Cyber war: The hidden side of the Russian-Ukrainian crisis

By: Ahmad Mohee *Cairo on 20th February, 2022*
ahmadmohee@gmail.com

Abstract:

Conventional political analysts point out that a Russian-Ukrainian military confrontation, if it does occur, could have its cyber repercussions. Cyber specialists are aware that behind all this is a cyber-war, whose battles have already begun and whose victims have multiplied since 2014.

This article aims to shed light on the history of the Russian-Ukrainian cyber war and the most important operations that took place during it. It also sheds light on the cyber capabilities of both sides, and prospects the future of cyber war for both sides and the role of the United States of America and the European Union in it.

While Ukraine suffers lack of cyber security expertise, poor regulation, limited response capacity and lack of coordination between cyber related agencies, Kiev is aware of the strength of the Russian cyber capabilities and is currently in a race against time to reduce the gap and improve means of defense and cyber deterrence in cooperation with allies, especially the United States and the European Union.

Keywords: cyber attack, cyberwar, cyber-war, Russia, Russian-Ukrainian, Ukrainia

History of The Russian-Ukrainian Cyber war

Ukraine has been under constant cyber-attacks from Kremlin-backed Russian hackers since Moscow annexed Crimea in 2014[1]. Cyber espionage, hacking into networks, databases and servers, disrupting energy and communications facilities, spreading rumors and disinformation has become part of the conflict between Russia and Ukraine.

The most notable Russian cyber attacks against Ukraine occurred during 2014 and 2015:

- During 2014, Russian cyber attackers gained access to the vote counting system in Ukraine on the eve of the general elections, destroying electronic records and forcing the Ukrainian authorities to manually count the ballots[2].

[1] Hall, Ben, et al. "Ukraine Shores up Cyber Defences in Readiness for Russian Attack." Financial Times, 13 Feb. 2022, www.ft.com/content/778997c3-50ce-4b40-9c20-c8564c840a57. Accessed 20 Feb. 2022.
[2] Schreiber, William, et al. "Authorities: Hackers Foiled in Bid to Rig Ukraine Presidential Election Results - May. 25, 2014." KyivPost, 25 May 2014, www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html. Accessed 20 Feb. 2022.

- In the following year 2015, during an operation attributed to a group linked to Russian military intelligence, a cyber attack caused a power outage for several hours in western Ukraine and part of Kiev. It was the first known blackout caused by a cyber attack[3].
- During 2017, the NotPetya attack occurred - which was carried out by the same group linked to the Russian military intelligence - and succeeded in infecting nearly 10% of all Ukrainian computer systems with a malware package before it spread around the world. In one of the most devastating cyber attacks in history, it cost companies around the world nearly $10 billion in losses, according to a US estimate[4].
- On January 15, 2022, Microsoft exposed malicious software, disguised as ransomware called WhisperGate, targeting dozens of government and non-profit organizations and IT institutions based in Ukraine[5].
- On January 19, 2022, a cyber attack disrupted certain functions of Global Affairs Canada GAC, after Canadian officials extended their support to Ukraine[6].
- And recently - in early February 2022 - Microsoft revealed the targeting of the Ukrainian military offices and government networks by the Actinium group, which is believed to be linked to the Russian security services. That targeting began since October 2021 and aims to spy and gather intelligence information[7].

On the other hand, several groups linked to Ukraine carried out several cyber-attacks with limited impact targeting Russian capabilities and interests, the most important of which were:

- Operation Prikormka, during May 2016, which included the publication of malicious software displaying the price list of fishing bait. It was not known for certain the extent of the damage caused by this malicious software[8].

[3] BBC News. "Hackers Caused Power Cut in Western Ukraine - US." BBC.com, 12 Jan. 2016, www.bbc.com/news/technology-35297464. Accessed 20 Feb. 2022.
[4] Aparna Banerjea. "NotPetya: How a Russian Malware Created the World's Worst Cyberattack Ever." Business Standard, 27 Aug. 2018, www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html. Accessed 20 Feb. 2022.
[5] Microsoft Security Blog. "Destructive Malware Targeting Ukrainian Organizations." Microsoft.com, 16 Jan. 2022, www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/. Accessed 20 Feb. 2022.
[6] Boutilier, Alex, and Mercedes Stephenson. "Global Affairs Canada Suffers 'Cyber Attack' amid Russia-Ukraine Tensions: Sources - National | Globalnews.ca." Global News, 24 Jan. 2022, globalnews.ca/news/8533835/global-affairs-hit-with-significant-multi-day-disruption-to-it-networks-sources/. Accessed 20 Feb. 2022.
[7] Microsoft Security Blog. "ACTINIUM Targets Ukrainian Organizations." Microsoft.com, 4 Feb. 2022, www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/. Accessed 20 Feb. 2022.
[8] Kovacs, Eduard. "Ukraine Separatists, Politicians Targeted in Surveillance Operation | SecurityWeek.com." Securityweek.com, 19 May 2016, www.securityweek.com/ukraine-separatists-politicians-targeted-surveillance-operation. Accessed 20 Feb. 2022.

- Operation "May 9, 2016", which consisted of 9 successful hackings of the websites of the separatist group "Donetsk People's Republic", in addition to Russian sites for anti-Ukrainian propaganda, and sites and networks of Russian private military companies[9].
- The “Channel One” hack, June 2016, during which the server of the Russian Channel One was hacked by the Ukrainian cyber alliance of hackers FalconsFlame, Trinity and Rukh8[10].
- The Surkov Leaks, October 2016, during which 2,337 emails and hundreds of attachments were leaked, revealing plans to seize Crimea and foment separatist unrest in Donbas[11].
- Recently, an Ukrainian group carried out a cyber attack that disrupted the operations of the railway system in Belarus on January 24, 2022, with the intent of slowing down the movement of Russian forces through the Republic of Belarus to the borders of Ukraine[12].

Cyber Capabilities of Both Sides

In general, the Ukrainian attacks were rudimentary and of limited effect. Ukraine suffers from a lack of cybersecurity expertise, poor regulation, limited response capacity and a lack of coordination between different agencies, all of which are shortcomings Kiev is trying to fix[13].

On the other side is the Russian bear, which is overstuffed with highly organized, efficient financial and human resources and cybersecurity advanced research centers. Russian cyber capabilities are very advanced in the field of defense and deterrence, and are always able to monitor and respond to cyber attacks, detect gaps in enemy systems, and plan effective and painful attacks that incur heavy losses to the enemy[14] [15].

[9] Shamanska, Anna. “Hackers in Ukraine Deface Separatist Websites to Mark Victory Day.” RadioFreeEurope/RadioLiberty, 9 May 2016, www.rferl.org/a/hackers-ukraine-deface-separatist-websites-victory-day-opmay9/27724532.html. Accessed 20 Feb. 2022.

[10] InformNapalm. “Ukrainian Hackers Break into the Russian Channel One.” InformNapalm.org (English), 11 June 2016, informnapalm.org/en/ru-channel-one/. Accessed 20 Feb. 2022.

[11] Walker, Shaun. “Kremlin Puppet Master’s Leaked Emails Are Price of Return to Political Frontline.” The Guardian, 26 Oct. 2016, www.theguardian.com/world/2016/oct/26/kremlin-puppet-masters-leaked-emails-vladislav-surkov-east-ukraine. Accessed 20 Feb. 2022.

[12] Pietsch, Bryan. “Hacking Group Claims Control of Belarusian Railroads in Move to ‘Disrupt’ Russian Troops Heading near Ukraine.” Washington Post, 25 Jan. 2022, www.washingtonpost.com/world/2022/01/25/belarus-railway-hacktivist-russia-ukraine-cyberattack/.

[13] Hall, Ben, et al. Financial Times, 2022. op. cit.

[14] Wolff, Josephine. “Understanding Russia’s Cyber Strategy - Foreign Policy Research Institute.” Fpri.org, 6 July 2021, www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/.

[15] Gady, Franz-Stefan. “Is Russia More Powerful than China in Cyberspace?” Thediplomat.com, 9 Apr. 2015, thediplomat.com/2015/04/is-russia-more-powerful-than-china-in-cyberspace/. Accessed 20 Feb. 2022.

The Ukrainian authorities are fully aware of the Russian cyber capabilities, and therefore they have engaged in a race against time to develop their capabilities in the field of cyber defense and security. The State Service of Special Communications and Information Protection has held several simulation exercises of cyber attacks targeting government servers and networks. During which, coordination with agencies concerned with cyber security is conducted for training on monitoring and responding to such attacks. One of the priorities of this Agency is to raise awareness among critical infrastructure operators and connect them with cyber information centers, so that attacks can be quickly monitored, analyzed and responded to[16].

The Role of US & EU

Ukraine is also making a good use of the generous aid received from allies, led by the European Union and the United States of America. The United States has sent experts and funds to bolster Ukraine's cyber defenses, of course the US administration understands that this will require a long-term effort. US is therefore ready to lead the Ukrainian cyber front to carry out defensive duties when necessary. A sound evidence of this was the statement of US President Joe Biden, during January 2022, warning Russia of the consequences with regard to cyber attacks, saying: “if they continue to use cyber efforts, well, we can respond the same way.”[17]

Russia has never conducted a military-level cyber attack to disrupt the enemy's command and control systems. Although some analysts dismiss this, we believe that Russia will not hesitate to use cyber attacks against the Ukrainian military to disrupt command and control systems prior to or during a military confrontation, if it occurs[18].

The next few days will be decisive and revealing of the fate of the conflict, diplomatic efforts may succeed in defusing the crisis and nipping the military confrontation in its bud. But the cyber confrontation will certainly not end, and the efforts of cyber mobilization on both sides will not stop. Cyberspace does not recognize efforts of diplomatic shuttle tours, and negotiating table is certainly not one of its components. And if Russia is determined to launch this military confrontation because of its annoyance over the deployment of a missile system, what will be the case if Ukraine’s efforts with its allies succeed in deploying a high-tech cyber defense and deterrence front in Eastern Europe?

[16] Hall, Ben, et al. Financial Times, 2022. op. cit.
[17] Hall, Ben, et al. Financial Times, 2022. op. cit.
[18] Kolbe, Paul R., et al. “The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict.” Harvard Business Review, 18 Feb. 2022, hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict. Accessed 20 Feb. 2022.