Chapter 14
Russian Aggressive Cyber-Policy During Russia-Ukraine War

Ilona Chukhua
International Black Sea University, Georgia

ABSTRACT

The most important details in this text are that Russia could make a military impact through cyber operations, but this was not exposed due to limitations created for Russia, the protection system of Ukraine, and support from partners. Russian cyber strategies and objectives regarding Ukraine have been addressed in the same direction as Ukraine space, and the method of collection of intelligence was the main objective for Moscow in the process of the Russia-Ukraine war, but it also had minimal benefits for the aggressor. Additionally, Russia appears to rely on non-cyber sources of target intelligence, despite previous thoughts which said that Russia used malware against the Ukrainian positions. In general, cyber-policy has both positive and negative sides, but it has a very negative impact in the case of Russia's war against Ukraine.

INTRODUCTION

Since the beginning of the war, Ukraine has struggled with an increase in cyberattacks, with Russia carrying out at least 10 attacks per day (Independent, 2023). More concretely, more than 4,500 cyberattacks have been recorded since the invasion (Independent, 2023).

The goals of cyberattacks are different: government resources, critical infrastructure facilities, etc.

The Security Service of Ukraine (SSU) declared that this institute recorded 800 cyber-attacks in 2020, about 2,000 in 2021, and more than 4,500 since the invasion. As a result, SSU opened more than 64,000 criminal cases against Russian forces, almost half of which are war crimes cases (Forbes, 2023).

Furthermore, the SBU has uncovered or detained 360 enemy agents since the invasion began last February.

In general, Russian hackers have infiltrated the Ukrainian military, energy, and other critical computer networks. Western cybersecurity experts predicted that if hostilities broke out, Ukraine would experience devastating cyberattacks.

DOI: 10.4018/978-1-6684-8846-1.ch014

In early November 2022, the German government allocated €1 billion from its 2023 budget to support Ukraine. This money will be used to protect against Russian cyber-attacks and collect evidence of war crimes.

Ukraine is documenting Russian hacking as part of a plan to prosecute Moscow in an international court.

For more than 1 year of all-out war, Russian hackers have not achieved strategic goals. in 2022, the Security Service neutralized hundreds of Russian cyber-attacks and cyber incidents on Ukrainian energy facilities, of which almost 30 could become supercritical. since October, 2022, systemic cyber-attacks of the Russian Federation have been carried out on the energy infrastructure of Ukraine (Forbes, 2022).

Russia's Wartime Cyber Operations in Ukraine

Military Impacts, Influences, and Implications

Firstly, it can be evaluated how Russia had possibility to make military impact by cyber operations, which almost was not exposed. There are many reasons of it, such as limitations created for Russia, the protection system of Ukraine and support from the partners addressed to Ukraine in many directions which has been aimed to make strong protective shell, the specific characteristics of this Ukraine-Russia war, its structural elements of cyber-policy circumstances and warfare in general. The cyber policy of Russia, like a cyberattacks effected in favor of Moscow which was objected for Moscow's military aspirations and military operations in Ukraine. It can be said that cyber fires and cyber war are equivalent of military attacks or is sometimes it is the strong catalysator or more than directly visible actions on the combat arena. In many cases, Russian cyber strategies and objectives regarding the Ukraine has been addressed the same directions of Ukraine space, battle try via kinetic capabilities which implies weapons, for example transportation infrastructure, electricity and communications with other sources as well. This everything is very dangerous and it can ensure a lot of harm. In generally everything has positive and negative sides, cyber-policy is between them, but it has very negative impact in case of Russia's war against of Ukraine. The military approaches of Russia rapidly denied any kind of goals which would reduce damages. Cyberattacks of Moscow did not achieve systematic implications and mostly they became less productive, in some situations with limitations of capabilities than it would be in the system of kinetic fires.

Instead of cyber fires, method of collection of intelligence most probably was the main objective for Moscow in the process of Russia-Ukraine war, but it also had very minimal benefits for aggressor. Although intelligence processes are more difficult for outsiders to observe and evaluate, Moscow artillery appears to rely on non-cyber sources of target intelligence, despite previous thoughts which said that Russia used malware to against the Ukrainian positions (Bateman, 2022). From the outside, it seems that maybe Russian missile powers have gained cyber-derived intelligence, however this one did not have something valuable for the main decisions and action of Moscow. Also, it's so interesting here that even influence actions, which are part of Moscow's cyber doctrine, have received only minimal support from Russian hackers and more generally, Russia's comprehensive approach to war, which implies each step from planning its campaign to occupying territory, assumes that major military decisions are not guided by a rigorous intelligence process (Bateman, 2022). Despite of the limitations created for the Russia's cyber policy productiveness, probably the most significant are not adequate Moscow cyber capacity, also weak sides in Russia's non-cyber spaces and special protective powers of Ukraine and its supporter countries. To have a significant impact on a war of this magnitude, cyber operations would