PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 191 (2108), 6 DECEMBER 2022 © PISM

BULLETIN

Cyberattacks Integral to Russia's Political and Military Strategies

Aleksandra Kozioł

To destabilise democratic countries that support Ukraine, Russia employs cyberattacks on the target state's public institutions and critical infrastructure. These activities have clearly intensified since the full-scale invasion began in February 2022 and is in line with the implementation of Russian military strategy. In this context, it would be beneficial within the EU and NATO to develop joint action plans to respond to future threats in cyberspace.

Russian Capabilities in Cyberspace. Russia for years has been actively using digital space to pursue its own interests, often violating international law. With the help of specialised units within military intelligence (GRU) and foreign intelligence (SVR), security service (FSB), and state-sponsored hacker groups, it attacks public institutions and private entities in other countries. Russia uses such attacks to steal, encrypt, or destroy data, and to infect computer networks, which become a source of malware spread to other entities. The actions of Russian hackers are primarily an element of hybrid activities, which Russia often coordinates with online disinformation as it intensifies their impact on society. Russians carried out extensive cyberattack and disinformation activity during the 2016 U.S. presidential elections and Brexit campaign in the UK, influencing the result in both cases. Russia is also responsible for the NotPetya malware attack in 2017, considered the most destructive in history. Originally aimed at Ukraine, it spread to dozens of countries and caused losses estimated at $10 billion. As indicated by recently published reports, for example, by Microsoft and the EU Agency for Cybersecurity (ENISA), the invasion of Ukraine has been accompanied by a significant increase in cyber-aggression. Russia is described in these reports primarily as a source of the threat, although it is also becoming the object of attacks more and more often.

Cyberattacks as an Element of the Aggression Against Ukraine. Russia even at the beginning of 2022 conducted intensified activities in cyberspace in preparation for the invasion. The most serious attack took place in mid-February, when Russian hackers disrupted several Ukrainian government websites, including the ministries of Foreign Affairs and Defence, as well as two of the largest state-owned banks. An hour before the invasion started, in order to surprise and slow down the response, Russia launched a cyberattack on the KA-SAT satellite network operating in Europe and the Mediterranean. By doing so, it disabled communication between several thousand public and private users in Ukraine and disrupted broadband connectivity to tens of thousands of recipients in several EU Member States. In the following months, victims of this massive Russian offensive in cyberspace included Ukrainian authorities, media, and critical infrastructure. Hackers, using mainly phishing campaigns and system loopholes, stole information needed by Russia, destroyed key data on the Ukrainian side, or conducted espionage operations. These cyberattacks were correlated with other actions taken by Russia, and in some cases they directly preceded events on the front, such as the offensive on the city of Sumy, the shelling of the TV tower in Kyiv, and the seizure of the nuclear power plant in Zaporizhzhia.

Moreover, Russia has intensified its activities in cyberspace, targeting, for example, public institutions, humanitarian organisations, and think tanks in more than 40 countries supporting Ukraine. The main target of the Russian operations is the U.S., perceived as the primary adversary on the international level. Poland is the most frequently attacked country in Europe because most transports with

military and humanitarian aid to Ukraine pass through its territory. Other NATO Member States, as well as Finland and Sweden, are also targeted. The threat posed by Russia is serious because it has the aim of not only breaking Western security measures (according to estimates, hackers are successful in about a third of the cases) but also to conduct long-term espionage in cyberspace. As in the case of Ukraine, some actions aimed at Western countries remain correlated with events of a political nature, for example, on 23 November the European Parliament's website was attacked by hackers after it declared Russia a state sponsor of terrorism.

Reaction to the Russian Threat in Cyberspace. Russia's full-scale invasion has increased the support of Western states in building up Ukraine's cyberdefence capabilities. Already in February, the EU launched the Cyber Rapid Response Team (CRRT) for the first time as part of PESCO, delegating experts from the Member States to assist the Ukrainians. Furthermore, Ukraine in March joined as a contributing participant to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). In the face of the Russian invasion, however, the Ukrainian authorities needed to quickly increase their offensive capabilities, which is why on 26 February Mykhailo Fedorov, deputy prime minister and minister of the Digital Transformation, announced the creation of the IT Army of Ukraine. Its main task is to attack Russian public and private entities, aiming to, among other goals, block administration websites and government media, spread true information about the war, as well as access critical data. Although inspired and actually managed by the Ukrainian authorities, this organisation remains an unofficial structure, based on a Telegram app channel. Other hacker groups, such as Anonymous and the Belarusian Cyberpartisans, are also taking action in support of Ukraine, but they are not affiliated with the Ukrainian authorities and their activities are ideologically motivated. Anonymous is credited with broadcasting in March true information about the war in Ukraine on the main Russian TV channels, including Channel One and Russia 24. The position of private companies, such as Microsoft and Google, is also unprecedented, as they started cooperation with the Ukrainian authorities and support them in detecting and combating the Russian attacks.

Conclusions. The Russian authorities use cyberattacks to increase the effectiveness of their actions on the international level. Russia's intensified offensive activities in the digital space are aimed at creating instability in democratic states, aiming to, among other things, discourage them from supporting Ukraine. The Russian hackers hit mainly Ukrainian targets (according to estimates, there are two or three attacks per week), as the situation at the front is most important. By forcing Ukraine to constantly defend itself, Russia is using tactics to try to exhaust the enemy, while trying to gain an information advantage and lower Ukrainians' trust in their authorities. Attacks on democratic states that support Ukraine are carried out in a more selective manner and are usually an element of Russia's political signalling. The Russian authorities are willingly and increasingly more open to using such tactics because cyberattacks, which are treated as actions below the threshold of war, are rarely responded to by public or private victims. The reasons include the difficulty in identifying the sources of the attack and the limited possibility of punishing the perpetrators. For example, the first sanctions in the EU's history for cyberattacks (including NotPetya) were adopted by the EU only in 2020, and covered just three entities and six persons.

The significant increase in the number of Russian cyberattacks against Ukraine is also a serious threat to Western countries as it is difficult to assess to what extent their current territorial concentration is dictated by the nature of operations or decisions made by the Russian authorities. The potential use of malware can lead to serious consequences if it leaks outside the targeted country in an uncontrolled manner, as was the case with NotPetya. In addition, even if Russian troops are pushed out of Ukraine, Russia will retain its aggressive cyber capabilities. In this context, it is worthwhile for Poland to initiate deepening of cooperation between EU and NATO countries in this area, as well as extending the capabilities to Ukraine and other partners such as Moldova and Georgia. This is crucial not only to improve information exchange and strengthen cybersecurity measures but also to prepare action plans in case of attacks. The growing involvement of international corporations operating in the digital space also requires deepening public-private cooperation, which becomes particularly urgent for the most threatened countries in Europe, including Poland. Examples of success in this area so far show that the diversification of service providers simultaneously strengthens the resistance to the possible effects of cyberattacks, hence the importance of internet access from alternative sources like the Starlink network, as well as cloud solutions for data storage, among other tools.