BESA
The Begin-Sadat Center
for Strategic Studies
Bar-Ilan University
PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

The Cyber Domain in the Russo-Ukrainian War

By Dr. Eyal Pinko

BESA Center Perspectives Paper No. 2,203, June 22, 2023

EXECUTIVE SUMMARY: Cyber attacks have been carried out by both sides in the Ukraine-Russia war to neutralize national infrastructures, banking systems, and government ministries; influence decision-makers, citizens, and soldiers; and gather intelligence. Cyber played no real role in disabling national capabilities or infrastructure, but has had psychological and cognitive effects. The first year of the war sharpened the need to build and upgrade information security measures, especially around critical national infrastructure; strengthen real-time information-gathering capabilities from social networks; strengthen awareness; and maintain information security.

The Ukraine-Russia war broke out on February 24, 2022, when the Russian army invaded Ukraine following a month's preparations and a ten-day armed exercise. The war, which is still ongoing, has included many cyber incidents. Cyber warfare changed the face of the military campaign, and with some calling this the first digital war – a nickname with no real basis, as a significant cyber campaign was conducted between Russia and Ukraine in 2014.

This article will provide an analysis of the role of the cyber domain in the first year of the Russo-Ukraine war and what it teaches us about modern warfare.

Credibility of Sources

A critical limitation on available information should first be noted. Descriptions of cyber attacks are based on media reports by publications that have their own agendas. Publications on both sides are often used for psychological warfare. As we have seen so far, both combatants in this war engage in deception and fake

news. These factors dominate the battlefield to such an extent that it is impossible to know which side's version is closer to the truth.

Descriptions of attacks described in this article are based on media reports and are quoted as they appeared. It should be remembered that the publications focus on attacks whose results are clearly visible. There is no real information on the number of silent attacks that have penetrated computer systems on both sides but not been exposed to the public.

Cyber Attacks Before the War

Russia has been conducting cyber operations against Ukraine since 2014 – intelligence gathering operations, influence operations and sporadic low intensity sporadic disruption operations against Ukrainian national infrastructure. Attacks relevant to the current war began about a month and a half before ground battles broke out. In early January 2022, the US warned Ukraine that its critical state infrastructures were under threat of cyber attack. Shortly after this warning, the websites of Ukrainian government ministries (Education, the Interior, Foreign Affairs, and others) were defaced and messages warning the residents of Ukraine about Russia were posted on them. The Ukrainian Internal Security Service claimed at the time that nothing had been stolen as part of the attacks, but tests carried out by American officials and Microsoft revealed viruses on Ukrainian networks – particularly those of critical infrastructures like the Ukrainian Ministry of Defense, power generation facilities, nuclear facilities, and others. About two weeks before the campaign officially began, the US sent expert assistance and technological solutions to protect Ukrainian infrastructure.

Russian Cyber Attacks During the War

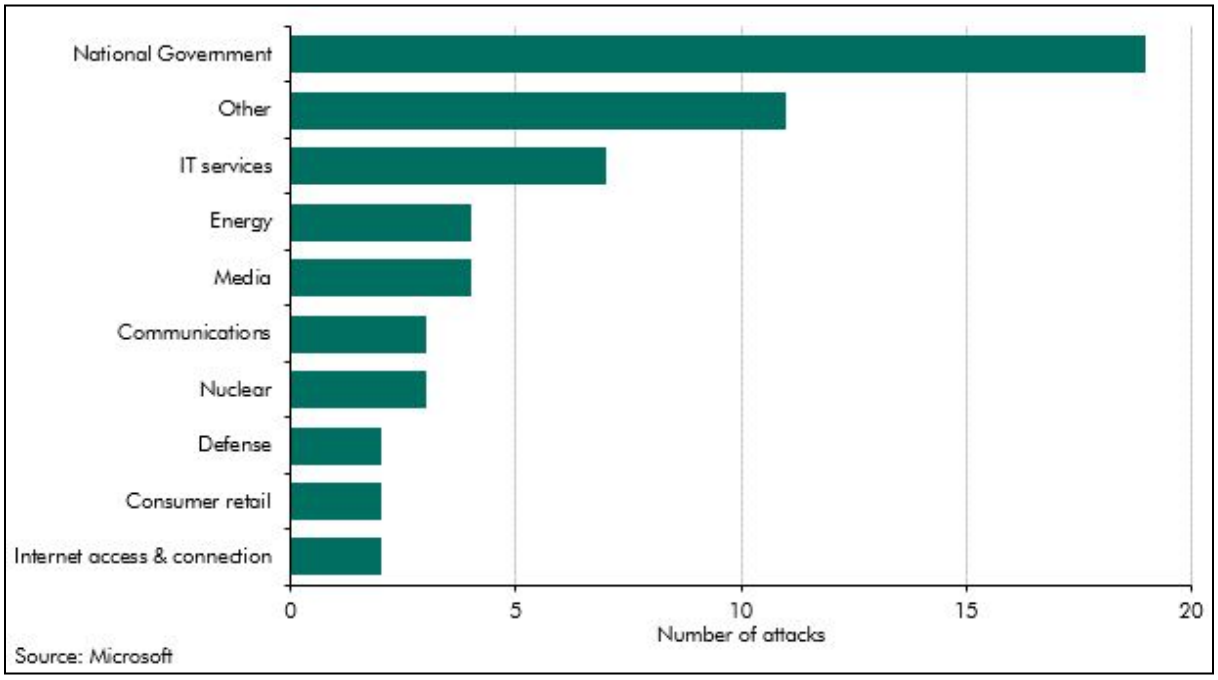
The day before the outbreak of the war and on its first day, many cyber attacks were launched on Ukraine's national infrastructure, government offices, and banking system. Most were Denial of Service (DoS) attacks and website defacement. Ukraine, which had suffered cyber attacks on its electricity company during the first war in 2014 and the shutdown of electricity in parts of the country for about half a day at that time, was prepared for the current campaign.

In the first months of the war, Russia repeatedly attacked strategic Ukrainian targets and national infrastructures like banking institutions, the electric company, nuclear facilities, and the transportation infrastructure, but the attacks failed. The Russians launched several strikes, mainly involving the deletion of information from servers and computers. A Russian cyber group called Armageddon targeted civilians and organizations in Ukraine in order to gather intelligence about the state of mind there, as well as other information that would assist in the ground

campaign and the shutdown of Ukrainian national infrastructure. Most Russian attacks from the beginning of February 2022 to October 2022 were directed against government institutions, IT infrastructures, and the energy sector.

Cyber attacks were also used in combination with ground force operations or fire strikes. In April 2022, during the ground attack to capture the Zhaporozhiya nuclear power plant, cyber attacks were conducted against the plant's corporate networks. The cyber attacks failed, but the plant was captured. In another case, the Russians attempted to disrupt the functioning of the Ukrainian Air Force headquarters in the city of Vinnytsia (200 kilometers south of Kiev). They first conducted a cyber attack on the regional communications network and then fired consecutive sporadic missile strikes on the airfield and headquarters itself. A similar attack was launched at government, military and national infrastructure installations in the city of Dnipro. The attack began with a DoS strike on the municipality's computers and website and continued with an attack by 11 cruise missiles on various installations in the city.

At the same time, through social media and attacks on news sites and radio stations, the Russians conducted large-scale influence operations of disinformation and fake news against the Ukrainian government and NATO. These operations continue today.



Source:https://obr.uk/box/cyber-attacks-during-the-russian-invasion-of-ukraine/

The Russians conducted offensive operations also against the USA, Great Britain, Germany, Poland, Latvia, and other countries. These operations were intended to disrupt national infrastructures, but also to create a deterrent against intervention in the war.

Ukrainian Cyber Attacks During the War

The Ukrainians responded by vandalizing Russian government websites in the first days of the war, creating DoS attacks and trying to create an understanding in Russia that Ukraine would respond to Russian aggression in the cyber domain as well as on the battlefield. Ukrainian president Volodymyr Zelensky even called on hackers from around the world to join the Ukrainian cyber army in attacking Russian websites and infrastructure as well as to be part of a cyber-based influence campaign. In the latter operation Ukrainians hacked into Russian government websites, sent messages to the cell phones of Russian citizens condemning the war, hacked the website of Russian television and broadcast messages there, and even hacked the website of the Russian Space Agency. The Anonymous organization claims to have penetrated and taken down the website of the Russian state intelligence service, the FSB. In addition to disrupting Russian state functions, the aim is to influence global and Russian public opinion to end the war.

Gathering Intelligence in the Cyber Domain

The purpose of military intelligence in wartime is to collect information about the opponent's capabilities, campaign planning, actions and unit locations so they can be stopped and destroyed quickly and efficiently. Military intelligence was collected before and during the war in Ukraine by various means, such as human intelligence (HUMINT), signal intelligence (SIGINT), visual intelligence (VISINT) and others. A further critical intelligence-gathering method is OSINT, or open source intelligence. OSINT makes use of the Internet, apps, and open communication networks.

The collection of OSINT takes advantage of the vast amount of information available on social networks, applications, and websites to which access is unobstructed and which provides the signature of users. This information can be collected and analyzed relatively quickly and with high accuracy by technological means. With that said, it can be difficult to know when the information collected is reliable and not disinformation.

Information was collected from photos, videos and stories uploaded by soldiers and civilians participating in or viewing operations. This information was used by the Ukrainian side to identify the location of Russian forces and turn them into targets. In June 2022, the Russians reported their intention to withdraw, but photos

and videos uploaded to social networks by Russian soldiers showed that they were not withdrawing and that the Russian announcement was a deception. According to reports, these videos and photos were reported by Ukrainian citizens to local security services.

The second dimension of intelligence gathering in cyberspace is the gathering of visual information, mainly through the purchase of satellite images that are sold online. This information was mainly used to designate targets for attack and to study the opponent's maneuvers. Countries that do not have photography satellites collect data from websites that operate their own satellites.

The war in Ukraine is not the first in which a parallel campaign was conducted in the cyber domain. It is precisely the connection between the cyber and the physical domains that makes cyber an element of modern war, one that many countries and organizations wish to exploit.

In the first Ukrainian war in 2014, the Russians used cyber operations to assist them in the land campaign. The most prominent example was an attack on the Ukrainian electricity system that left about a quarter of a million households without electricity for hours. Preparation for this attack was conducted about a year and a half before the actual attack, creating a back-door that would allow the Russians to penetrate the Ukrainian electricity network at a time of their choosing.

Attacks on national infrastructures are conducted to produce psychological, economic and military effects that help the military campaign. Such attacks take time. They are not real-time attacks like those seen in "Mission Impossible" movies. In order to carry out a cyber attack on national infrastructure, intelligence must be gathered about the target over a long period. An operational plan must be prepared and suitable malware must be inserted that will hide inside the target until activation.

After the 2014 war the Ukrainians and Americans studied the Russian *modus operandi* and raised the level of security at Ukrainian national infrastructures, thus foiling a majority of the Russian cyber attacks on Ukrainian infrastructure in the current war.

Bearing in mind the limitations on published information and spread of fraudulent information by both sides, it can be concluded that in this campaign, unlike the earlier one, cyber operations had no real role in disabling Ukrainian national capabilities and infrastructures. In fact, despite the deletion of information from servers (the Ukrainians claim most of the information was backed-up in invulnerable locations) the Russian achievements were minimal and did not rise above the level of harassment.

The cyber campaign in Ukraine did, however, create cognitive and psychological effects that influenced global public discourse, NATO, and the populations of both countries. While Russian cyber attacks on Ukraine delegitimized Russia and prompted other countries to provide the Ukrainians with additional assistance in cyber defense, they nevertheless created great anxiety in Ukraine. While it is difficult to isolate this anxiety from the broader fears of the local population during the Russian onslaught, it is likely that the cyber domain significantly elevated the anxiety of the Ukrainian population.

The world media has for the most part legitimized and even encouraged Ukrainian cyber attacks on Russia. They did not even disapprove of the Ukrainian president's call for hackers around the world to launch such attacks – an interesting move in which criminal elements with no direct connection to the campaign were essentially granted legitimacy to act against Russia by a silent Western world. Russian cyber attack groups, conversely, have consistently received scorn and condemnation.

The evidence indicates that during the first year of the war, the cyber domain had a negligible military effect. The adversaries employed cyber oeprations primarily for the purposes of psychological warfare and influence on local and global public opinion.

Analysis

In the cyber domain, where attack capabilities change every day depending on newly discovered weaknesses and fresh attack tools, countries do not necessarily have advantages over civilian attackers. A country can invest effort, money, and human resources to find weaknesses, attack capabilities, and defense capabilities, but this does not necessarily grant it superiority over its enemies in the cyber domain. Hackers can find new weakness at any given moment. Cyber supremacy, unlike military supremacy, is therefore a loose and dynamic concept that can change rapidly.

The matter of recruiting amateur or professional hackers from around the world is highly significant and can affect future campaigns, including in Israel. Israel could find itself facing not only Iranian, Hamas, and Hezbollah cyber attacks, but also attacks from others who share the goal of destroying Israel. We cannot know who might enlist in such a campaign, either beforehand or while it is going on. Nor can we know what new abilities such free agents might possess. These people could include Israeli citizens acting against it in concert with Israel's enemies.

Another important element of the cyber domain in the first year of the Russo-Ukraine war was fraud. False information was spread via news channels and fake

profiles were disseminated to confuse the enemy about military movements, gathering places, and attack plans. The Russians broadcast their maneuvers through their own news channels, which were in turn quoted in global news reports. These announcements sometimes caused Ukraine to activate forces and maneuver for defense when not required, sapping readiness for real military moves.

The third and final component of cyber is the gathering of intelligence through social networks, websites, and applications that allow the locating of targets and forces and an understanding of military maneuvers.

Recommendations

First, the Russo-Ukraine war has sharpened understanding of the need to build and upgrade information security measures, especially around critical national infrastructures like electricity, transportation, water, the financial system, communications, the health system and the defence organizations. In addition, protection measures should be strengthened for companies and organizations in the supply chains of national infrastructures. These will often be more vulnerable to and less aware of danger. They thus constitute an attack path to the heart of national infrastructures.

Second, real-time information-gathering capabilities must be strengthened on social networks to identify enemy soldiers and track their activity, location, and interactions. These tools must be able to distinguish between genuine and false information, which can be done using artificial intelligence. These capabilities should include detection of adversary cell phones, even when used among the civilian population, in order to create targets in real time. It should be noted that in the Second Lebanon War, Hezbollah apparently had such capabilities.

Conversely, the third recommendation, which is a corollary of the second, is to strengthen awareness of Israeli soldiers and civilians to maintain security of information before and during combat and not to reveal military secrets, including the location of forces, their size, or their use in social networks. Soldiers must be prevented from activating their phones during operations.

The fourth recommendation is the development of a national, uniform, timed and coordinated approach among all relevant bodies to create disinformation and influence on social networks and media channels. If the various bodies work together, they can achieve great influence in the domestic arena, in the eyes of the opponent, and in the often critical international diplomatic arena.

The fifth recommendation is the creation of permanent superiority in the cyber domain, the main element of which is the constant development of weaknesses,

loopholes and access points into enemy systems. Such an ability can be based on self-development but also on the discovery of existing weaknesses in the network, with an emphasis on the Telegram and Darknet channels, as well as on the operation of private bodies in state service.

Navy Commander (ret.) Eyal Pinko is a senior research fellow at the Begin-Sadat Center for Strategic Studies and a researcher and lecturer in intelligence, cyber, national security, and maritime security.