PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BULLETIN

No. 175 (1246), 21 December 2018 © PISM

US Electoral System Infrastructure: Threats and Protection Against Russian Interference

Andrzej Dąbrowski

Russia's interference in the 2016 U.S. elections highlighted the vulnerability of American society and the political and electoral system to hard and soft cyberattacks. Despite preventive measures being voted on by Congress and efforts by the social media industry, it has been impossible to eliminate the flaws in electoral infrastructure and social media, which were seen again in this year's "midterm" elections. These factors will affect future elections and the U.S. in time will probably intensify its efforts to prevent attacks and manipulation attempts. This experience could become instrumental for Poland in securing its own electoral process.

Key threats to the U.S. electoral process include not only faulty technical infrastructure, such as systems for collecting and processing voter data or electronic voting machines, but above all, the vulnerability of public opinion to manipulation by foreign entities. These phenomena were recorded for the first time on a large scale during the 2016 elections. The latest major elections (the "midterms") held in November 2018 showed that the problems with infrastructure and the influence of foreign entities remain.

Threats to Electoral Infrastructure. The procedure for voting in general elections is regulated by the Help America Vote (HAVA) Act of 2002. HAVA was supposed to reform the outdated vote-counting system based on perforated cards. For this, HAVA established the Election Assistance Commission (EAC). According to HAVA, the states are required to create computerised registers of voters and use either machines that scan voting cards or utilize touchscreen technology. In the midterm elections in November, some obsolete devices counting the votes failed, making it difficult for voters in many states to cast ballots (including in Florida, New York, and Georgia). This led to a re-count of votes in the Florida Senate race. A separate problem is the threat of vote-counting-software infiltration. Before the 2016 election, Russian hackers managed to breach the security of one company (VR Systems) providing software of this type. The hackers gained partial access to the electoral systems and voter registries in at least 21 states. In 2017, it was also revealed that voting machines used in several states contained key components produced in China and that one of the companies involved in the production of election software was co-financed by a fund controlled by Russian oligarch Vladimir Potanin, who is on the list of sanctioned individuals. Last year, federal authorities decided to remove software made by Russian company Kaspersky from the government's computers, citing a threat to the integrity of government security systems. While it is true that the EAC investigates the security measures used by software providers, it does so only by request of the states, which are not obligated to use the certified systems.

A separate threat to the electoral process is false content on the internet. Social media networks, despite the experiences of the 2016 election campaign, remain vulnerable to the proliferation of targeted misinformation. As in 2016, before the November midterms, inaccurate information was disseminated on social media using fictitious accounts.

Actions by Congress and the Administration. In May 2017, U.S. President Donald Trump signed a cybersecurity executive order and in September 2018, the administration published the first cybersecurity strategy since 2003. These documents do not address the issue of protecting electoral infrastructure. The president's national security advisor, John Bolton, also terminated the post of cybersecurity coordinator, whose task was to coordinate strategy regarding the protection of electoral processes. However, in September this year, President Trump issued an executive order allowing the administration to impose sanctions on foreign entities that, according to U.S. intelligence services, "tried to interfere in the elections and undermine public confidence in the electoral process". This October, the Cyber Command responsible for conducting activities in cyberspace within the Department of Defense, carried out an offensive operation against Russian hackers. It was the first-ever American operation in cyberspace aimed against foreign state actors and was intended at preventing an attempt to influence the election.

Congress also took action to secure the elections, allocating in March this year $380 million for modernisation of electoral infrastructure, including conducting of audits of election procedures and systems, purchase of modern voting machines, and new and secured computer election software. Congress also began working on the Secure Elections Act (SEA), according to which the Department of Homeland Security (DHS) would become the central institution responsible for securing elections. DHS could cooperate with intelligence agencies in identifying threats and coordinating actions with state bodies in the event of an attack on electoral infrastructure. Under SEA, state officials responsible for conducting elections would gain access to classified information, which has so far been a problem in establishing cooperation between state authorities and the intelligence community. Despite bipartisan support in Congress, work on the bill continues.

Public Opinion at Risk. According to the U.S. intelligence community (FBI, CIA, NSA), most of Russia's actions aimed at influencing the 2016 elections took place on the internet. Under public pressure, which accused social media of a lack of control over published content, and out of fear of decreasing user trust and stock value, the authorities of platforms such as Facebook and Twitter began to take action to counter propaganda, disinformation, and verifiably false information. Facebook has refined algorithms that make it difficult to send unsolicited information, forced re-verification of accounts that publish false information, and created tools to report suspicious content to administrators. Facebook also has begun cooperating with the governments of countries from which false information originates. Twitter and Facebook, in cooperation with state electoral commissions also deleted a large number of accounts spreading disinformation.

In 2018 alone, Facebook deleted 652 fake accounts focused on disseminating political and social content. Among them, at least 32 showed similar activity as those associated with the Russian Internet Research Agency, the main organisation responsible for spreading disinformation on behalf of the Russian authorities. Facebook also admitted that it has identified and removed over 300 accounts related to Iran that were able to collect about 800,000 followers since 2011. In September, major social media companies announced a plan to combat false information in the U.S. and the European Union.

Conclusions. The U.S. may be interested in deepening cooperation with allies in the area of protecting electoral infrastructure and fighting disinformation. NATO member states, especially those located on the Eastern Flank, should take into account cyberthreats and disinformation as significant risks to their security environment. It is in Poland's interest to use the American experience to combat misinformation and secure Poland's own electoral infrastructure.

Despite the intelligence community's proof of Russian interference in the 2016 elections and attempts to influence the voting results again in 2018, Congress and the administration have not yet taken sufficient measures to protect electoral infrastructure. Part of this stems from the constitutional principle of protecting freedom of expression, and thus, the American authorities should not influence content published on the internet. However, under heavy public scrutiny, Facebook and Twitter began to introduce further mechanisms limiting the flow of false information. U.S.-based social media industry, under the influence of the American government and public opinion, will most likely change the mechanics and rules for publishing content on such websites. Having global outreach, they will be able to influence the shape and quality of public debate, including in NATO member states.