PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

No. 10/2022, 17 FEBRUARY 2022 © PISM

SPOTLIGHT

The Cyberattack on Ukraine

Oskar Szydłowski, Maciej Zaniewicz

Ukrainian banks and government websites have become the target of a massive cyberattack, the source of which is believed to have been Russia. Further Russian cyberattacks are very likely, including on Ukraine's critical infrastructure. NATO countries are exposed to similar threats.

How did the attack proceed?

The cyberattack began in the afternoon of 15 February and continued for the next two days. It targeted the websites of the Ukrainian Ministry of Defence, the armed forces, and the two largest state-owned banks, PrywatBank and Oszczadbank, which have 26 million customers combined. It was a DDoS-type attack, which consisted of overloading servers with massive, artificial queries. As a result, the attacked government websites, internet banking, and the banks' mobile applications remained inaccessible for several hours. The operation of some payment systems was also hampered. In response, Ukrainian network monitoring services blocked addresses from which the suspicious traffic originated. At the same time, bank customers received fake SMS messages from Polish area codes informing them of technical problems. However, the cyberattack did not pose a threat to deposited funds. Russia was most likely behind the attack, based on a similar attack that took place in Georgia in 2008 and preceded the Russian invasion there. The U.S. also warned that a full-scale Russian invasion of Ukraine would be preceded by cyberattacks.

A spokesman for the Russian president denied the accusations.

What was the purpose of the attack?

If speculation about the Russian source of the 15 February cyberattack is confirmed, it would fit with the objectives of a Russian hybrid war against Ukraine. The aim of this attack was not to do long-term damage or obtain information, but to sow panic in society. The blocking of the Ukrainian army and Ministry of Defence websites was intended to reduce Ukrainians' confidence in the state's defence capabilities. The attack on banks, in turn, was intended to intensify the sense of imminent danger among citizens and undermine confidence in the financial system. The simultaneous use of fake SMS messages was intended to encourage bank customers to withdraw cash *en masse* from ATMs and bank outlets.

Was the objective achieved?

Although the cyberattack conducted on 15 February was the largest DDoS attack in terms of scale, Ukraine has been the target of such operations since 2014. Therefore, the psychological impact of such operations on Ukrainian society is limited. Efficient communication about the incident from banks and the quick restoration of websites and payment systems prevented the spread of panic. It was possible to avert, among other things, a massive withdrawal of cash from banks. In addition, the U.S. has offered help to Ukraine to combat similar attacks, which will increase the security of Ukraine's cyberspace. However, Russian hackers have probably already infiltrated Ukraine's critical infrastructure. This could be used to launch a cyberattack on, for example, the Ukrainian electricity grid. Russian hackers mounted a similar attack in December 2016, depriving one-fifth of Kyiv of electricity, and the year before, affecting more than 200,000 Ukrainians.

What have Poland and NATO learnt from the attacks?

The risk of similar attacks on Poland and NATO countries has increased significantly. In order to counter threats in cyberspace, the first alert level, ALFA-CRP, became effective in Poland on 15 February this year. Poland may also consider testing existing mechanisms for detecting and countering threats in the sphere of cyberspace, as well as the infrastructure's resilience to overload. This should

concern both state institutions and large private entities, especially those operating in key sectors such as energy or banking. At the same time, in response to the growing number of cyberattacks, it would be beneficial to increase spending on cybersecurity. It would also be advisable for Poland to actively participate in the exchange of information and broader cooperation on cyber security within NATO and with partner countries, including Ukraine. It would be beneficial, in the context of preventing similar attacks, to strengthen NATO's messaging in response to breaches in the digital sphere.