claimed responsibility for the attacks, saying an anti-Muslim YouTube video was the impetus for the attack. Cybersecurity specialists yet argue that this came as a tit-for-tat response to the Stuxnet attack. It was quite a successful retaliation step especially if to consider the cost-to-damage ratio.

The Iranian-orchestrated denial of service attack hit forty-six financial institutions, including Bank of America, JPMorgan, or NASDAQ. Although rudimentary, it caused damage that cost tens of millions of dollars.

Iran received another blow in 2012. In the first three months of 2012, the Wiper malware took aim at Iran's oil production industry, irreversibly erasing data from thousands of computer and forcing Iran to disconnect key oil facilities[12]. The data wiped by the worm was lost forever and it was unknown who had created the virus. Experts at Kaspersky Lab made efforts to link the code of Wiper to that of Stuxnet yet no one officially admitted responsibility for the operation[13].

Nor is it known who was behind the Shamoon computer worm that struck a few months after the Wiper attack and crippled the activities at Saudi Aramco, the world's global leader in oil production. Much indicates this was Iran as the country had a clear reason to attack a U.S. ally[14]. The Shamoon virus attack destroyed over 30,000 computers, all key systems, and data. The situation was grave and to ensure supply continuity, the company shipped oil commodities with no financial papers submitted, thus hoping that its contractors are honest. The political reason behind the attack was absolutely clear. On August 15, 2012, some 50,000 employees were absent as they gathered on the occasion of the Laylat al-Qadr, one of the most important Muslim celebrations. As most Saudi Aramco workers were on holidays, the computer virus Shamoon began wiping data from hard drives, overwriting file data from 1024 bytes with an image of a burning American flag. The attack hit also RasGas, a Qatar-based company producing and exporting liquefied natural gas. It affected a completely different market. Seeking to restore its system operational capabilities, Saudi Aramco immediately purchased tens of thousands of hard drives from computer manufacturers, a move that once combined with flooding in Asia took its toll on both the global availability and prices of the components.

The Shamoon virus attack destroyed over 30,000 computers, all key systems, and data.

An updated version of the Shamoon computer virus emerged in 2017, roughly triggering an explosion at a Saudi refinery. Iran's increased cyberspace activity dealt a blow not only to Washington's allies, but also the United States itself. Within twenty-four hours of President Donald Trump announcing that the United States would pull out of the Iran nuclear deal (JCPOA), Iranian hackers started to send emails

12. www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html

13. www.wired.com/2012/08/wiper-possible-origins/

14. www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/

SOURCE: PEXELS / MATI MANGO

containing malware to people having links to the U.S. government and other related institutions[15]. In many cases, American officials managed to avoid cyberdanger, yet not all of them[16]. The Iranian-origin ransomware caused the disruption of service to the City of Atlanta for many days. Two Iranian computer hackers were charged in the U.S. malware scheme, with its costs estimated at $17 million. A similar incident took place in May 2019 in Baltimore and it cost $6 million in losses. Between 2017 and 2019, Iranian cyber operations targeted over 200 businesses and institutions throughout the United States, according to data from Microsoft.

U.S. forces gave as good as they got by launching cyber missions in Iran. The world will probably wait a long time before learning about them yet many reports already show some disruptions in the operations of Iran‘s critical infrastructure systems as was the case of the Natanz incident in July 2020[17]. It is worth adding that civil activists also joined the fight, siding with the United States. In 2018, hackers attacked several thousand computers throughout Iran that showed a U.S. flag on screens along with a warning: „Don‘t mess with our elections.“ The attack came from an unknown hacking group that used a vulnerability in routers[18], issuing the notice in Iran and China where it affected thousands of devices.

15. https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html
16. www.businessinsider.com/cyberattacks-on-american-cities-responses-2020-1
17. www.forbes.com/sites/kateoflahertyuk/2020/07/03/iran-nuclear-facility-explosion-accident-sabotage-or-cyber-attack/
18. www.reuters.com/article/US-iran-cyber-hackers/iran-hit-by-global-cyber-attack-that-left-us-flag-on-screens-idUSKBN1HE0MH

Hybrid warfare

Cyber skirmishes involving the United States, China, North Korea, and Iran are in most cases limited to cyberspace. Of course, each of these attacks brings political consequences and to some extent affects the economy and social moods in the targeted country. But what poses the biggest threats are hybrid attacks. This is what Russian neighbors experienced first-hand.

The Russian-suspected denial of service cyberattack on Estonia in 2007 was the first known cyberattack on an entire country[19]. It indeed froze all the country's major telecoms systems, making them practically unreachable in the campaign lasting a total of 22 days, yet the conflict was over after that and everything came back to normal.

Georgia was less fortunate, though. In 2008, „the attacks were significant in that it was the first time that there had been a coordinated cyber component to an international armed conflict. however, despite the obvious links to the ongoing conflict, there is only circumstantial evidence that the Russian Federation was in any way involved in the attacks[20]." On August 8, Russian troops crossed the Russian-Georgian border. Denial of service cyber attacks against Georgian telecoms systems began simultaneously with the invasion, bringing memories of the Estonian cyberattack. In the aftermath of the hack, the Georgian government was barely able to communicate with citizens and the military on the internet. As residents of Tbilisi were cut off from information access, this sparked panic in the Georgian capital especially after a disinformation campaign claiming that the Russian military had rolled into the city. Analysts agree that command-and-control, or C&C, servers that coordinated the denial of service attack were based in Russia. At least a part of infrastructure belonged to cyber contractors who kept in touch through Russian hacking forums.

Four days after Russian servicemen marched through the Georgian frontier, the then Russian President Dmitry Medvedev said the Russian military operation had attained its goals. On August 15, both countries inked a peace deal ending the five-day hybrid war.

It was only during the Russian-Ukrainian conflict that the real force of cyber operations performed under hybrid warfare measures could materialize. In Ukraine, hacking groups like Fancy Bear[21], Cozy Bear and Sandworm – the last of which stood behind NotPetya, the most devastating cyberattack in history – and hackers of both governmental and non-governmental organizations unveiled their operational capabilities while compromising Ukraine's national systems and networks.

The Ukraine-Russia conflict began in February 2014. Simultaneously with the war, analysts at F-Secure discovered a new version of the BlackEnergy malware. Before, the BlackEnergy malware family had served many purposes throughout its history, including DDoS attacks, spam distribution, and bank fraud. Its modified version allowed the use of plugins that boosted software capabilities. It was immediately used to hit many

The Russian-suspected denial of service cyberattack on Estonia in 2007 was the first known cyberattack on an entire country.

19. warsawinstitute.org/russia-strengthened-natos-cyber-defence/

20. Dinniss, H. (2013), Participants in Conflict: Cyber Warriors, Patriotic Hackers and the Laws of War „

21. www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

SOURCE: PEXELS/TIMA MIROSHNICHENKO

targets in Poland and Ukraine[22]. BlackEnergy Trojan was employed as a backdoor to deliver a destructive KillDisk component in attacks against Ukrainian news media and the electricity industry. On December 23, 2015, regional power grids went down in a coordinated cyberattack. Ukrainian power companies experienced power outages impacting a large number of customers in Ukraine. Over fifty power stations were unplugged as a result of the attack. A year later, just two days before Christmas, Russian hackers struck again. As they hacked on the infrastructure of Ukraine's national power company, the lights went out in Kyiv, the country's capital. Power operators could restore power after no longer than an hour. They were very lucky. As it turned out a few years after the incident, the malware used in the attack bore similar traits to those of the computer worm Stuxnet. It could target components of the industrial control system (ICS) by irreversibly damaging physical devices and provoking a mass-scale failure. Specialists say this might have taken whole weeks or even months for the systems to recover after a failure that fortunately did not take place. It is unclear whether the operation failed or the attacker just spared Ukrainian systems yet making it clear it could destroy it at any moment at its will[23]. Another example of using cyberweapons in the conflict was devising the hostile software that targeted Android smartphones. The Russian group Fancy Bear developed the malicious application that tracked the location of users of infected devices[24]. The Попр-Д30.apk malware could gain access to contacts, text

It was only during the Russian-Ukrainian conflict that the real force of cyber operations performed under hybrid warfare measures could materialize.

22. www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

23. Greenberg, A. (2019), Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

24. www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

WHO'S WHO IN RUSSIAN CYBER ESPIONAGE?

CYBER CRIMINALS AND HACKTIVISTS

FSO

Federal Protective Service of the Russian Federation

SPETSSVJAZ

The FSO's Spetssvyaz sub-unit organizes national government and military communications and ensures the security of the data transmitted along these channels.

FSB

Federal Security Service of the Russian Federation

16th CENTRE

18th CENTRE

The 16th Centre is the FSBs's main signals and cyber intelligence unit. The cyber operations of the FSB's 18th Centre may have targets outside state borders.

SVR

Foreign Intelligence Service of the Russian Federation

In the cyber sphere, the SVR's activity level and capabilities are not comparable to the other Russian special services, but the SVR is engaged in developing its cyber capability.

GRU

Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation

6th DIRECTORATE

From the Russian territory, the GRU actively carries out signals and cyber intelligence around the world, possessing the best technological capability among all Russian special services.

TURLA
Snake/Uroburos

APT29
The Dukes/Cozy Bear

APT28
Sofacy/Fancy Bear

APT – or ***Advanced Persistent Threat*** – carefully targeted, long term cyber operations in the course of which attackers combine multiple techniques to obtain the needed information about the target.

SOURCE: INTERNATIONAL SECURITY AND ESTONIA 2018, ESTONIAN FOREIGN INTELLIGENCE SERVICE

messages, call logs, and device location. Many sources blamed it for Russian hits on Ukrainian artillery positions. The malware was allegedly used to monitor positions of the battalions from Ukraine's 24th and 72nd Mechanized Brigades. Analysts at Crowdstrike found evidence that the application probably could not have provided all the necessary data. This was possibly an unmanned aerial vehicle (UAV) that had been used in the area prior to an attack.

Cyber defense

It is possible to prevent cyberattacks, even those most sophisticated. In recent years, a number of companies and governments have poured huge amounts of money into security systems. This should barely come as a surprise as back in 2019 analysts at the Cyber Defense Magazine predicted cybercrime damages would cost the world $6 trillion in 2020[25]. Today we know they were wrong while making their estimates, with the costs being higher than that.

Many countries start to spend more and more on cyberspace forces every year. In 2017, the United States spent $6.7 billion on cyberspace operations while this spending grew to $8.5 billion in the 2019 budget scheme. For the sake of comparison, in 2019, the total budget of Poland's Ministry of National Defense amounted to less than PLN 45 billion ($12 billion). Commands of all armies across the globe have notched the need to educate their personnel in this respect. Military training takes place at each level as confirmed by the fact that in its 2020 budget, Poland's defense ministry allocated roughly PLN 3.5 million ($1 million) for its CYBER.MIL z Klasą [CYBER.MIL with Style] scheme. The program aims to prepare candidates to work in state institutions and the Cyber Defence Forces by passing some knowledge in areas like cryptography, information security management, and other cybersecurity-related domains[26].

Money is not the only problem. Many institutions began to form professional IT security groups and crisis management teams. Unfortunately, human resources in this domain are scarce, both in Poland and elsewhere. According to some estimates, there are as many as 3.5 million unfilled positions in the cybersecurity industry across the globe.

Undeniably, with the increase in digitalization schemes and technological progress in the coming years, cyberspace will grow in importance for individuals, societies, states, and businesses. However, it has not been fully formalized yet in defense studies amid its vaguely defined boundaries. Nonetheless, efforts to secure national critical infrastructure and shield people against cyberthreats should be the same priority as protecting boundaries on land, at the sea, and in the air. As the example of Iran shows, there are new rules on the power projection skills on a relatively new battlefield while actors that had no chance

In 2017, the United States spent $6.7 billion on cyberspace operations while this spending grew to $8.5 billion in the 2019 budget scheme.

25. cybersecurityventures.com/cybersecurity-market-report/

26. www.rp.pl/Sluzby-mundurowe/301069964-MON-tworzy-zaplecze-dla-Wojsk-Obrony-Cyberprzestrzeni.html

to win in a conventional clash with a far stronger and wealthier opponent might cause severe damage in cyberattacks. But the fact remains that the world's biggest powers won a major advantage in this respect long ago. Over time, this type of warfare may become dominant and have the greatest impact on the global balance of power. Officials – also in the domain of security – are becoming more and more aware of this, but due to vacancies in the cybersecurity industry and the very nature of cyberspace, states will be able to control it just halfway for long time.

Nonetheless, efforts to secure national critical infrastructure and shield people against cyberthreats should be the same priority as protecting boundaries on land, at the sea, and in the air.

Author: Wiktor Sędkowski
Wiktor Sędkowski graduated in Teleinformatics at the Wrocław University of Science and Technology in the field of cybersecurity. He specializes in cyber threats. A CISSP, OSCP, and MCTS certificates holder. He worked as an engineer and solution architect for leading IT companies.

© COPYRIGHT 2020 Warsaw Institute

The opinions given and the positions held in materials in the Special Report solely reflect the views of authors.

Warsaw Institute
Wilcza St. 9, 00-538 Warsaw, Poland
+48 22 417 63 15
office@warsawinstitute.org