Cyberwatch Finland

WEEKLY REVIEW

THEME REVIEW:
TWO YEARS OF WAR IN UKRAINE

"CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS"

Cyberwatch Finland

KEY TAKEAWAYS

1. Perceptions of the role of cyber operations have varied during the war in Ukraine. It seems that the pre-war perception of the destructive power of cyber weapons has been exaggerated. However, when used correctly, it has a role to play in intelligence, information influencing and disrupting critical infrastructure.

2. Ukraine seems to have won the information war in the West – but only there. The challenge is to turn victory into tangible help and achievements on the battlefield.

3. It is challenging to assess how the cyber lessons of the war in Ukraine will affect future conflicts. Cyber expertise does not necessarily win wars, but its absence can contribute to defeat.

Cyberwatch Finland

1. TWO YEARS OF CYBER WAR

The cyber environment as one of the fields of warfare is the phenomenon of modern conflict concretized by the war in Ukraine, which previously could only be discussed in the form of theories or guesses. Cyber struggle between states, or even cyber war, is nothing new per se, but the war in Ukraine is the first in which the fighting in the cyber environment coincides with a physical conflict and a state of war between the parties. Particular interest in cyber operations is how warring parties have tried, succeeded and failed to leverage their cyber capabilities to achieve broader strategic objectives and combine them with conventional warfare and broader hybrid warfare.

Before the start of the conflict – almost exactly two years ago – there were many estimates of how and where cyber operations would play a role. In particular, there was a lot of talk about Russia's superior capabilities. The expectation seemed to be that Russia, with its advantage, would bring Ukraine to its knees with its cyber power by crippling critical infrastructure nodes and disrupting the communications network. The war began with a massive wave of cyberattacks, but contrary to what had been anticipated, these failed to achieve a significant, or at least a long-lasting, impact on Ukraine's ability to wage physical war. After the first few months, there was widespread speculation as to why this had not happened. Was it Russia's failure, Ukraine's surprising ability to protect itself and recover from attacks, or something else entirely?

A lot of reasons were found. The most significant of these have been considered to be the support provided by foreign countries, especially the United States, and the relocation of critical data centers outside missile range or outside the country. During the first year of the war also idea that the most powerful weapons are being kept in reserve for future exploitation, and thus not yet been used and was very popular and used to reason why there have been no cyberattacks with a significant impact. After all, cyber weapons are disposable in the sense that once a weapon has been fired, it is much easier to protect against it in the future when its operation method (i.e. typically very advanced malware) is known. For this reason, it was thought that Russia, which supposedly possessed these weapons, had not yet found it necessary or useful enough to use them. The assumption was that weapons would be kept in reserve until the damage they could achieve was maximum. This moment was thought to be the first winter of the war, when Ukraine's supply security would be stretched to the limit, and the war that has been going on for a long time has exhausted energy and raw material reserves. However, winter came and went without a massive-impact cyberattacks from Russia. Of course, smaller-scale cyberattacks continued to occur on both sides, but neither side was able to achieve a devastating or long-lasting impact.

Gradually, the perception began to change to the fact that the cyber weapons prepared before the war and the gained foothold in the opposing parties' networks had actually been used, or that these weapons had been identified in advance and protections against them were put in place. As a result, the talk turned from successes or failures in carrying out operations to the idea of whether cyber operations could after all be used effectively in war. Although it seems clear from current understanding that the conflict in Ukraine, or probably any other ongoing or near-future war, will not be resolved in cyberspace, what is happening on this battlefield should not be downplayed when looking at the conflict as a whole. Cyber operations have played a significant role, for example, in intelligence gathering. Ukraine, in particular, has also made effective use of cyberattacks to make the conflict tangible for the Russian people. The role of cyber activities is also often extremely difficult to assess, as information about all operations or their effectiveness is not shared publicly. This is particularly true in intelligence-related projects, where cyber activities are currently thought to be most useful. When assessing the significance of cyber operations, it should not be forgotten that although no lasting damage has been achieved, both sides have had significant, albeit temporary, effects with their cyberattacks. Cyberattacks have continued throughout the conflict. Ukraine's strikes also show both development and growth when looking at operations in recent months.

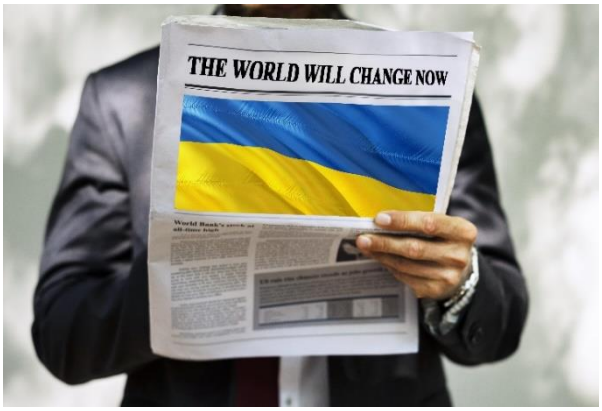
It seems more that the role of cyberspace was misunderstood before the war. It has not been that either side has significantly succeeded or failed on the cyber front. With cyber operations it is extremely difficult to cause permanent damage or destroy things beyond reparability, and therefore by their very nature do not seem to fit what they were thought to be used for in the conflict. It should also be noted that since this is indeed the first major modern war in which the cyber environment plays an important role, the warring parties themselves may have had to learn through trial and error how and where cyber operations are most useful.

It is difficult to estimate how much the parties relied on cyber operations before the conflict began. Russia seems to have failed in many of its war-related assessments, and therefore it would not be very surprising if more had also been expected from cyber capabilities. Over the past year, there has also been growing evidence of how successfully Ukraine, with US support, was able to identify and remove Russian invaders or malware from its systems just weeks before the start of the war. It is still unclear how well Russia was aware that the weapons prepared may not have been as effective as thought.

Thus, a cyber weapon is functional, but its role was previously misunderstood. Its primary purpose, in the light of current knowledge, is not to destroy or paralyze, but to obtain information, prepare operations, consume the resources of the opposing side and make war felt throughout society. Both sides have succeeded in this.

2. UKRAINE WON THE INFORMATION WAR - DOES IT MATTER?

Information warfare is a central part of every modern conflict, including the war in Ukraine. The means of information influencing aim to influence the outcome of an ongoing conflict. Information influencing refers to activities that aim to systematically influence public opinion, people's behaviour and decision-makers. The goals include supporting one's own agenda or, alternatively, fomenting mistrust in the target society. Furthermore, information influencing can take the form of individual actions or extensive influencing campaigns, for example through botnets, social media or other means of communication. This can manifest itself, among other things, in the dissemination of false or misleading information and in presenting information that is correct in itself in a way that supports false narratives.



Ukraine can be considered to have defeated Russia in information warfare, at least in the West. An example of this is the dominance of narratives and perceptions presented by Ukraine, which can be seen to have triumphed over the alternative course of events presented by the Russians. Especially in the early stages of the war, Ukraine's strategic communication was particularly successful. War-related stories and memes spread around the world. Similarly, Russia has failed to spread its own narrative. Before the war, there was much fear of Russia's information weapon and trolls, but their impact both in Ukraine and in the West has remained limited. Despite the contradictions in attitudes towards Ukraine and Ukrainian refugees, Europe has even been disconcertingly united in its support of the country. Ukraine's successful communications and Western media, which have clearly supported Ukraine in the war, play an important role in this. Of course, when it comes Russia's information influence one must remember that it is not necessarily meant to convince the West, but the target group is its own citizens and countries outside Europe.

On the other hand, there are indications that Russia controls its own information space relatively well, and neither Ukraine nor the West is able to influence Russian citizens. There has been no major anti-war movement in the country, despite attempts at informing Russian citizens, although the nature of an authoritarian society and sanctions for protesting certainly play a role in this. However, the Russian information space is also indicated by statistics from the research center Levada, according to which the amount of support for Putin has increased during the war, while attitudes towards the West have deteriorated. Although statistics from Russia should always be treated with caution, Levada has traditionally been considered one of the most reliable sources of information in the country. In this light, Russia’s information influencing directed at its own citizens seems to have been successful. On the other hand, for those Russians who want independent information, such would certainly be available, for example, from independent Telegram channels and opposition media often operating abroad. However, there is a considerable threshold for obtaining information openly from sources opposed to one’s own regime, and it is extremely easy for the Russians to simply turn a blind eye to the war. It is virtually impossible for Ukraine to penetrate and gain a foothold within this information wall, and it is unlikely that Russia will lose control of the narratives within its own borders.

Information warfare is constantly taking place. Although Ukraine has already won Western hearts, the country is also waging a kind of consumer war in the information environment. Recently, Western media has also featured more news than before about Ukraine's challenges, such as the shortage of personnel and ammunition. The possibility of defeat for Ukraine and the need for peace have also been seen here and there. Ukraine's challenge is to maintain its own narratives and war in people's minds as topical, important and international. At home, it is critical to maintain the morale of citizens, faith in victory and support for the continuation of military operations. In the end, the key question is how Ukraine will succeed in transforming information domination into concrete domestic and Western support. Winning the information war is of no comfort if on the physical battlefield only a silver medal is on offer.

3. LESSONS LEARNED FROM CYBERWAR AND POSSIBLE FUTURE DEVELOPMENTS

What can be said about the cyber component in future wars based on experiences from Ukraine? As first of its kind cyberwar in Ukraine is naturally an interesting object of study. But when preparing for future wars, it would also be important to try to understand how observed phenomena or lessons learned will affect future cyber conflicts. It is essential to bear in mind that we are currently analysing a situation that is still in progress, and the information provided is usually both inaccurate and coloured, because the parties tend to present things as advantageous to themselves, hiding their own failures. Obtaining impartial and accurate information is extremely challenging. Therefore, it is good to take the conclusions now made with this fact in mind.

However, it is easy to say that two years of war in Ukraine have clearly changed the perception of what kind of role cyber component plays in the war. The opportunities and limitations it offers are now better understood, as it has been possible to observe how operations are carried out in practice and what kind of effects they achieve. If the cyber environment is thought of as one of the battlefields of war, an interesting analogy can also be found in history and the combat environments that emerged from previous wars. For example, air warfare, which's first experience was gained in the First World War, did not yet play nearly as significant or decisive a role in this conflict as it did in the Second World War, where the use of the element had developed and the possibilities were better understood. However, we should not rush to say that cyber operations will acquire the same significance as bomber campaigns in World War II, although it is likely that their importance will also be emphasised in future conflicts.

Two different wars are never the same by their conditions. The unique characteristics of the war in Ukraine may also have affected how the cyber environment could be utilised. For example, the information environment has been inherently divided into camps supporting either of the sides, and influencing them with one's own narratives is practically impossible. In future conflicts, this may not be the case. For example, in the ongoing Israeli-Hamas conflict, the world globally – and also the West – is clearly more divided on which side's narratives are believed. Moreover, the war in Ukraine is, after all, about the struggle of a small country against a larger one. Although Ukraine has received and continues to receive a lot of support from many major Western cyber actors, the conflict cannot be considered a cyber struggle between two superpowers. If this kind of unrestricted and open cyber war were to break out between two superpowers, such as China and the United States, the aftermath could be much more devastating and the global effects more noticeable than what has now been experienced in Ukraine. The interdependencies of the global world may have surprising ramifications. In the future, Russia's hybrid warfare and its development possibilities will affect the principles of the use of cyber weapons, i.e. doctrine.

In the context of the war in Ukraine, the lack of spectacular cyber operations is certainly also explained by the relatively equal resources and capabilities of the parties. Both have proven to be able to both attack and defend in cyberspace. If the situation had been more uneven or, for example, if Ukraine had lacked foreign support, Russia's cyberattacks would probably have caused more extensive and lasting damage. Cyber expertise alone may not win wars, but its absence can contribute to defeat.

Cyberwatch Finland

NOTABLE PHENOMENA OF THE WAR IN UKRAINE

U.S.-UKRAINE OPERATION HUNT FORWARD

DATE: A few weeks before the start of the war and continuing until the end of February 2022.

DESCRIPTION: Hunt Forward operations are cyber threat mapping and mitigation operations conducted by the United States outside its own borders. In practice, in an operation, US experts who specialize in identifying the cyber activity of a specific threat actor (in this case, Russia) bring with them both expertise and advanced technology to identify threat actors or infected malware that has already infiltrated the target country's network and render them harmless.

IMPACT: The aim is to understand the threat picture, increase understanding of the means and methods of the threat actor and, in the case of Ukraine, essentially also prevent prepared operations. In Ukraine, Operation Hunt Forward was launched just weeks before the start of Russia's ground offensive, and the situational awareness it produced is considered one of the main reasons why, in the first weeks of the war, Russia's cyber campaign on Ukraine did not have such a significant impact. Ukraine was also autonomously, without U.S. assistance, prepared for cyberattacks, and for nearly a decade had gained first-hand experience in countering Russian cyber operations, but has itself emphasized the impact of Operation Hunt Forward on the cyber victories of the early weeks.

HACKTIVISM/CROWDSOURCING

DATE: From the beginning of the war to the present day

DESCRIPTION: Both sides have attempted to crowdsource their own and foreign citizens into their own cyber operations. In the ranks of Ukraine, the most significant player has been the country's IT army, in Russia several patriotic hacker groups. Although crowdsourcing provides the ordinary citizen with a tool to participate in war, it does present legal problems and can also pose a personal threat if the identity of a cyberfighter is leaked.

IMPACT: Low-level cyber operations, such as DDoS attacks, have mainly been carried out by cyber volunteers. According to the Center for Strategic &; International Studies, Ukraine's IT army is split in two. A public section organising DDoS attacks, which anyone can join, and a more "professional" section directed by defence and intelligence agencies, where little information is available. In addition to concrete cyber effects, crowdsourcing also has an information impact.

RUSSIAN DDOS ATTACKS IN EUROPE

DATE: From the beginning of the war to the present day

DESCRIPTION: Russian hacktivist groups have carried out a continuous stream of DDoS attacks during the war. The most well-known actor has been the NoName057(16) group. Attacks are often targeted at a specific political decision or event. For example, Germany's decision to hand over Leopard battle tanks and, among other things, the date of the NATO summit.

IMPACT: The impact of DDoS attacks has been limited, with the main achievement being to make websites temporarily inoperative. However, the value of attacks lies in their information effect, as they can generate publicity and cause deterrence in the target society and organisations. However, the information value of attacks is declining, as they are being widely accustomed to.

Cyberwatch Finland

EXAMPLES OF CYBERATTACKS

Kyivstar, Ukraina

LOCATION: 12.12.2023

DESCRIPTION: Ukraine's largest telecom operator, Kyivstar, was the victim of a cyberattack. The attack is considered one of the biggest and most significant cyber attacks of the war so far.

ACTOR: Responsibility for the attack was claimed on its Telegram channel by the Russian hacktivist group Solntsepyok. Most likely, however, Sandworm, an APT group under the Russian military intelligence GRU is in the background.

IMPACT: The telecom operator's services were unavailable for several days for up to 24 million users. The destructive effects of the attack were great – up to thousands of the operator's virtual servers and computers were wiped out. The threat actor has been in the operator's systems since at least November and has had the ability to intercept text messages and view phone locations, among other things. The attack also has a psychological impact on the population and information value in other parts of the world.

Viasat, Ukraine

DATE: 24.2.2022

DESCRIPTION: Ground-based routers and modems of the US satellite company Viasat were subject to data-destroying malware on the eve of the land attack. This had repercussions both in Ukraine and elsewhere in Europe.

ACTOR: Russia, however, the attack has not been linked to any specific Russian APT group or actor

IMPACT: The attack paralysed communications links in Ukraine and hampered communication between Ukrainian forces in the early stages of the war. The effects of the attack were also visible elsewhere – for example, in Central Europe, the impact affected the operation of wind turbines connected to the grid that lasted for months.

Attacks carried out by Ukrainian intelligence

DATES: December 2023 – January 2024

DESCRIPTION: In late 2023, the Ukrainian intelligence service (Головне управління розвідки Міністерства оборони України, GUR) began communicating openly about its attacks against Russian targets. In December, international attention was drawn to the successful attack on the Russian tax administration, in which the GUR announced that it had destroyed systems and that recovery from the attack would take several months. In January, GUR announced that it had attacked the Russian state research center Planeta, causing massive financial losses by destroying files.

ACTOR: Ukrainian intelligence service GUR.

IMPACT: While the allegations should be viewed critically, Ukrainian intelligence says the impact of the attacks has been substantial. The tax office's infrastructure will allegedly never be able to return to the same level, and in the case of Planeta, several hundred thousand dollars worth of data and hardware were damaged. 2 petabytes of data were also allegedly stolen from Planeta. Russia has denied the effects of the attacks and, in the case of the tax office, the whole incident in general.

REFERENCES

Cyberwatch Finland publications 2022–2024
https://www.cybersecurity-insiders.com/bo-team-hackers-wipe-2-peta-bytes-satellite-data-from-planeta/
https://therecord.media/illia-vitiuk-interview-ukraine-sbu-defend-forward
https://www.wired.co.uk/article/viasat-internet-hack-ukraine-russia
https://theworld.org/stories/2023-06-30/exclusive-inside-american-hunt-forward-operation-ukraine
https://www.secior.com/en/resources/uncategorized/ukrainian-datacenters-moved-outside-their-borders/
https://therecord.media/ukraine-hunt-forward-teams-us-cyber-command

Pictures: Pixabay