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

BULLETIN

No. 67 (1313), 23 May 2019 © PISM

The Lithuanian Model in the Fight against Disinformation

Kinga Raś

To counter Russian disinformation and cyberattacks, Lithuania has adapted its administrative structures and modified national legislation. At the same time, it aims to mobilise the other countries of the European Union to systemically counteract the use of fake news to manipulate public opinion. Poland, which is also exposed to Russian disinformation campaigns, can take advantage of the Lithuanian experience.

Goals and Methods of the Russian Activities. Disinformation inspired by Russia is aimed at interfering in the social and political processes of other countries. It takes the form of intentional actions to manipulate public opinion. Since November 2015, the EU vs Disinfo team, operating under the East StratCom Task Force, has identified more than 5,000 cases of disinformation in Europe that favours Russian interests.

Currently, Russian activity targeted on Lithuania focuses on important strategic matters and publicly sensitive areas such as historical memory, and social and economic issues (including those related to the energy sector). In the broader context, the use of disinformation reflects Russia's long-term interests and aspiration to maintain control and influence over the information space in post-Soviet states.

Russia wants, above all, to undermine public confidence in Lithuania's defence and security policy. This is confirmed by official reports by the Lithuanian intelligence and security services, which emphasize that although in 2018 the number of cases of false information about NATO's military presence in Lithuania decreased, Russia maintained a steady message against the Alliance and the Lithuanian armed forces.

The disinformation activities are often paired with cyberattacks, such as the intentional spread of malware to computer networks of state institutions, to steal sensitive data. For example, in 2018, after a hack of the systems of television channel TV3, false information about the sexual orientation of Defence Minister Raimundas Karoblis was disseminated. The message, along with a link and an infected file, was forwarded via e-mail and disseminated to media and state institutions.

At the same time, Russia is actively involved in intelligence activities (cyber-espionage). It has conducted this activity, among others, through the spread of the "Agent.btz" or "Snake" viruses. Their latest versions have been detected in data-processing systems and Lithuanian state institutions. The attacks are carried out by, among others, APT28, a hacker group directly connected to Russian intelligence and whose activity has been identified in the Lithuanian cyberspace.

Lithuania's Methods of Fighting Disinformation. Lithuania, with its historical background, geographical proximity, and the presence of the Russian minority (about 5%), is a country greatly exposed to Russian disinformation activities. These clearly intensified after Russia's aggression on Ukraine in 2014. One of the reasons for this was Lithuania's policy stances that put it amongst the group of states most principled in opposing Russia's aggressive actions in the region. Lithuania also has indirectly supported social circles in Russia critical of the Russian authorities, for example, after the protests of December 2011. As a result, Lithuania is a strong advocate of the sanctions on Russia despite the costs to itself, especially in the

economic dimension. In addition, the Russian authorities continue to perceive Lithuania (and other Baltic states) as part of a zone of Russia's privileged interest.

In response to the disinformation attempts, Lithuania takes action in several dimensions. For example, it has modified its management model for the national cybersecurity system. It assumes the cooperation of state bodies, including the uniformed services, as well as institutions and entities with critical infrastructure (such as energy companies). For this purpose, in 2015, the National Cybersecurity Centre (NCC) was established, and in 2017, the country's law on cybersecurity was amended to, among others, centralise information-security management and to integrate the monitoring of national electronic communications networks.

Lithuania is also trying to adapt existing procedures to meet the new threats by enabling and facilitating the identification and detection of disinformation and countering it. A regulation allowing authorised state bodies (including the NCC) to temporarily block the servers of an entity being used in a cyberattack or to spread fake news.

The Lithuanian authorities also have attempted to limit the influence of Russian media in the Lithuanian public space. They have blocked, temporarily, the possibility of broadcasting Russian television in Lithuania (although it is still available on the internet). In April, the Lithuanian parliament voted in amendments that will allow the Lithuanian Committee on Television and Radio Broadcasting (LRTK) to quickly stop television channels from broadcasting in the event of a threat to national security.

The Lithuanian authorities also strive to increase public awareness of the threats. The high level of competence and broad administrative powers are not enough to fight disinformation, which is why bottom-up initiatives, such as the "movement of elves" is very helpful in this case. This group consists mainly of Lithuanian volunteers who are focused on identifying and combating the Russian trolls. Their main task is to expose fake online accounts to prevent the spread of false information. To assist with this task, the platform Demaskuok.lt was established, bringing together representatives of state institutions as well as journalists and IT professionals.

Tangible proof of the effectiveness of Lithuania's actions is the growing number of unmasked fake news and false accounts (which are subsequently blocked). This was confirmed also by the rapid action against German sporting goods maker Adidas, which, under scrutiny from the public and Lithuanian diplomacy, withdrew a jubilee collection commemorating USSR sports clothing.

Conclusions and Perspectives. The mechanisms used by Russia against Lithuania are also used against other EU and NATO countries (e.g., Germany or Poland). The coordinated approach of the Lithuanian authorities to the problem of disinformation turns out to be an effective recipe to counter the Russian actions. It is supported by organisational and institutional solutions, as well as by a high level of public awareness and debate.

Lithuanian experts signalled an increase in Russian disinformation activity in connection with European Parliament elections and called for closer cooperation between the Member States, media, and information companies operating in the EU. Here again, the Lithuanian example can be an effective model in the fight against disinformation.

Poland and Lithuania's joint actions to strengthen energy and military security will be one of the main and more prominent targets of Russian disinformation. It can be expected that Polish and Lithuanian efforts to strengthen NATO's Eastern Flank and increase the U.S. military presence in the region will be subject to Russian disinformation and cyberattacks. The cooperation between Poland and Lithuania in the energy sector also will remain a target, especially since both countries not only oppose the construction of Nord Stream 2 but are implementing projects themselves to increase their independence from Russian energy supplies by expanding their own gas terminals or interconnector gas connections (GIPL). For Poland, not only is the Lithuanian experience of integrating countering disinformation into the wider context of cybersecurity useful but also its centralised organisational solutions and procedures in case of cyberattack.

The common fight against disinformation offers the chance to increase cooperation at the institutional level and among IT experts and journalists, for example, through special training workshops devoted to the analysis of content and disclosure of disinformation. Poland may also strengthen cooperation within the EU's Cyber Rapid Response Teams (CRRTs) and support Lithuania in implementing the "cyber Schengen" initiative. In practice, this would improve the response to cyberattacks, including by allowing fast data and information exchange. Lithuania emphasizes that the EU could more effectively support countries in its neighbourhood, including Ukraine, in strengthening cybersecurity and combating disinformation.