Open Access Repository
www.ssoar.info

Russian Information Warfare: The Case of Poland

Brzeski, Jessica

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Brzeski, J. (2022). Russian Information Warfare: The Case of Poland. *Russian Analytical Digest*, 282, 6-8. https://doi.org/10.3929/ethz-b-000541999

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY-NC-ND Lizenz (Namensnennung-Nicht-kommerziell-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

Terms of use:
This document is made available under a CC BY-NC-ND Licence (Attribution-Non Comercial-NoDerivatives). For more Information see:
https://creativecommons.org/licenses/by-nc-nd/4.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

Diese Version ist zitierbar unter / This version is citable under:
https://nbn-resolving.org/urn:nbn:de:0168-ssoar-86988-4

Russian Information Warfare: The Case of Poland

By Jessica Brzeski (George Washington University)

DOI: 10.3929/ethz-b-000541999

Abstract

Poland presents an interesting case study for Russian information warfare, as Russia's strategies and methods carry deeper meanings given the long history of antagonism between the two countries. Polish strategies to counter Russian information warfare have been much more effective than those of other countries that have fallen victim to this war tactic. In Poland, the Law and Justice Party has been tightening control over the domestic political space and adding new physical structures—such as cybersecurity hardware, surveillance mechanisms, and new federal agencies—that have contributed to its efforts to combat Russian information warfare. At the same time, however, these methods have undermined the rule of law within Poland.

One of the greatest emerging threats to Polish national security over the past decade has been the increasing use of Russian information warfare, which aims to create instability by widening political and social divides both domestically and internationally. Given the nation's long history with Russia, Poland represents a significant case study of Russian information warfare. Over the last several decades, Poland has transformed from a satellite state of the USSR into an independent state that has joined the most important institutions of the liberal international order: the EU and NATO. These accessions have further strained Poland's already difficult relationship with Russia. Such hard feelings leave space for Russian information warfare to manifest in strategic ways and through various venues. However, the governing party in Poland, Law and Justice, has sought to combat Russian information warfare even as it works to undermine the rule of law domestically. This case study seeks to tally the effective measures Poland has taken to combat Russian information warfare while calculating the domestic costs.

A Long-Standing Contested Relationship

As a former satellite state of the USSR, Poland suffered under Soviet occupation for decades, fueling negative popular sentiments toward Russia. Once the USSR fell, Poland regained real independence for the first time in almost two centuries. The main objective of the newly formed Polish government was to create a foreign policy that protected this independence. Integration into the international liberal order and further promotion of democracy became the two pillars of foreign policy in newly independent Poland (Kacewicz and Wenerski 2017, pg, 13). In order to further these two goals, the new government sought to join the European Union (EU) and the North Atlantic Treaty Organization (NATO). These two institutions shape the way Poland approaches Russian information warfare.

As a NATO member state, Poland must bring its domestic laws into line with the international organization, which has resulted in the strengthening of domestic security measures focused on information security (Kogut et al. 2021, p. 70). In addition, NATO relies on member states to contribute to combating information warfare. One example of this can be found in the creation of the Center of Excellence NATO Cooperative Cyber Defense (CCDCOE), which promotes the implementation of new policies within the cybersecurity realm (Colesniuc 2013, p. 127).

Although the relationship has been contested in recent years, Poland's accession to the EU has provided the country with critical resources to further develop the legal and physical structures needed to combat Russian propaganda. Like NATO, the EU seeks to integrate the security infrastructures and information systems of every member state into a cohesive whole. This approach allows for member states like Poland to further strengthen the structures that support information security with direct resource allocation (Kogut et al. 2021, p. 75). A specific example comes from the creation of the Network of Computer Security Incident Response Teams: each member state must house a response group that works with the broader network of groups to secure information systems in member states and within the EU as a whole (European Agency for Cybersecurity 2022).

Russia's Tools and Strategies

Russia claims that the West was the "first mover" when it comes to using information warfare to gain political and military advantage. The Russian leadership considers the expansion of NATO, a decade of color revolutions, and a deeply integrated EU to be threats (Śliwa and Antczak 2018, p. 23). In response, Russia has devised a number of approaches that focus on Poland. These include:

- Cybersecurity Threats: Poland has witnessed a steady increase in attacks on hardware, such as govern-

ment servers, since the invasion of Ukraine began (Reuters 2022).
- Cyber Hacking: Efforts to leak data and critical information, with a view to adversely affecting the nation, include a government-wide leak in June 2021 (AP News 2021).
- Media / Online Warfare: Campaigns seeking to create countering narratives to inflame divisions, such as an extensive anti-NATO campaign (The Guardian 2020).
- Historical Memory Warfare: Altering or erasing historical facts with false narratives (Sukhankin 2020).

These four tactics define Russian information warfare against Poland. Russian propagandists use different tactics for different audiences; in the case of Poland, the tactics used are a mix of those seen in Western countries such as the United States (i.e., media/online warfare) and those seen in neighboring countries such as Ukraine (i.e., historical memory warfare). Ultimately, the goal of Russian information warfare in Poland can be summarized as attempting to destabilize national security by impugning information security through various outlets that call into question historical, political, and social aspects of Polish statehood.

Impact of Russian Information Warfare in Poland

Russian information warfare has negatively affected Poland in various ways, ranging from intelligence leaks to the physical destruction of historical landmarks. Historically speaking, Poland has ties with Russia, but these are less significant than those Russia has with Ukraine, making the desired outcome of Russian information warfare different. Poland and Russia have frequently fought over various issues, and given the significant technological developments of the past two decades, this conflict has spilled into the field of information security. Polish identity has also changed significantly since the fall of the USSR, with the country's accession to the EU and NATO allowing for Russian information warfare to be dispersed within Poland in ways more similar to the countries that uphold these pillars of the liberal international order (Čižik 2017, pg.15). Thus, Poland has fallen victim to Russian information warfare in a blend of ways, as both a historical adversary and a now-Westernized nation. The most immediate impacts of Russian information warfare on Poland have been:

- Weakening Hardware Network: Poland's information technology and computer networks have been compromised due to their general accessibility and openness, making it possible for hackers to leak government information (Chojnacki 2012, p. 56–57).
- Creating Social Instability: Russia's use of media/online warfare and historical memory warfare further support certain narratives of the Law and Justice Party, which itself benefits from inflaming political divisions within Poland (Lucas and Pomeranzev 2016, p. 30).
- Intensifying Multilateral Tensions: The inflammatory domestic effect of Russian information warfare spills over into Poland's relationships with regional partners such as Ukraine (Belavusau et al. 2021, p. 19–20).

The above impacts have greatly tested the integrity of Poland's internet infrastructure and the population's ability to resist Russian information warfare. Ironically, Poland's ruling Law and Justice Party itself benefits from the anti-Western and anti-liberal narratives propagated by Russian information warfare.

Poland's Response

The Law and Justice Party has played a proactive role in countering Russian propaganda, which has had the effect of undermining the rule of law within the country. Primary counter-tactics to Russian information warfare by Poland include, but are not limited to:

- Tighter Legal Restrictions: The National Security Strategy of 2014, National Anti-Terrorist Programme (NATP) for 2015–2019, and the Strategy for the Development of the National Security System of the Republic of Poland (2022).
- Restricted Access: The Act on Anti-Terrorist Activities of 2016, the creation of the Anti-Terrorist Center, and the Government Center for Security have all increased government surveillance of Polish society.
- Media Curation: The Law and Justice Party has sought to impose media control, including attempting to take down the biggest independent television company in Poland (Discovery+) in 2021.

Conclusion

Overall, Polish measures to counter Russian information warfare have primarily been taken through the legal system and internet hardware. However, the Law and Justice Party has implemented certain legal restrictions that allow it to increase surveillance of the population and clamp down on critical media outlets. Therefore, in the case of Poland, combating Russian information warfare has come at the price of the rule of law.

About the Author

Jessica Brzeski is a graduate student at the Elliott School of International Affairs pursuing her M.A. in International Affairs with a focus on U.S. Foreign Policy and European/Eurasian Affairs. Previously, she earned a B.A. at Loyola

University Chicago in Global and International Studies and French Language, during which she studied abroad in Sydney, Australia, and Paris, France. She has held various positions within the sphere of international relations.

References

- Anon, 2020. Russia-aligned hackers running anti-Nato Fake News Campaign – Report. *The Guardian*. Available at: https://www.theguardian.com/technology/2020/jul/30/russia-aligned-hackers-running-anti-nato-fake-news-campaign-report-poland-lithuania (Accessed March 23, 2022).
- Anon, 2021. CSIRTS network. *ENISA*. Available at: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network (Accessed March 18, 2022).
- Anon, 2021. Polish intelligence agencies link cyberattack to Russia. *AP NEWS*. Available at: https://apnews.com/article/europe-russia-intelligence-agencies-technology-government-and-politics-261df587ec9f93e781be8203a083eea1 (Accessed March 23, 2022).
- Anon, 2022. Poland sees more cyberattacks on government servers, official says. *Reuters*. Available at: https://www.reuters.com/technology/poland-sees-more-cyberattacks-government-servers-official-says-2022-02-25/ (Accessed March 23, 2022).
- Belavusau, U., Gliszczynska-Grabias, A. and Mälksoo, M., 2021. Memory laws and memory wars in Poland, Russia and Ukraine. *Jahrbuch des öffentlichen Rechts, Forthcoming*. 1–22.
- Čižik, Tomáš, 2017. Russian information warfare in central Europe. *Information Warfare–New Security Challenge for Europe. Bratislava: Centre for European and North Atlantic Affairs*. 8–34.
- Chojnacki, Włodzimierz, 2012. Future cyberspace war and its impact on Polish Armed Forces. *Zeszyty Naukowe/ Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki*. 53–61.
- Gasztold, A. & Gasztold, P., 2020. The Polish Counterterrorism System and Hybrid Warfare Threats. *Terrorism and political violence*. 1–18.
- Kacewicz, Michał and Łukasz Wenerski, 2017. Russian soft power in Poland – The Kremlin and pro-Russian organizations. *Political Capital*. 1–58.
- Kogut, B. et al., 2021. Information Security in Poland and in the European Union: Administrative and Legal Conditions. *European Research Studies Journal XXIV.* (2). 68–77.
- Lucas, Edward, and Peter Pomeranzev, 2016. Winning the information war. *Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. Washington: The Center for European Policy Analysis.* 1–66.
- Sukhankin, Sergey, 2020. Russia's "Memory wars", Poland, and the forthcoming 75th Victory Day. *ICDS*. Available at: https://icds.ee/en/russias-memory-wars-poland-and-the-forthcoming-75th-victory-day/ (Accessed March 23, 2022).
- Śliwa, Zdzisław, and Anna Antczak, 2018. Military Domain as a Component of Information Warfare. *Kaitseväe Akadeemia*. 16–17.
- Świątkowska, Joanna, 2017. Cybersecurity Statecraft in Europe: A Case Study of Poland. *Georgetown journal of international affairs*. 18 (3), 83–94.