Pulaski Policy Papers
Komentarz Międzynarodowy Pułaskiego
ISSN 2080-8852 Warsaw, 17.08.2022

Author: A. Kozłowski

Russia-Ukraine war in cyberspace

> *Along with the experts predictions the first fires were shot in cyberspace. However, the CyberPearl Harbor did not happen and Russian operations in cyberspace did not paralyse Ukrainian defenders despite many attempts.*
>
> “

The Russo-Ukrainian war, which started on 24 February has been the most significant armed conflict in Europe since the II World War. Alongside the traditional fight with artillery, tanks and ground troops' fighting, it is also the first time when a cyber component is used on the wider scale by both sides. Many theoretical works have been published predicting how the war in cyberspace may look like but the war in Ukraine delivers actual answers to some questions bothering the experts and also brings important lessons for Poland.

The myth of Cyber Pearl Harbor

The term of cyber Pearl Harbor or 9/11 reappeared many times in studies over a war in cyberspace repeated by experts, politicians and journalists. It means a devastating, surprising cyberattack, which would cripple the IT systems, critical infrastructure and other vital elements of a country paralysing it and making vulnerable to next adversary actions. Such a thing did not happen in Ukraine. There was not a cyberattack which destroyed or significantly damaged the Ukrainian infrastructure or even came closely to a scale of destruction from NotPetya attacks from 2017.[1]

Every modern war starts with cyberattacks

The theorists and experts believe that a modern war will start with the cyberattacks or rather the first fires will be shot in cyberspace. The war in Ukraine confirmed it. Hours before the conventional Russian invasion the American company Viasat was attacked by denial of service attack by Russian Military Intelligence GRU and it disrupted broadband service to tens of thousands of users in Ukraine and through Europe. However, it was not the only Russian cyberattack before the war. Russia groups of hackers deployed also Fox Blade wiper to 19 systems in Ukrainian government and critical infrastructure, however it did not cause significant damage. There were also DDoS attacks a few days before the invasion but also they did not significantly harm Ukraine administration.

Cyber component was incorporated in other kinetic operations and used accordingly Russian doctrine

Conceptual View of the Armed Forces of the Russian Federation's Action in Information Space tends to use cyberattacks as a part of information warfare, which is intended to win confrontation in the information space by causing damage to critical information systems and undermining political, economic and social systems of a hostile state in order to bring its destabilisation. The operations are aimed at degrading troop morale, discrediting the leadership and undermining potential of the adversary. This conception was introduced in practice during the war in Ukraine. 40% of the Russian destructive attacks were aimed at organisations acting in infrastructure sectors and could have effects on the government, Armed Forces, economy and society. The media, which also are a crucial element in information sphere were attacked many times to disable communication between government and society. The first cyberattack, which followed the war, aimed at satellite of ViaSat companies was also intended to cut off Ukraine from communication. So the cyberattacks were clearly conducted according to the doctrine. Some Russian military officials believed that information means can be more effective than traditional weapons, however the war in Ukraine contradicted this thesis.

Russian cyberoperations were well coordinated with the military operations and there are many examples of such coordination. At the beginning of the war on February 28 threat actor compromised Kyiv-based media company. One day later the missile stroke Kyiv TV tower as later at the same day other Ukrainian media company faced destructive attacks and data exfiltration. The cyberattacks also followed the occupation of nuclear power company at the beginning of March or stroke against Vinnitsa airport, which happened after Russian hacking group targeted government network in Vinnitsa. A similar situation also happened in Dnipro and Odessa. Also the Lviv's railway substations were hit after the hackers conducted reconnaissance against transportation network sector in this city. These examples show that Russian hackers presumably gained information about potential targets and one can assume that it was transferred to military units planning the attacks.

Russian cyberattacks also confirm that the whole operation was expected to be relatively short and that Russians really believed that Kiev would be seized in days and President Zelensky brought down. Russians massively and on unique high operation tempo developed and deployed cyber capabilities burning them in the same time. The scope of Russian cyber arsenal is unknown, but such an unpreceded tempo of using visible malware may in long term weaken the Russian cyber operations and make them less advanced and destructive.

IT volunteers amassing in one big cyber army

The war which was condemned by Western powers caused the rise of voluntary movement in cyberspace, which wanted to punish Russia for unjustified aggression. Hackers from all around the world joined together under the auspices of Anonymous group conducted various cyberattacks against Russia and Belarus. Most of them were Distributed denial of service DDoS attacks against the websites of Kremlin administration and leakages of database, which were not very harmful and could not influence the battlefield. Although in some cases hackers breached the Kremlin infosphere and were able to show the true image of war for ordinary Russian citizens, these actions were too limited and too short to alter the Russian society approach to war. With the prolonging war, the intensity of cyberattacks conducted by hackers from Anonymous also decreased.

Nevertheless, there was also an important role of Belarusian Cyber Partisans, who were able to disrupt Belarusian trains infrastructure and probably impede logistics of Russian forces advancing on Kiev direction. The volunteer hackers from all around world were also used by Ukrainians, who set up a IT Army of Ukraine at the beginning of the invasion (due to the lack of military cyber command and the experience in conducting offensive cyber operations they were employed to attack Russia entities in cyberspace). The war in Ukraine shows that cyber clashes engaged a significant number of people from various countries, however, the Ukrainian cyber counter-attacks do not develop in any meaningful success.

The Russia as the cyber super power

Russia has been perceived as top-tier power in cyberspace almost on the same level with China and the United States, but it seems that the war in Ukraine challenged this assumption. The cyber fire did not generate spectacular breakthrough on battlefields, however maybe cyber capabilities have never been aimed at doing it. It is a perfect force multiplier allowing or facilitating the conventional forces to reach out mission objectives. But the significant defeat of the Russian forces in the first weeks of war would cause that even successful cyber operations would be treated as the defeat as the Russia main mission aims were not achieved. Secondly, Russia had to face the coalition of the most advanced technologically countries and IT giants providing support for Ukraine. However, despite the potential failure in Ukraine Russia has not employed all the capabilities and still existing risks should not be neglected, especially in Western countries (as these capabilities are a reliable and effective tool in grey-zone area and they will not cause the significant response from NATO, it may be tempting to use them).

You can prepare to a war in cyberspace

The popular opinion claims that attackers have a massive advantage over defenders and defenders could not successfully prepare. However, Ukraine showed that they could. Despite some successes of Russian cyber operations, Ukrainian infrastructure has not been crippled with cyberattacks, the communication and internet infrastructure was maintained and many of Russian malware were detected before they caused significant damages thanks to the unparalleled cooperation with private industry, especially US IT companies (e.g. Microsoft detected Whisper gate before it caused serious damage and therefore burned these Russian cyber capabilities before they were used). The Ukrainian cyber defence was significantly levelled up also by the assistance from the United States and NATO allies. The US Cybercommand sent to Ukraine the defence forward team and later during the war supported Ukraine with all types of operations, what was confirmed by general Paul Nakasone the head of US Cybercommand and NSA.

Look from Poland

Poland as a neighbouring country of all sides of war: Russia, Belarus and Ukraine is affected on many layers by the war in Ukraine. One of them has been Russian attempts to infiltrate systems and networks. Head of Polish Cyberspace Defense Forces general Karol Molenda said that the number of attacks from Russian ATP against military IT systems and networks was 4 time bigger in first quarter of 2021 than in the whole 2021 year. His remarks are confirmed by Microsoft report, which detected Russian network intrusion on 128 targets in 42 countries. Poland is on top of the list with 8% of intrusions. However, Microsoft has not revealed more details about the institutions, which were targeted and the scope of their success.

In order to prevent intrusions and strengthen Polish IT networks and systems from rising hostile Russian activity Poland introduced the 3th Charlie CRP[2] alarms just before the war outbreak. Since February 24th there have not been major incidents noticed in cyberspace by Polish authorities. The Russian group Kill net, which has declared war on Poland, conducted DDoS attacks on Polish police website, but with the minor effects. The most serious incident concerned delays of Polish trains, which paralysed this means of transport for almost whole day. Despite the initial suspicions, it was caused by malfunction of key systems not a cyberattack. However, this error shows the possible effects of cyberattack on critical component as the train system is, particularly in the crisis situation. Maintaining 3th Charlie CRP seems to be effective and should be continued. Especially that other countries such as Lithuania and Latvia face the growing Russian hackers activity.

Conclusion

1. Along with the experts predictions the first fires were shot in cyberspace. However, the CyberPearl Harbor did not happen and Russian operations in cyberspace did not paralyse Ukrainian defenders despite many attempts.

2. Russia showed the good coordination between cyber and conventional components, where many targets were first reconnoitered by hackers and later stroke by conventional attacks. Russian cyber component was also prepared for a short and decisive operation confirming that it was well integrated with military plans.

3. The war in Ukraine shows that cyberwar will not replace the traditional forms of combat in the foreseeable future.

4. The first months of war also confirmed that countries may prepare for the cyber war and also show the importance of close cooperation between private and public sector and international support.

5. The strategies and tactics during the war in Ukraine should be studied further as it may be repeated by Russia against other countries, but also other actors like China, Iran or North Korea that may learn from Russian failures and use them more effectively in other armed conflicts.

6. Poland should take into account the experiences from the war in Ukraine in building own cyber components. This branch of armed forces is important on the 21st battlefield but they

will not replace kinetic, traditional forces such as artilleries, tanks or military jets. The claims that instead of building air and ground capabilities army should invest in cyber should be reconsider.

7. Polish cyber forces should develop cooperation with Ukrainian counterparts to learn about methods, techniques and malware used by the Russian aggressors.

8. Poland should maintain the Charlie CRP alarm for the next months, until the situation will improve and the risk of Russian cyberattack will decrease. Poland has not suffered yet the serious cyberattack, but with rising tensions between the West and Russia, such a scenario could not be excluded.

Author: Dr Andrzej Kozłowski, Head of Research Office, Head of Research of the Casimir Pulaski Foundation

The Paper was prepared in cooperation with International Centre for Ukrainian Victory

[1] Not Petya was a wiper malware, which looked like the ransomware and attacked multiple systems in Ukraine causing the temporary paralysis of metro, airports, banks and other critical objects. It later spilt over to other countries inflicting serious damage for both private and public sector.

[2] This alert is introduced when events suggest a probable subject of an attack targeting public security, the security of Poland, or the security of another country, creating a potential threat to Poland,". CHARLIE can also be introduced when there is credible and confirmed information about a planned event of a terrorist nature.

The Casimir Pulaski Foundation is an independent Polish-think tank specialising in foreign policy and international security in the Transatlantic space.

The Foundation publishes analysis describing and explaining international events, identifying trends in the international environment and recommending solutions for government decision-makers and the private sector.

The Casimir Pulaski Foundation brings together dozens of experts in various fields and publishes reports and commentaries on current events recommending implementable solutions for the future.

The Casimir Pulaski Foundation is the initiator and main organiser of the annual Warsaw Security Forum conference, which has become a permanent feature of the European landscape of conferences devoted to transatlantic cooperation and focusing on elaborating shared responses to common transatlantic security challenges. Organised since 2014, the Warsaw Security Forum is a platform for the exchange of views between the highest representatives of governments, international institutions, industry, think tanks and experts in the field of politics and defence.

Each year the Foundation presents the "Knight of Freedom" award to outstanding figures who contribute to the promotion of the values of General Kazimierz Pulaski, i.e. freedom, justice and democracy. It is also the home to the Women in International Security Poland network.

The Casimir Pulaski Foundation ranks first among Polish Think Tanks dealing with defence and national security according to the 'Global Go To Think Tank Index' report in 2018, 2019 and 2020.

The Foundation also has the status of a partner organization of the Council of Europe.

www.pulaski.pl