PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NO. 172 (2291), 21 NOVEMBER 2023 © PISM

BULLETIN

Russia Continuing Cyberthreats Against NATO Countries

Anna Maria Dyner

In recent years, Russia has increased the intensity of hostile operations conducted in cyberspace against NATO members and Ukraine. This activity will continue, as evidenced by the work on the concept of a cybersecurity strategy. On the part of the Alliance and member states, there is therefore a growing need to further build up defensive capabilities in this domain, including active defence, and to expand cooperation with partners.

Since the Russian invasion of Ukraine in 2022, NATO countries, especially those supporting Ukraine, have become a prime target for Russian cyberattacks. A Microsoft report from October this year indicates that 36% of the hostile Russian actions identified by the company targeted members of the Alliance (compared to 48% targeting Ukraine), with 13 of the 15 most frequently attacked countries being NATO members and pending member Sweden. Excluding Ukraine, Russia most frequently attacked targets located in the U.S. (21% of all hostile activity), Poland (10%) and the UK (9%), focusing on government infrastructure (27%). Moreover, data from the Cyberspace Defence Forces shows that there was a five-fold increase in the number of attacks carried out from February 2022 to October 2023 by pro-Russian cyber communities and hacking groups on military infrastructure (under the remit of the head of the Defence Ministry's CSIRT). Russia mainly attempted to steal data, paralyse systems critical to the functioning of the state, or impersonate state institutions, among other things, in order to sow disinformation or gain access to data.

Russian Approach To Cyberspace. Russia attaches great importance to cyberspace as an operational domain in which it can conduct effective offensive operations as part of broader hybrid operations against adversaries. Cyberattacks require relatively small resources and can result in large costs on the part of the attacked state. Russia has been increasing the scope of its cyber activity since 2015-2016, which coincided with the adoption of its Doctrine of Information Security of the Russian Federation. The document identifies influencing information infrastructure for the purposes of war, technological reconnaissance, conducting information and psychological operations aimed at destabilising the intra-political situation, and coordinated cyberattacks on IT critical infrastructure. Russia is currently working on the concept of a cybersecurity strategy, a draft of which has been posted on the Federation Council website. That document indicates that Russia will seek to increase the scope of activities undertaken in cyberspace, explaining this by the need to protect state infrastructure and business and educate the public. It should be assumed that in these areas the Russians will develop offensive capabilities against NATO and its partners.

The Intelligence Board of the Russian General Staff (GU), the Information Technology Forces, the Federal Security Service and the Foreign Intelligence Service are responsible for cyber activities in Russia. Officially, they are supposed to secure the functioning of critical information infrastructure and protect it from hostile action. In practice, they carry out offensive operations in cyberspace, mainly targeting Ukraine and NATO countries. Cybersecurity reports published after Russia invaded Ukraine by major Western technology companies point to numerous examples of Russians' direct involvement and the activities carried out by their affiliated hacking groups. The most frequently mentioned are the Killnet group and those tied directly to the GU and the

Russian armed forces, including Fancy Bear (APT28), Cozy Bear (APT29) and Sandworm (which is a subunit of GU 74455).

In addition to stepping up the scale of offensive cyber activities, Russia is seeking to increase its control over the shaping of the international legal regime on cybersecurity. That's why it is active at the UN, where work is underway on a treaty on cybercrime, of which Russia was a key initiator. It is supported there by some of the countries with which it has signed bilateral cooperation agreements on ensuring information security since 2020, including Azerbaijan, Belarus, China, India, Indonesia, Nicaragua, South Africa, Uzbekistan, and Vietnam. Some of them are calling for, among other things, the legalisation of surveillance across borders, which could mean additional persecution of dissidents or independent media writing about the situation in non-democratic states. This approach is opposed mainly by NATO and EU countries.

Threats and Challenges to NATO. Cyberattacks are part of Russia's hybrid activities that can lead to destabilisation in NATO countries and undermine the Alliance's political cohesion. They also create constant pressure on allies' information systems and demonstrate Russia's capabilities. At the same time, the war in Ukraine has shown that Russian cyberattacks can be an integral part of its military operations, as its full-scale invasion was preceded by attempts to destabilise the Ukrainian energy and banking systems, among others. Thus, the successful elimination of this threat could delay the start of full-scale Russian attack against NATO states.

Identifying the growing importance of cyber operations, NATO recognised it as its fifth operational domain at the 2016 Warsaw Summit. At the Brussels Summit in 2021, a comprehensive cyberdefence policy was endorsed and the Allies committed to using capabilities to proactively deter, defend and counter cyberthreats, including through collective response. Since 2008, the NATO Cooperative Cyber Defence Centre of Excellence, established in Tallinn, has been operational, providing cyberdefence research, training, and exercises covering the areas of technology, strategy, operations, and law. Moreover, the Cyber Operations Centre was established in 2018 and the Virtual Cyber Incident Support Capability was inaugurated as a result of the Vilnius Summit. NATO also conducts regular drills, such as the *Cyber Coalition Exercise* held annually. The Alliance also cooperates with international partners, particularly the EU.

The most important challenge to dealing with Russian cyberthreats is, however, the Alliance's defensive doctrine, which, while NATO recognises that cyberattacks can trigger an Article 5 response, may undermine the credibility of its defence and deterrence policy in this domain. This is all the more important as the notion of a single state of peace or war cannot be applied to cyberspace where hostile action is constant, nor can the beginning of a conflict be clearly identified, which in other operational domains is easily defined as physical aggression by an adversary. This means that Alliance members should redefine their approaches to threats in cyberspace and begin to develop the concept of active defence, which means the use of offensive means for defensive purposes. This consists of intercepting, disrupting, or deterring an attack or preparations for it in advance and in self-defence. In the event of a threat of military aggression, NATO should be able to take pre-emptive action in cyberspace to minimise the impact of an attack.

Conclusions. Russia's approach to cyber operations means cyberattacks against NATO states can be expected to continue or intensify. The targets will be infrastructure crucial to the functioning of states, including military infrastructure. Russia's anti-Western coalition of cyber actors can also be expected to strengthen with states such as China, Belarus, and Iran undertaking hostile activities in cyberspace against Alliance states.

Russian actions will therefore require NATO countries to develop forces designed to operate in cyberspace, and due to the different nature of threats in this domain, the Alliance will need to develop the concept of active defence. Member states' reconnaissance capabilities and resources, as well as ways to prevent hostile activity, will be key here. Therefore, the actions of states such as Poland, which are already declaring their willingness to develop offensive capabilities and transfer them to the needs of the Alliance, will be important. The more states make such declarations, the more the credibility of Allied deterrence and defence.

The growing number and scale of such threats also require increased inter-allied counter-intelligence cooperation. Cooperation with partners such as the EU will remain important, including the further development of cooperation of cyber-response teams and in areas including training, research, and exercises. It will also be important to maintain cooperation with major technology companies that are actively supporting NATO and member states in the fight against cyberthreats.