Anonymous Sudan and Killnet Factor in the Russia-Ukraine War in the Context of Cyber Security

Alika Guchua
Ph.D. in Political Science, Associate Professor,
Caucasus International University (Tbilisi, Georgia)
E-mail: alika_guchua@ciu.edu.ge
https://orcid.org/0000-0003-0347-9574

Thornike Zedelashvili
Ph.D. in Political Science, Caucasus International University (Tbilisi, Georgia)
E-mail: thomaszedelashvili@gmail.com
https://orcid.org/0000-0003-2630-1779

Guchua, Alika and Thornike Zedelashvili (2023) Anonymous Sudan and Killnet Factor in the Russia-Ukraine War in the Context of Cyber Security. *Future Human Image*, Volume 19, 34-40. https://doi.org/10.29202/fhi/19/5

The war between Russia and Ukraine has been going on for the second year. Almost all types of war weapons are used in this confrontation, except for nuclear weapons. At the same time, Russia uses a component of hybrid warfare, bombing Ukrainian cities daily. Now, it is known that the heaviest battles are taking place in Bakhmut. One of the important issues in this regard is the cyberattacks both in the real space and in the virtual world. Different hacker groups are involved in this project both at local and international levels. The United States of America, NATO, the European Union and other leading countries are trying to help Ukraine, both in real and cyberspace. This cyber war is being monitored by international-level experts and organizations in order to find out who is fighting on whose side. Not only during wars, but also without conducting a conventional war, it is often difficult to detect where cyberattacks are launched. However, in this case, various hacker groups take this or that cyberattack upon themselves, That is, they admit that they are the authors of cyber-attacks and directly express their sympathy towards Russia or Ukraine. The presented article discusses the role of Anonymous Sudan and Killnet in the Russia-Ukraine war and the factors in cybersecurity policy. The aim of the paper is to show the importance and influence of cyber security in the Russian-Ukrainian war in modern wars.

Keywords: cyber war, cyberattack, hacktivists, Russia, Ukraine, Georgia, NATO, European Union, hybrid war.

Received: 18 May 2023 / Accepted: 20 June 2023 / Published: 5 August 2023

Introduction

The Russia-Ukraine 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 attacks have been carried out by both sides in the Russia-Ukraine 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 (Pinko, 2023).

There is a hacktivist group called Anonymous Sudan. According to cyber experts, it is a Russian group of malevolent hackers with direct links to the Russian hacktivist group Killnet. This hacker group has declared that it supports the Russian Federation in the Russia-Ukraine war; therefore, it often acts against Ukraine.

The story of Anonymous Sudan emphasizes that the group carries out cyberattacks for anti-Islamic activities. The impression remains that the reason is to cover up the actual goal that the disclosed position, as if it is an Islamic hacking group, is fictional. Suspicions are also strengthened by the fact that all targets of both Killnet and "Anonymous Sudan" have been countries that oppose Russia's invasion of Ukraine.

Killnet is a pro-Russian hacktivist group active since at least January 2022 and known for its DDoS campaigns against countries supporting Ukraine, especially NATO countries, since the Russia-Ukraine war broke out last year. DDoS is the primary type of cyber-attack employed by the group, which can cause thousands of connection requests and packets to be sent to the target server or website per minute, slowing down or even stopping vulnerable systems. While Killnet's DDoS attacks usually do not cause major damage, they can cause service outages lasting several hours or even days. Although Killnet's ties to official Russian government organizations such as the Russian Federal Security Service (FSB) or the Russian Foreign Intelligence Service (SVR) are unconfirmed, the group should be considered a threat to government and critical infrastructure organizations including healthcare (Pro-Russian Hacktivist Group 'Killnet' Threat to HPH Sector, 2023: 1).

Anonymous Sudan and Killnet cyber-attacks on Ukrainian cyber systems

Although the said hacktivist group does not hide its sympathies towards Russia, the similarities between the two groups are still abundant. For example, a large proportion of their attacks include DDoS attacks. In January 2023, "Anonymous Sudan" published a statement that it helped Killnet carry out DDoS attacks against the German Federal Intelligence Service. Apparently, Anonymous Sudan is a hacking group based in Sudan. He is said to have been involved in cyberactivism and hacking processes around the world. This organization is considered part of the Anonymous network, which is an international association of hacktivists and activists. Many high-profile so-called #OP cyberattack *(#OP is a kind of shortened version of cyber special operation)* (Sigal, 2023). Such attacks are known as #OPIsrael, #OPAustralia and others.

"Anonymous Sudan" often uses the social network Telegram and Twitter to spread its statements. However, its goals and objectives are still vague. We have tried to find different studies and discuss this topic.

Anonymous Sudan has claimed responsibility for many cyberattacks since the Russian invasion of Ukraine, including DDoS attacks in France, Germany, the Netherlands and Sweden. As we have already mentioned, on the one hand, it is known that these cyberattacks seem to have occurred due to anti-Islamic activities. For instance, in the case of Sweden, activists burned the Koran, and the incidents were followed by cyberattacks. At the same time, data was stolen from the website of the airline company. The stolen data is most likely be used for blackmail, extortion, or sold on the black market. Anonymous Sudan and Killnet jointly claimed responsibility for many cyberattacks in March 2023, including against Latvian government agencies, NASA systems, and Ukrainian systems. Both separately and jointly carried out DDoS attacks on French hospitals, universities, airports, and systems of the ministries of justice and interior. Based on such facts, there is an assumption that "Anonymous Sudan" is a Russian hacktivist group and their claim to fight the anti-Islamic campaign is merely a cover-up.

Killnet launched DDoS attacks on the systems and websites of various organizations and government structures around the world in the months following Russia's war in Ukraine. The targets of Killnet were all countries, except the USA, which aid Ukraine in one way or another. The hacktivist group launched cyberattacks 2022 Year in February on more than a dozen hospitals in the United States (*Stanford Health, Michigan Medicine, Duke Health and Cedar-Sinai and others*) (The New Era of Hacktivism, 2022: 1).

In October, it carried out DDoS attacks on several airports in the United States "(Los Angeles International Airport, Chicago O'Hare International Airport, Hartsfield-Jackson Atlanta International Airport, etc.)" (The New Era of Hacktivism, 2022: 1), which caused flight suspensions and paralysis.

Killnet fully shifted its focus in April 2022 to supporting Russia's geopolitical interests. According to them, "more than 550 cyberattacks were carried out, of which 45 attacks were on Ukrainian systems, which is less than 10 percent of the total attacks" (The New Era of Hacktivism, 2022: 1).

"In March, a hacktivist group launched cyberattacks on the Connecticut International Airport of the United States of America. In April, it launched cyberattacks on the websites of the Ministry of Defense of Romania, the Border Police, the National Railway Transport Company and the Commercial Bank, as a result of which these websites were unavailable for several hours. In May, massive DDoS attacks were carried out on two leading countries of the European Union – Germany and Italy. And in June, two significant waves of cyber-attacks were carried out against Lithuania and Norway. In July, Killnet turned its efforts to Poland and managed to shut down several government websites. In August, cyberattacks were carried out on institutions in Latvia, Estonia and the United States of America. In September, the hacktivist group attacked Asia for the first time and carried out cyberattacks on Japan, and the reason was Japan's support for Ukraine" (The New Era of Hacktivism, 2022: 1).

Affected organizations consider these cyberattacks to be a medium-level threat. However, if security measures are not taken duly, they may lead to major problems. For example, when Killnet carried out cyberattacks on hospitals in the United States, the American Healthcare Association stated that "their attacks are not causing major damage but may cause service interruptions of several days" (Vijayan, 2023).

Mary Masson, Director of Public Affairs Unit at Michigan Hospital, explains that the Killnet cyberattacks on January 30, 2023, affected almost all of the hospital's websites (Uofmhealth.org, mottchildren.org, and others). According to Mason:

"None of the websites that were hacked contain patient information. When the attacks took place, patients had no problem accessing their information, they used the myuofmhealth.org portal as usual" (Bracken, 2022).

If you look at the facts, the cyberattacks of Killnet and "Anonymous Sudan" do not cause much damage, but the propaganda works – they do manage to carry out powerful cyberattacks. What is obvious is that their goal is simply to attract attention and spread pro-Russian statements. They attack the public websites of institutions and organizations aiming to show the general public their influence and create the feeling that Russia is invincible not only in the real world, but also in the virtual space.

As mentioned, even though Killnet cyberattacks are not very damaging, they cannot be ignored. The American Hospital Association has stated that Killnet is an active threat to the healthcare industry as well:

"Most of the time, Killnet cyberattacks do not cause us much damage, they can cause service interruptions, which usually last for a few hours or a day. However, it should be considered an active threat to government and critical infrastructure defense organizations, including healthcare" (Bracken, 2022).

Killnet's recent DDoS attacks on the systems of medical institutions in the USA, Germany, Poland, and Great Britain, as the hacktivist group stated, was the main reason for the decision of the United States of America to send battle tanks to Ukraine.

Killnet said they were able to launch token DDoS attacks aimed at supporting Russia and punishing supporters of Ukraine. For example, one of the targets was Elon Musk's Starlink broadband satellite network, which was subjected to cyberattacks that resulted in many customers complaining that they were unable to log into their accounts for several hours on November 18. Various groups were also involved in the implementation of the mentioned cyberattacks – for example, the hacker group Radis, Halva, Anonymous Russian, and others. Killnet carried out cyberattacks on the White House website on November 17, which it called "30 minutes of test attack". Regarding these attacks, the group released a statement saying that they wanted to carry out attacks for a longer period of time. The White House uses military-grade protection from Automatic to protect itself from DDoS attacks. Then, on November 22, they carried out "cyber-attacks on the Prince of Wales website and published a statement saying that the UK health system, the London Stock Exchange, the British Army and so on would be next" (Bracken, 2022).

The goals and objectives of hacktivist groups are extremely complex, with a large proportion of cyberattacks being DDoS attacks. Their actions should be monitored, as the Russia-Ukraine war is in an active phase, the list of Killnet targets may expand, and the cyberattacks may take a more intense, more damaging form.

It is also noteworthy that the number of followers on "Telegram" → Killnet reserve has increased from 34 thousand to over 85 thousand. If we compare this with the IT army of Ukraine, they have more than 200 thousand subscribers. It should be noted here that Killnet, in addition to "Anonymous Sudan", also has affiliated groups – Passion Group, NoName and others. They help Killnet with their botnets to carry out DDoS attacks. As it is known recently, "the mentioned hacktivist group received financial support of USD 44,000 from the Dark Web Marketplace" (Vijayan, 2023).

Rob Joyce, Director of Cybersecurity at the National Security Agency of the United States of America, notes that the Russian Federation and its hired hackers are carrying out attacks on Ukrainian information technology systems. In particular, one of their "targets is closed circuit television cameras, which are used by local authorities and private businesses to monitor the environment" (Russian hackers 'target security cameras inside Ukraine coffee shops, 2023: 1). Russian hackers are trying to hack the security cameras of various stores and institutions to obtain information about the movement of aid convoys. Joyce believes that they are also, "watching Russian hackers log into public webcams that are available to everyone, but Russian hackers also use that to watch aid convoys and trains"(Russian hackers 'target security cameras inside Ukraine coffee shops, 2023:1). According to Rob Joyce, "They know that the Russians are also monitoring logistics transport companies to find out more about the supply of arms to Ukraine" (Russian hackers 'target security cameras inside Ukraine coffee shops, 2023: 1).

Recently, a large amount of information about hacking activities from Russia has been leaked. This is against the background that there is a war going on in Ukraine, and a great number of Russian citizens do not support their country in this war. As for the leaked information, apparently an imperceptible office with the displayed sign of "Business Center" has existed for years in the northeastern suburbs of Moscow. There are modern buildings built around the office and an old cemetery with war memorials right beside it. The mentioned area is the place where Peter the Great once trained his army. For the media, it has become known that certain individuals in the mentioned office help Russia in military operations for hacking activities. According to reports, these are the employees of NTC Vulkan – software engineers. At first glance, their activities remind cybersecurity consultancy services, but the leaking of information and files from the said company put a veil over everything. Thousands of documents demonstrate how they work to support Russian military and intelligence hacking operations, how they prepare attacks on critical infrastructure, spread disinformation, and try to control situations in the Internet space. Also, it is known that "their activities are connected with Russian state services, such as FSB, GOU, GRU, SVR and others" (Harding et al., 2023). In the leaked documents from the mentioned company, we find such issues that "Vulkan is directly connected with the famous hacker group Sandworm, which twice left more than half a million people without electricity and heating in Ukraine, disrupted the Olympics in South Korea with cyber-attacks and created the world's most destructive malware NotPetya" (Harding et al., 2023). This information was spread by an employee of one of the companies, who expressed dissatisfaction with Russia's invasion of Ukraine. The source gave the mentioned documents to German publishing houses, and after the information spread, various well-known publishing houses such as The Guardian, The Washington Post and others started a journalistic investigation. As a result, five Western intelligence agencies confirmed that the mentioned files and documents were authentic. Files include e-mails, project plans, contracts, internal information documents, budgets, and more. The files reveal that Russian hackers have repeatedly targeted Ukrainian computer systems, some of which were already known some were not. Moreover, the files expose information about possible upcoming attacks; among others, the documents include potential targets and illustrative materials, a map showing targets for possible cyberattacks in the United States, and important details about a nuclear power plant in Switzerland that would be needed for further cyberattacks. Based on the available information, Russia is in constant conflict with the West, both in real space and in the digital world – with the United States of America, Great Britain, NATO, the European Union, Australia, New Zealand, Canada, and so on.

Conclusion

As we can see, parallel to Russia, conventional war is also active in the digital direction, and it is impossible to accurately calculate the losses so far. However, based on the daily information, we can conclude that we should expect big losses in the virtual space as well. Despite the fact that Ukraine is helped by the United States of America, NATO, the European Union, Great Britain, Georgia and other countries, it is still not possible to fully ensure security even in the virtual space, but there are many cases that Ukraine successfully copes with. For example, Ukraine and the US recently seized and shut down the servers of nine websites that offered cryptocurrency exchange services to cybercriminals. It is not clear how long the war will last. Although, it is true that advanced countries help Ukraine intensively, according to analysts, this is not sufficient. What happens in the conditions of real war is very similar to what happens in the conditions of virtual war, that is, in the Internet space. Both are tightly interlinked and it is impossible to discuss the two phenomena separately. Ukraine needs its defense systems equipped with the latest technologies, not only in the form of weapons, but also in terms of cybersecurity. Looking at this issue superficially would be a serious mistake, because the conquest of cyberspace can disable critical infrastructures and even military bases. Hence, a lot of attention, equipment, observation, research and action are required in this regard.

🕮 References

Bracken, B. (2022) *Killnet Gloats About DDoS Attacks Downing Starlink*, White House, 2022. Available online: https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov

Harding, L., Simeonova, S., Ganguly, M., and Dan Sabbagh, D. (2023) Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics. *The Guardian*. Available online: https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

Kovacs, E. (2023) US, *Ukraine Shut Down Cryptocurrency Exchanges Used by Cybercriminals, Security Week*. Available online: https://www.securityweek.com/us-ukraine-shut-down-cryptocurrency-exchanges-used-by-cybercriminals/?fbclid=IwAR0xr7MGMHg_RJ2PPh5DRrMlYCJvuoY_34j4CJzKe3A4v8v4tEnNzTuqAyA

Pinko, E. (2023) The Cyber Domain in the Russo-Ukrainian War. *BESA Center Perspectives Paper* No. 2, 203, June 22, 2023. Available online: https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/

Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector (2023) *HC3: Analyst Note,* January 30, 2023. Available online: https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf

Russian hackers 'target security cameras inside Ukraine coffee shops (2023) *The Guardian*. Available online: https://www.theguardian.com/world/2023/apr/11/russian-hackers-target-security-cameras-inside-ukraine-coffee-shops?fbclid=IwAR3JWtpSmI9UvvADsMqx5aVTbM8SjpsvCIUYPX389Ff_HxSarZV_ctLoMIQ

Sigal, L. (2023) What You Need to Know About the Anonymous Sudan Hacker Group. *CYE Blog*. Available online: https://cyesec.com/blog/what-you-need-to-know-about-the-anonymous-sudan-hacker-group

The New Era of Hacktivism – State-Mobilized Hacktivism Proliferates to The West and Beyond (2022) Check Point Research Team. Available online: https://research.checkpoint.com/2022/the-new-era-of-hacktivism/

Vijayan, J. (2023) Inside Killnet: Pro-Russia Hacktivist Group's Support and Influence Grows, *Dark Reading*. Available online: https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows

Vijayan, J. (2023) Pro-Islam 'Anonymous Sudan' Hacktivists Likely a Front for Russia's Killnet Operation, *Dark Reading*. Available online: https://www.darkreading.com/attacks-breaches/pro-islam-anonymous-sudan-hacktivists-front-russia-killnet-operation?fbclid=IwAR3RMbRQgQbRcMxmv-iZNGRGsvGEyuMUOK5IRfACYLzZQBPbcPmH6yo5uDA