CENTRE FOR AIR POWER STUDIES

In Focus

New Delhi

CAPS InFocus: 15/2022

04 March 2022

Ukraine's Piling Problems: Fighting the "Russian Bear" in the Cyberspace

Ms Khyati Singh
Research Associate, CAPS

Keywords: Ukraine-Russia, Cyberwar, Cyberattacks, Anonymous.

Image Source: Bing.com [cybersecurity - Bing images]

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS]

Centre for Air Power Studies | @CAPS_India | Centre for Air Power Studies | Centre for Air Power Studies

Wars are no longer a hegemonic domain of tanks and missiles; rather they have proliferated into space and tech. The ongoing crisis in Ukraine and Russia has also kick-started a parallel crisis in the cyber domain. Cyber Attacks has added a new theatre to the wargaming with the operational air, surface, and maritime theatres. The present breakout of the crisis has provided an active playfield or wargaming zone to the cyber attackers, most of which remained theory till now. The 'future' that was debated at length citing cyber concerns, has become a reality. Furthermore, it unfolds at a time when the world is integrated like never before in human history.

Russia is not new to the domain of cybercrime and has exploited this window in the past as well. It was responsible for some of the most profound and powerful cyberattacks on Ukraine's power grid in 2015 and 2016.[1] Moreover, the famous 2017 "NotPetya" wiper attack, causing nearly $10billion of damage to the companies associated with Ukraine, had a global impact. This malware was sent across ostensibly as a software update for tax preparation. Therefore, the cyber front that was introduced during the Ukraine-Russian Crisis was unprecedented but not unexpected.[2] Hacker groups across the globe was activated, with each picking a side and capitalizing on the chaos. The prominent players at present are the Conti ransomware gang, the Anonymous, a hackers collective, and threat actors in Belarus. In addition, the United States Cyber Security Infrastructure Agency (CISA) has raised alarms against the Iranian Advanced Persistent Threat Actor (APT), where hackers gain access to networks for a prolonged period in order to acquire crucial information continuously.[3]

Anonymous (Anon), that has surfaced time and again, taking moral grounds over the issue of global concerns, has declared its open and upfront support for Ukraine. Their official twitter handle confirmed their position, and their first cyberattack involved disabling the official Russian news outlet, the RT News. This was followed by a series of attacks that targeted operations in Russia and brought down several crucial state sites. Their mode of operation and attack largely exploited the 'Distributed Denial of Service' (DDoS) capabilities that flood the targeted website beyond its traffic handling capacities and hamper legitimate service requests.[4] This, at times, leads to server crackdowns as well. DDoS is often coupled with Structured Query Language (SQL) injection, which allows extracting confidential information by injecting malicious SQL codes. Through the active deployment of these cyber weapons, Anon managed to breach the Russian Ministry of Defense database and leak the desired data. They have also cautioned against taking hostage ‘the industrial control systems’, which are a vital component of critical infrastructure. However, the Anonymous group is not operating unchallenged. It is being countered by “the Conti”, which is believed to be a hacker group that operates out of Russia and is sponsored by it. Therefore, it is the proxy channel Russia has well intact in the system to gain the technological cyber edge. Like the Anon, the Conti group too made it loud and clear on its dark web that they would take on the cyberwar from the Russian front. They have been operational in the past and caused a critical ransomware attack on the health services of Ireland in 2021. As a result, all IT systems in the nation were shut down. The group that was identified behind the attacks was “Wizard Spider” which operates from Russia. The Conti, while committing their support, has warned to strike back at the enemies ‘critical infrastructure’ in case of an escalated cyberwar.[5]

This cyberwar is not a ‘two-front’ battle; there are multiple players and layers to it. Apart from the major actors, there has been a volley of cyber actors involving nations like Iran and Belarus[6]. The Ukrainian Computer Emerging Response Team detected a wave of phishing attacks by a hackers group that works under the hand of the Ministry of Defense of the Republic of Belarus. The ‘phishing attacks’ send fraudulent emails to the targets that are camouflaged as legitimate. Therefore, their access ends up installing malware into the system, along with data theft. In addition, a new variant of wiper malware, named “Hermetic Wiper” was detected in the Ukrainian machines and systems.[7] This malware ‘wipes out’ or corrupts data. Russian cyberattacks are not only attacking large bases but also penetrating the system from all ends. Their famous cyber threat actor Sandworm, commonly known as Voodoo Bear, was identified. It used a new malware called Cyclops Blink, which picked on the loopholes in the networking hardware company Water Guard and attacked their systems. Cyclops Blink is equipped with modules that allow it to upload and download files from its command-and-control server. Moreover, it targets machines that can be utilized in attacking others.[8]

Further coming down from government to industries and then to individuals, the cyberattacks have touched all possible stakeholders. The Russian cyberattacks also included scare tactics and had spillover effects as well. Fake messages were circulated amongst the citizens of Ukraine that the ATM would not work. Thus, creating panic in an already disturbed atmosphere. Likewise, due to the integrated nature of affairs of world operations, it is comparatively difficult to contain cyberattacks to a particular domain.[9] They are prone to spillovers. For instance, the attacks on Ukraine took down the Ukrainian contractors in Latvia and Lithuania along with it. So far, the Russian cyberattacks have been territorial or physical. They have not delved into the economic sphere. However, that doesn't guarantee a future abstinent from the same.

There are no two opinions about the fact that cyberattacks are increasingly becoming 'weapons of the first strike' and are supplementing conventional warfare tactics. However, unlike conventional warfare methods, which are visible, cyberspace operates completely on the web, which remains a mystery to the naked human eye but is a crucial component of its everyday operations. Nevertheless, the brownie point with technology remains that technology can be outpaced by better technology, with the attached factor that it becomes obsolete at the fastest possible pace. The moment a hacker cracks the code for the deployed cyber weapon, it instantly becomes redundant and cries for an upgrade. Albeit, that remains a tall order in itself, but there is always a possibility.

The current cyberwar is nothing short of a wake-up call for the nations to 'web-up' their games and inculcate the changing realities of war games. The solution that countries have against such a nuanced challenge are still emerging and evolving. The most profound impact of these attacks happens on the supply chains. Hence, it is crucial that countries become highly self-reliant and take the indigenous approach at all levels, from code writers to software engines, hosted servers to chips. Moreover, the threat of cyberattacks should be taken seriously at all levels. The passcodes need to be made putting different variables and changed on a regular basis. Firewalls (virtual wall existing between the computer and the Internet, which filters the incoming and outgoing traffic for the user to safeguard the network) and Honey Pots (dummy computer systems which are used to lure attackers by making them appear accessible and vulnerable), also work as safeguards, along with multifactor authentication. Much like rapid action forces for ground operations, nations should work to build a strong 'Cyber Rapid

Response Team' with efficient hackers that can carry out cyber missions at the drop of a hat. Similarly, countries need to invest heavily in R&D concerning artificial intelligence (AI). AI can prove to be the Ramban (ultimate weapon) of modern warfare. Therefore, it is of crucial importance to develop its capabilities. Lastly, the world at large needs to adapt and adopt the cyber reality of the 21st century. Behavioural changes, nudged towards creating a security mindset, are the need of the hour. When wars go online, security has to go online as well.

NOTES

[1] an Emir, "The other side of 'war': Looking inside Russia's cyberattack on Ukraine", *Interesting Engineering*, February 25, 2022, https://interestingengineering.com/russias-cyber-attack-on-ukraine, Accessed on February 26, 2022.

[2] Nick Beecroft, "Ukraine's Allies Need a Better Framework to Assess Cyber Threats", *Carnegie*, February 25, 2022, https://carnegieendowment.org/2022/02/25/ukraine-s-allies-need-better-framework-to-assess-cyber-threats-pub-86528, Accessed on February 27, 2022.

[3] Michelle Petersen, "Ukraine-Russia Conflict – Cyber Resource Center", *SANS*, February 25, 2022, https://www.sans.org/blog/ukraine-russia-conflict-cyber-resource-center, Accessed on February 26, 2022.

[4] "Staying Secure in a Global Cyber Conflict", *Rapid7*, February 25, 2022, https://www.rapid7.com/blog/post/2022/02/25/russia-ukraine-staying-secure-in-a-global-cyber-conflict, Accessed on February 26, 2022.

[5] Anna Delaney, "Ukraine Crisis: How the Rules of Cyber Warfare Are Changing", *Bank Info Security*, February 24, 2022, https://www.bankinfosecurity.in/interviews/ukraine-crisis-how-rules-cyber-warfare-are-changing-i-5030, Accessed on February 26, 2022.

[6] Carly Page, "Ukraine says Belarusian hackers are targeting its defense forces", *Tech Crunch*, February 25, 2022, https://techcrunch.com/2022/02/25/belarus-hackers-ukraine/?guccounter=1&guce_referrer=aHR0cHM6Ly90LmNvLw&guce_referrer_sig=AQAAAKFW0Akk8a50AybQHqYCNGZQ4aRgx4j0USC4l0v5aj9T_BLL7qdbdYODDdYOroHvUcfa6AnTm9iSSybHvzQzA4RisY6R6aOnm6xHpZsyAjcPIk_WWQpyNryf10CfgzPiX8T27QejBEhStAZo6GWwK89lEJLVuxuIEeRQCp-R1Lqh, Accessed on February 26, 2022.

[7] Mathew Schwartz, "Wiper Malware Attacks Have Not Escaped Ukrainian Networks", *Gov Info Security*, February 25, 2022, https://www.govinfosecurity.com/wiper-malware-attacks-have-escaped-ukrainian-networks-a-18608, Accessed on February 26, 2022.

[8] Prajeet Nair, "New Malware in Russia-Linked Sandworm's Portfolio", *Data Breach*, February 24, 2022, https://www.databreachtoday.com/new-malware-in-russia-linked-sandworms-portfolio-a-18601, Accessed on February 27, 2022.

[9] Dan Goodin, "Russia's most cutthroat hackers infect network devices with new botnet malware", *ARS Technica*, February 24, 2022, https://arstechnica.com/information-technology/2022/02/russias-most-cut-throat-hackers-infect-network-devices-with-new-botnet-malware, Accessed on February 26, 2022.