State Service of Special Communications
and Information Protection of Ukraine

CYBER; ARTILLERY, PROPAGANDA. GENERAL OVERVIEW OF THE DIMENSIONS OF RUSSIAN AGGRESSION

17.01.2023 03:52

GENERAL OVERVIEW OF THE DIMENSIONS OF RUSSIAN AGGRESSION

The authors of the study have tracked the coordination of missile attacks on local governments and cyber attacks on community services, precise coordination of missile and cyber attacks on media and communication centers, and preparation and implementation of cyber attacks on institutions that help Ukraine (logistics, refugee support, and even cultural events), etc.

- Russian war against Ukraine has many dimensions: conventional, economic, cyber, informational, and cultural. Only understanding these dimensions' interaction allows for assessing the aggressor state's actions adequately.

- The world's first large-scale cyber war did not demonstrate new "types of weapons" in existing cyberspace. All attacks are carried out using previously known techniques. The attacks used by Russia have long been categorized and have straightforward solutions for counteraction.

- Cyberattacks are entirely consistent with Russia's overall military strategy. Moreover, cyber-attacks are often coordinated with other attacks: conventional attacks on the battlefield and information-psychological and propaganda operations. This effect was demonstrated in the autumn and winter of 2022, when, after a series of cyberattacks on the energy sector, Russia launched several waves of missile attacks on energy infrastructure. While simultaneously launching a propaganda campaign to shift responsibility for the consequences (power outages) to Ukrainian state authorities, local governments, or large Ukrainian businesses.

- Such coordination of attacks in different dimensions of aggression is widespread, although coordination is not an absolute constant rule.

- Doctrinally, Russia often considers cyber and information dimensions as a single "information confrontation" domain. This confrontation can include either pure information campaigns or something more complex. However, in any case, the goal is information manipulation, to which all democratic regimes are naturally vulnerable.

- Cyber attacks, like conventional attacks of the Russian Federation, do not recognize any rules - infrastructure, humanitarian organizations, and private and state-owned companies are under attack. Russian hackers do not accept restrictions and do not recognize international borders, attacking different countries if they cooperate with Ukraine.

- There is no reason to believe that the intensity of cyber attacks will decrease. The only question is what they will focus on.

● The study shows that it is necessary to adapt military doctrines to modern challenges, using the lessons of the Ukrainian-Russian war for forecasting and modeling tactics to effectively stand up against Russia and other authoritarian regimes.

● Change legal approaches to the definition of aggression, significantly expanding the relevant legal interpretations;

● Restrict authoritarian regimes' access to modern technologies by strengthening sanctions, including sanctions against the most critical sectors of the economy of such regimes.

The multidimensionality of Russian aggression manifested itself even before the full-scale invasion. Examples are the so-called "economic wars" and powerful hostile propaganda campaigns. But on February 24, 2022, the correlation between different types of attacks became systemic.

Russia practiced this tactic in previous armed conflicts (for example, during the aggression against Georgia). If it is not studied and effectively countered, this tactic will be used in the future against other countries. For example, suppose Russia has yet to receive a solid response for all its aggressive actions against Ukraine. If no hefty action is taken, it will return with even more daring attacks that will not be limited to Ukraine or our region alone.

The need to protect against multidimensional aggression creates a demand for

- multidimensional information and multidimensional (not isolated) forecasts;

- multidimensional strategies to counter attacks;

- multidimensional legal responsibility of the aggressor.

Another critical issue is the need for complete economic isolation of the aggressor state. First of all, it is about restricting access to all modern technologies. After all, those are all used by Russia as a weapon.

Unfortunately, the international community lacks these components necessary for success. For that reason, most of the developments need to be sufficiently systematized. Therefore, it is essential to change all approaches urgently.

It is commonly believed that cyber-attacks are the weapon of the future. However, the war in Ukraine proved that this future is already here. Therefore, defense doctrines and international laws must adapt quickly.

The multidimensionality of warfare is a new security challenge (which could have been predicted but still needs to be adequately prepared for). There is no doubt that Russia is not the only threat to international security. Other authoritarian regimes will also conclude and use these approaches in the future.

Paradoxically, conventional attacks may eventually yield to cyber attacks in their negative consequences. Even today, in the example of Russian aggression, we can see hackers attack every object. However, in priority:

- state institutions (as decision-making centers responsible for maintaining stability within the country)

- civilian and energy infrastructure (because Russia is a terrorist who wants to increase the suffering of civilians without having successes on the battlefield),

- media and communications (these attacks strengthen Russian propaganda, a proven weapon of the Putin regime).

The main goal of Russian hackers has changed since the beginning of the war. Before the invasion and in the first month of the war, cyberattacks were aimed at the communication department, which was supposed to limit the functionality of the military and government in Ukraine. However, after the first defeat at the front, the Russian aggressor focused on inflicting maximum damage on the civilian population. This change of strategy can be traced in all dimensions of aggression. The attack on energy infrastructure is the best example. This attack was well thought out both in terms of timing and targets. During the cold snap, the first massive attacks on the energy infrastructure took place to put additional pressure on the civilian population, which adapts to inconveniences much worse than the military.

Therefore, the main task for Ukraine and our international partners is to identify all correlations in the Russian Federation's actions and develop a comprehensive strategy to counter these attacks.

INTERCONNECTIONS BETWEEN EVENTS OF DIFFERENT DIMENSIONS OF RUSSIAN AGGRESSION

The intensification of large-scale cyberattacks preceded the conventional full-scale invasion.

On February 15, Russian hackers launched the most powerful DDoS attack in the history of Ukraine, which, among other things, was aimed at the financial sector (DDoS attack on 15 banking sites, sites with the gov.ua domain, as well as sites of the Ministry of Defense, the Armed Forces and the Ministry of Reintegration of the Temporarily Occupied Territories, which lasted about 5 hours). On February 23, before the Russian invasion of Ukraine, several government and banking websites were attacked again. According to the state-owned electricity transmission system operator Ukrenergo, the peak of cyber attacks against the energy sector occurred when the Ukrainian power grid was connected to the European ENTSO-E (i.e., on February 23-24). During some attacks on Ukrenergo, Russian hackers did not even try to hide their origin and used Russian IP addresses to scan the network of the state-owned energy operator.

Thus, the cyberattacks were designed to increase the chaos of a conventional invasion, reduce the country's governability, and damage critical infrastructure.

Detailed information in the attached file.

CONCLUSIONS AND RECOMMENDATIONS

Russian armed aggression against Ukraine began in 2014 and was multidimensional from the beginning. In addition, Russia has constantly used hybrid attacks (economic warfare, propaganda campaigns, etc.) to achieve its own goals. Furthermore, unconventional Russian aggression continues against Ukraine; such attacks are carried out against all "unfriendly" countries. These attacks pose global threats. Therefore, the correlation between different dimensions of aggression needs to be studied in detail, and all world powers (except for a few allies of the Russian Federation) are interested in effective counteraction to these attacks.

Recommendation 1: Ukrainian experience should be systematized and used to counter Russia and other authoritarian regimes.

Russia's large-scale invasion has demonstrated many logical connections between different types of attacks. The Russian aggression against Ukraine has no analogs in the modern history of Europe. At the same time, this war indicates the approaches that could be used in future armed conflicts.

The confrontation between democracy and authoritarianism is only gaining momentum and will be decisive in shaping the global agenda in the upcoming decades. Therefore, Ukraine's experience is the key to the victory of democracy. The main weakness of authoritarian regimes is that they use each other's experiences and are always similar. Their centralization and predictability are not a strength but Achilles' heel.

Recommendation 2: Defence doctrines should adapt to the requirements of the times. Logical connections between different dimensions of Russian aggression can be used for forecasting and modeling.

Some of the data used to model the wars until February 24, 2022, were wrong. And it is not only that many analysts underestimated Ukraine and overestimated Russia. The problem is also that many theoretical assumptions have never been tested in practice.

Defense doctrines must consider that there are other ways to inflict significant damage on adversaries. And the more digitalized the world becomes, the more deadly cyber attacks can be.

Therefore, all strategic documents should consider modern warfare's multidimensionality.

Recommendation 3. International legal approaches to the legal definition of aggression should change (aggression in the XXI century is not only conventional). Moreover, responsibility should extend to all manifestations of aggression, not just the classic ones.

The legal definition of aggression was formulated by the United Nations General Assembly Resolution 3314 back in 1974. Since then, the international community has not dared to question the relevance of this definition. Unfortunately, international law also almost completely ignores the concept of economic aggression. Although Resolution 3314 provides that aggression is "the use of any weapon by a State against the territory of another State," there is currently no clear answer to whether "any weapon" includes economic, information, and cyber weapons. Most lawyers will have doubts. And this ambiguity is used by the aggressor state (and will be used by other authoritarian regimes). Therefore, the definition of aggression should be updated.

Recommendation 4. Cyberattacks can be equated to war crimes. Therefore, international humanitarian law should establish a stricter framework for unconventional attacks.

Russia's attempts to destroy the Ukrainian energy system have demonstrated that cyber-attacks often accompany conventional attacks against critical infrastructure. In theory, cyber attacks can cause no less harm and suffering to civilians than missile attacks. Consequently, cyber attacks can be war crimes. Thus, international humanitarian law should become more predictive and offer adequate regulation of the relevant legal relations.

Recommendation 5. The multidimensionality of Russian aggression proves the need for sanctions against the most critical sectors of the economy. Sanctions should be strengthened, and international companies should leave Russian market. Today, complicity in aggression is not only the sale of drones but also the provision of access to technology.

The power of unconventional attacks further exacerbates the need for complete economic isolation of the aggressor state.

In addition, peculiar aggression (primarily Russian cyber attacks) has no geographical restrictions. It means that Western companies that continue to supply Russia with the latest technologies not only contribute to the continuation of aggression against Ukraine. In addition, they undermine the security of their own countries because no one knows against whom a Russian attack will be launched tomorrow.