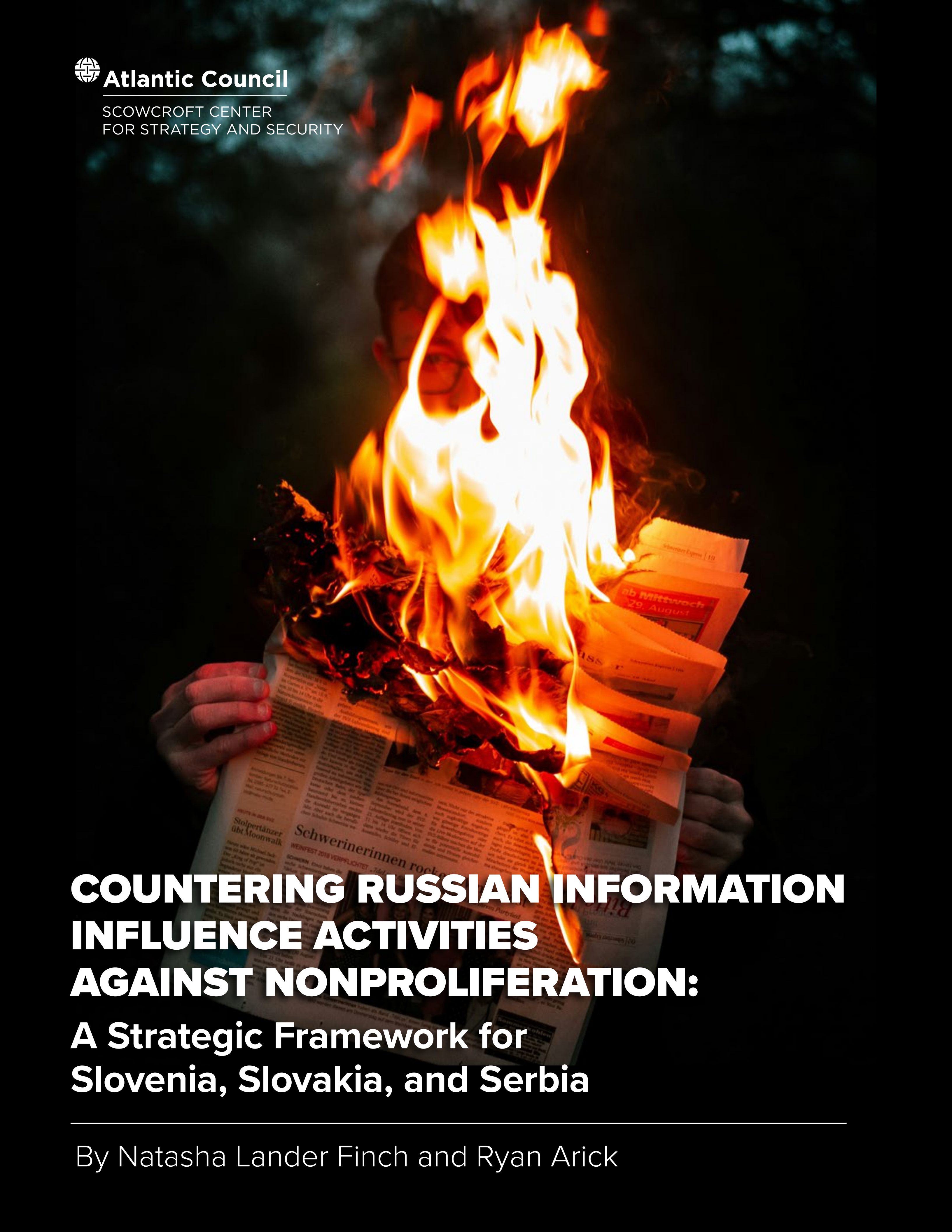
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY



COUNTERING RUSSIAN INFORMATION INFLUENCE ACTIVITIES AGAINST NONPROLIFERATION:

A Strategic Framework for Slovenia, Slovakia, and Serbia

By Natasha Lander Finch and Ryan Arick

Atlantic Council

COVER: An individual holds burning media, representing disinformation's deleterious impact on society, Dec. 1, 2018. Photo by Julius Drost @juliusdrost.

This report was written and published in accordance with the Atlantic Council policy on intellectual independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

ISBN-13: 978-1-61977-343-1

September 2024

Atlantic Council, 1030 15th Street NW, 12th Floor, Washington, DC 20005

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

COUNTERING RUSSIAN INFORMATION INFLUENCE ACTIVITIES AGAINST NONPROLIFERATION:

A Strategic Framework for Slovenia, Slovakia, and Serbia

Natasha Lander Finch

Senior Fellow, Transatlantic Security Initiative, Scowcroft Center for Strategy and Security, Atlantic Council

Ryan Arick

Associate Director, Transatlantic Security Initiative, Scowcroft Center for Strategy and Security, Atlantic Council

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Scowcroft Center's **Transatlantic Security Initiative** brings together top policymakers, government and military officials, business leaders, and senior experts from Europe and North America to share insights and develop innovative approaches to the key challenges facing NATO and the transatlantic community.

Acknowledgments

The research team thanks the US Department of State Bureau of International Security and Nonproliferation's Office of Cooperative Threat Reduction for their strategic guidance and overall support throughout the project. Special thanks go to the wide range of stakeholders in Slovakia, Slovenia, and Serbia who contributed their invaluable insights to our workshops and participated in other contexts to enrich the analysis.

We would also like to acknowledge Sarah Jacobs Gamberini and Amanda Moodie of the National Defense University’s Center for the Study of Weapons of Mass Destruction for their critical contributions to our workshops in Slovakia and Serbia. Sarah Jacobs Gamberini and the Atlantic Council's Eto Buziashvili from the Digital Forensic Research Laboratory also provided valuable peer reviews that improved our strategic framework. Within the Atlantic Council, we recognize the critical contributions of Leah Scheunemann, Zelma Sergejeva, and Kristen Taylor for their project management, research, and analytical support; Dr. Matthew Kroenig and Christopher Skaluba for their oversight of the project; and Gretchen Ehle, Nicholas O’Connell, Caroline Simpson, and Ursula Murdoch for their operational guidance and assistance.

This report is intended to live up to General Brent Scowcroft’s standard for rigorous, relevant, and nonpartisan analysis on national security issues. The Atlantic Council’s Scowcroft Center for Strategy and Security works to continue his nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The views expressed herein are those of the authors and do not necessarily reflect the official policy or position of the Atlantic Council, the Office of Cooperative Threat Reduction, the Bureau of International Security and Nonproliferation, the US Department of State, or the US government.

Table of Contents

About the report

Russia has a long history of using false and unfounded narratives around chemical, biological, radiological, and nuclear (CBRN) weapons to undermine European security. These information influence activities (IIA) have intensified in recent years. Russia's tactics, which include disinformation, misinformation, malinformation, and propaganda as defined in Chapter 1, consist of false claims that US cooperative nonproliferation efforts are a front for developing CBRN weapons. Through its IIA, Russia also has circulated false narratives that attack transatlantic cooperation meant to encourage nonproliferation efforts.

In this context, the Atlantic Council's Transatlantic Security Initiative (TSI) in the Scowcroft Center for Strategy and Security conducted a cooperative research project with the US Department of State's Office of Cooperative Threat Reduction (CTR) within the Bureau of International Security and Nonproliferation (ISN) to better understand the extent of Russia's nonproliferation-related IIA in three European countries: Slovenia, Slovakia, and Serbia. This project focused on how to identify Russian IIA and coordinate a multistakeholder response to counter these tactics, which can ultimately strengthen nonproliferation norms and regimes.

This report documents the research and analysis conducted for this project, which TSI led from October 2022 to December 2023.

CHAPTER 1:
Russian information influence activities against nonproliferation

Russia relies on a range of malign tactics to complement its conventional warfare capabilities, including information manipulation. Throughout Europe, Russia creates or amplifies false narratives that support the Kremlin's ultimate geopolitical goals: undermining unity and security in Europe and abroad.[1] These narratives attempt to evoke emotional and psychological responses from the public with the broader aim of amplifying polarization, undermining democracy, and weakening support for international norms and institutions.

Russia's information manipulation networks—which consist of official spokespeople, state-run media, proxy websites, social media, and other entities—aim to exploit fears and sensationalize threats through a range of information influence activities (IIA), a term we use to capture the multifaceted nature of information manipulation. IIA includes disinformation, misinformation, malinformation, and propaganda (see definitions in Table 1 and a full list of key terms in Appendix I).

Russia has perfected its use of information influence activities to achieve its geopolitical goals. Through its information networks, Russia attempts to inject narratives favorable to the Kremlin.[2] Russia's tactics include saturating the information space, continuously sharing false and misleading information, and amplifying preexisting narratives.[3] These narratives try to damage the credibility of political institutions and instill feelings of distrust, confusion, and fear.[4]

Historically, Russia has targeted states around the world with information warfare. In Europe, topics such as inflation, migration, and energy shortages are regular targets of Russian disinformation.[5] To amplify its IIA, Russia uses a broad network of fake pages, social media accounts, and private messaging

Table 1: Definitions of Key Terms Included in Information Influence Activities

DISINFORMATION
False or misleading information that is intentionally created, presented, and disseminated to deceive or mislead the public.

MISINFORMATION
False or misleading information that is spread unintentionally.

MALINFORMATION
Information built around truth and facts, but taken out of context or otherwise misleading to inflict harm.

PROPAGANDA
Information, especially of a biased or misleading nature, used to promote or publicize a particular political cause or point of view.

Sources: Atlantic Council, https://www.atlanticcouncil.org/issue/disinformation/; James Pammen, A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference, NATO Strategic Communications Center of Excellence, November 2022; Dean Jackson, "Distinguishing Disinformation From Propaganda, Misinformation, and 'Fake News,' " National Endowment for Democracy and International Forum for Democratic Studies, n.d.; "How to Identify Misinformation, Disinformation, and Malinformation," Canadian Centre for Cyber Security, ITSAP.00.300, February 2022; and "Understanding Propaganda and Disinformation," European Parliament, November 2015.

[1] Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," RAND Corporation, 2016, https://www.rand.org/pubs/perspectives/PE198.html.

[2] Sarah Jacobs Gamberini and Justin Anderson, "Russian and Other (Dis)Information Undermining WMD Arms Control: Considerations for NATO," Speech before NATO Committee on Proliferation, July 12, 2022.

[3] Sarah Jacobs Gamberini, "Social Media Weaponization: The Biohazard of Russian Disinformation Campaigns," *Joint Force Quarterly* 99 (November 19, 2020), https://wmdcenter.ndu.edu/Publications/Publication-View/Article/2422660/social-media-weaponization-the-biohazard-of-russian-disinformation-campaigns/; "Russia's Top Five Persistent Disinformation Narratives," Office of the Spokesperson, US Department of State, January 20, 2022, https://www.state.gov/russias-top-five-persistent-disinformation-narratives/.

[4] "Russia's Top Five Persistent Disinformation Narratives," US Department of State.

[5] Paul and Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model."

groups. However, authentic accounts—including many within the countries that Russia is targeting—are often just as involved in these campaigns, whether they know it or not.[6] Media outlets within targeted countries frequently pick up, repackage, and amplify Russian narratives, furthering the impact and resonance of the Kremlin's influence.[7]

Russia's reinvasion of Ukraine in 2022 featured IIA as a prominent Kremlin tactic to augment Putin's conventional war. Russia's methods included frequent narratives designed to target nonproliferation norms and regimes, which continues a pattern the Soviets followed during the Cold War. These tactics mirror previous Soviet patterns of employing "active measures," or covert propaganda and influence operations to project control surrounding CBRN weapons and erode trust in democratic institutions.[8] As part of its active measures campaign, the Soviet Union made false allegations that the United States had developed and used biological weapons.[9] After the dissolution of the Soviet Union, Russia targeted the activities of the US Cooperative Threat Reduction (CTR) program by alleging the US government employed the CTR program as a cover to develop CBRN weapons throughout Europe and Eurasia, even though the CTR program was developed to curb the possible spread of weapons of mass destruction (WMD) throughout the region after the Soviet Union's collapse and included Russian participation until 2014.[10]

Russia continues to spread unfounded allegations that ongoing partnerships between the United States and other countries are fronts for biological weapons development programs.[11] Russia intensified its use of propaganda and false claims that argued Ukraine was engaged in developing biological weapons to be used against Russian civilians.[12] These efforts damage the credibility of the work conducted in legitimate research facilities, undermine public trust in these institutions, and potentially jeopardize the safety of laboratory staff.

After the re-invasion of Ukraine, Russia intensified its influence operations across Europe to sway public opinion in its favor. Many of Russia's claims included that Moscow is seeking peace, Ukraine is inherently aggressive, the West instigated the war, and the European Union (EU) and NATO are to blame for increased tensions in the region.[13] Russia complements its conventional war in Ukraine with information warfare to fracture Western support for Ukraine, and shore up global support from nonaligned countries within multilateral organizations.[14]

IMPACT OF RUSSIAN INFORMATION INFLUENCE ACTIVITIES ON NONPROLIFERATION NORMS

Russia's manipulation of the information space to erode support for nonproliferation includes continued support

[6] Elina Treyger, Joe Cheravitch, and Raphael S. Cohen, "Russian Disinformation Efforts on Social Media," RAND Corporation, 2022, https://www.rand.org/pubs/research_reports/RR4373z2.html.

[7] For example, see: Goran Georgiev and Ruslan Stefanov, "Russian Disinformation in the Balkans: Predating the Invasion?," *Euractiv*, March 21, 2023, https://www.euractiv.com/section/enlargement/opinion/russian-disinformation-in-the-balkans-predating-the-invasion/; Paul Farhi, "Voice of America Journalists Put on Leave After 'Russian Propaganda' Accusations," *Washington Post*, February 24, 2023, https://www.washingtonpost.com/media/2023/02/24/voice-of-america-russian-propaganda/; and Tony Wesolowsky, "Barred in EU, Could Russia's RT Find a Home in Serbia?" *Radio Free Europe/Radio Liberty*, July 21, 2022, https://www.rferl.org/a/serbia-rt-russia-propaganda/31954082.html.

[8] These tactics also include espionage, assassinations, and other forms of political sabotage. For more on the Soviet Union's active measures, see: Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: MacMillan Publishers, 2020); Megan Ward, Shannon Pierson, and Jessica Beyer, "Formative Battles: Cold War Disinformation Campaigns and Mitigation Strategies," Wilson Center, August 2019, https://www.wilsoncenter.org/publication/formative-battles-cold-war-disinformation-campaigns-and-mitigation-strategies; and Nicholas J. Cull et al., *Soviet Subversion, Disinformation, and Propaganda: How the West Fought Against It*, LSE Consulting with Arena for Google's Jigsaw, London School of Economics and Political Science, October 2017, https://www.lse.ac.uk/business/consulting/reports/soviet-subversion-disinformation-and-propaganda-how-the-west-fought-against-it.

[9] "The Kremlin's Never-Ending Attempt to Spread Disinformation About Biological Weapons," Global Engagement Center, US Department of State, March 14, 2023, https://www.state.gov/the-kremlins-never-ending-attempt-to-spread-disinformation-about-biological-weapons/.

[10] For example, see: Milton Leitenberg, "False Allegations of Biological-Weapons Use from Putin's Russia," *Nonproliferation Review* 27, nos. 4-6 [Special Section: Chemical and Biological Warfare] (2021): 425-442, https://www.tandfonline.com/doi/full/10.1080/10736700.2021.1964755; "Debunking Russia's Chemical, Biological, Radiological, and Nuclear Disinformation," US Embassy and Consulates in Indonesia, March 16, 2022, https://id.usembassy.gov/debunking-russias-chemical-biological-radiological-and-nuclear-disinformation/; and "The History of Cooperative Threat Reduction," Defense Threat Reduction Agency, accessed December 22, 2023, https://www.dtra.mil/Portals/61/Documents/History%20of%20CTR.pdf?ver=2019-04-25-140558-733.

[11] Natasha Lander Finch, "How NATO Can Curb Russia's Chemical Weapons Threat," *New Atlanticist* (blog), Atlantic Council, April 8, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/how-nato-can-curb-russias-chemical-weapons-threat/.

[12] Douglas Selvage, "Moscow, 'Bioweapons,' and Ukraine: From Cold War 'Active Measures' to Putin's War Propaganda," Wilson Center, March 22, 2022, https://www.wilsoncenter.org/blog-post/moscow-bioweapons-and-ukraine-cold-war-active-measures-putins-war-propaganda.

[13] Nika Aleksejeva and Andy Carvin, *Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression Against Ukraine*, Atlantic Council, February 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/.

[14] For example, see: Elina Lange-Ionatamišvili, "Analysis of Russia's Information Campaign Against Ukraine," NATO Strategic Communications Center of Excellence, 2015, https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf; and Vera Bergengruen, "Inside the Kremlin's Year of Ukraine Propaganda," *Time*, February 22, 2023, https://time.com/6257372/russia-ukraine-war-disinformation/.

Russia published false claims of "dirty bombs" being built in Ukraine on state-run media. In reality, the photo evidence was taken from Slovenia. Source: Deutsche Welle/Agency for Radwaste Management of Slovenia

for the Assad regime in Syria through disinformation and misinformation, despite Assad's well-documented history of using chemical weapons against civilian populations in Syria's civil war in the mid-2010s.[15] Russia has also used the information domain to spread false and misleading information related to the Kremlin's targeted assassination attempts with chemical weapons. This included Moscow's attack on Russian dissidents in the United Kingdom (UK), against a former KGB agent and his daughter, as well as on its own territory against prominent dissident Alexei Navalny.[16]

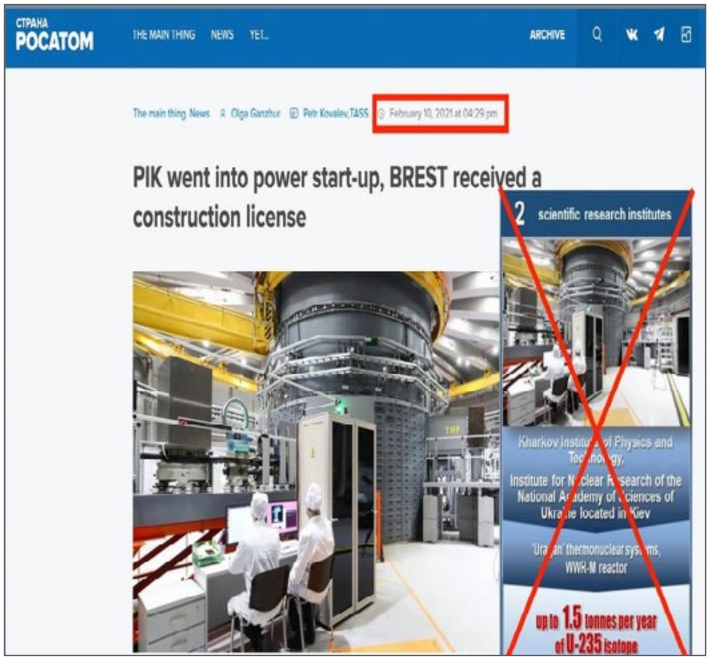
Russia combines information influence activities with disruptive behavior in multilateral institutions, such as the Organization for the Prohibition of Chemical Weapons (OPCW), Biological Weapons Convention (BWC), and the United Nations Security Council (UNSC) to interrupt proceedings, derail procedures, and slow down investigations.[17] Russian diplomats levy false accusations against nations Moscow deems hostile to stymie progress and undermine the authority of these organizations.[18] These actions are not necessarily used to persuade others to accept Russia's arguments, but instead to create doubt

[15] Daryl Kimball and Kelsey Davenport, "Timeline of Syrian Chemical Weapons Activity, 2012-2022," Arms Control Association, accessed June 26, 2024, "https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity#2022"; Dion Nissenbaum and Carol E. Lee, "White House Says Russia Tried to Cover Up Syrian Chemical Attack," Wall Street Journal, April 11, 2017, https://www.wsj.com/articles/white-house-says-russia-tried-to-cover-up-syrian-chemical-attack-1491935440.

[16] Karl Dewey, "Poisonous affairs: Russia's evolving use of poison in covert operations," *The Nonproliferation Review*, Vol. 29, No. 4-6, December 16, 2022, https://www.tandfonline.com/doi/full/10.1080/10736700.2023.2229691; Patrick Reevell, "Before Navalny, A Long History of Russian Poisonings," ABC News, August 26, 2020, https://abcnews.go.com/International/navalny-long-history-russian-poisonings/story?id=72579648.

[17] Related to the OPCW, see: OPCW, "Joint Statement on Russian action in the OPCW with regard to Ukraine," Organization for the Prohibition of Chemical Weapons, 2022, https://www.opcw.org/sites/default/files/documents/2022/11/With%20Co-Sponsors_%20JointStatementonUKR_CSP-27.pdf; Alberto Nardelli, "Russia Sought to Sway Weapons Watchdog Vote Using Disinformation," Bloomberg, December 4, 2023, https://www.bloomberg.com/news/articles/2023-12-04/russia-sought-to-sway-weapons-watchdog-vote-using-disinformation. With respect to the UN Security Council, see "Security Council Rejects Text to Investigate Complaint Concerning Non-Compliance of Biological Weapons Convention by Ukraine, United States," United Nations, November 02, 2022, https://press.un.org/en/2022/15095.doc.htm; Missy Ryan, Adela Suliman, and Maite Fernández Simon, "Russia Accuses U.S. of Supporting a Biological Weapons Program in Ukraine at U.N. Security Council Meeting," Washington Post, March 11, 2022, https://www.washingtonpost.com/world/2022/03/11/un-council-ukraine-russia-chemical-weapons-zelensky/.

[18] Nika Aleksejeva and Andy Carvin, *Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression Against Ukraine*, Atlantic Council, February 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/.



The main thing, News Olga Ganzhur Petr Kovalev,TASS February 10, 2021 at 04:29 pm

PIK went into power start-up, BREST received a construction license

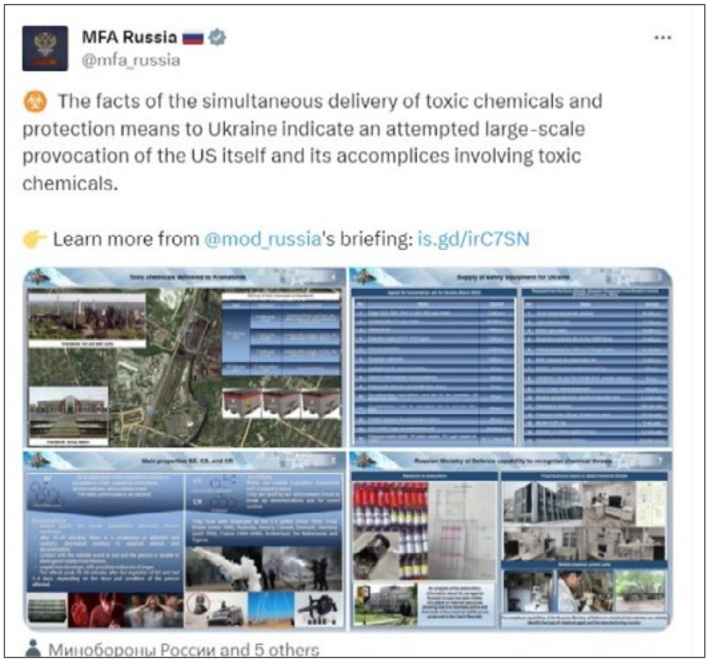
2 scientific research institutes

Kharkov Institute of Physics and Technology,
Institute for Nuclear Research of the National Academy of Sciences of Ukraine located in Kiev

'Uragan' thermonuclear systems,
WWR-M reactor

up to 1.5 tonnes per year of U-235 isotope

Figure 1: Russia published false claims of "dirty bombs" being built in Ukraine on state-run media. In reality, the photo evidence was taken from a Russian reactor. Image: Deutsche Welle, https://www.dw.com/en/fact-check-russias-false-case-for-a-dirty-bomb-in-ukraine/a-63590306.


MFA Russia 🇷🇺
@mfa_russia

The facts of the simultaneous delivery of toxic chemicals and protection means to Ukraine indicate an attempted large-scale provocation of the US itself and its accomplices involving toxic chemicals.

👉 Learn more from @mod_russia's briefing: is.gd/irC7SN

Минобороны России and 5 others

Figure 2: Russia's Foreign Ministry claimed the United States shipped chemicals to Ukraine to be used against Russian soldiers, while only providing a random assortment of graphics taken from other contexts as "evidence." Image: Twitter/strana-rosatom.ru, http://twitter.com/mfa_russia/status/1630683781215526912.

and confusion, undercut the unity and effectiveness of the organizations, and weaken protections of nonproliferation norms and regimes.[19] Russia's allegations include that Ukraine is concocting plans for a potential chemical attack (articulated at the OPCW in 2022),[20] preparing to deploy dirty bombs and nuclear weapons (UN, 2022),[21] and using and developing biological weapons (BWC, 2022).[22]

Russia's false claims weaken accountability and verification measures established to monitor compliance with international treaties that ban CBRN weapons and regulate the legitimate use of technologies that have a dual-purpose capacity to create such weapons.[23] These claims also undermine efforts to strengthen and modernize nonproliferation norms and regimes, especially with respect to emerging technologies. Russia's actions also distract from the Kremlin's own harmful activities and noncompliance with nonproliferation obligations, especially Russia's support for and use of chemical weapons, their sympathy for other regimes that have used CBRN weapons, and their escalatory rhetoric.

[19] Sarah Jacobs Gamberini, "Arms Control in Today's (Dis)Information Environment: Part I," Inkstick Media, May 11, 2021, https://inkstickmedia.com/arms-control-in-todays-disinformation-environment-part-i/.

[20] "Joint Statement on Russian Action in the OPCW with Regard to Ukraine," submitted by fifty-four state parties to the Organization for the Prohibition of Chemical Weapons, prepared for the twenty-seventh session, 2022, https://www.opcw.org/sites/default/files/documents/2022/11/With%20Co-Sponsors_%20JointStatementonUKR_CSP-27.pdf.

[21] Michelle Nichols, "Russia Raises Accusation at U.N. of Ukraine 'Dirty Bomb' Plans," Reuters, October 25, 2022, https://www.reuters.com/world/europe/russia-raises-accusation-un-ukraine-dirty-bomb-plans-2022-10-25/.

[22] For example, see: Leanne Quinn, "U.S., Ukraine Refute Russian Bioweapons Charges," Arms Control Association, October 2022, https://www.armscontrol.org/act/2022-10/news/us-ukraine-refute-russian-bioweapons-charges; Nika Aleksejeva and Andy Carvin, *Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression Against Ukraine*, Atlantic Council, February 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/.

[23] "The Kremlin's Chemical Weapons Disinformation Campaigns," Global Engagement Center, US Department of State, May 2022, https://www.state.gov/wp-content/uploads/2022/05/The-Kremlins-Chemical-Weapons-Disinformation-Campaigns_edit.pdf.

In several posts on state-run media and on social platforms, the Kremlin shared so-called evidence that Ukraine was developing a "dirty bomb," an explosive device that contains radioactive material. However, the photo—depicted in Figure 1—was taken from other websites. In this instance, the photo provided as "evidence" was taken from the Russian state-owned nuclear energy company Rosatom. In Figure 2, Russia claimed the United States was providing toxic chemicals and other CBRN-related materiel to Ukraine, which indicated a "large scale provocation." These kinds of narratives could serve as false flag scenarios for Russia's own potential use of CBRN weapons, which would have severe consequences for nonproliferation norms in Ukraine and more broadly in Europe.

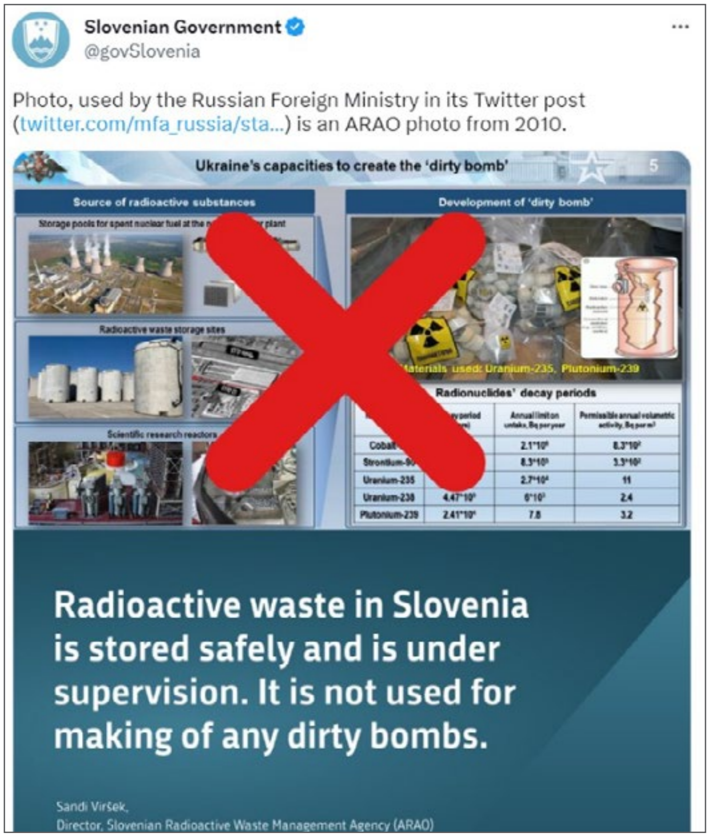
Overall, these tactics serve as tools in Russia's toolbox to discredit and weaken the multilateral institutions and regimes that govern nonproliferation. Russia's persistent IIA erode trust and credibility in nonproliferation, which safeguards the international community from the development and use of CBRN weapons. The effects of Russian IIA are widespread, as evidenced by the experience of three European countries: Slovenia, Slovakia, and Serbia. The following sections provide an overview of each country's recent experience with Russia's false claims associated with nonproliferation and CBRN weapons.

SLOVENIA

Slovenia has been an active target of Russian disinformation and information influence activities. In 2016, Russia claimed NATO would harbor a secret arsenal of nuclear weapons throughout Eastern Europe,[24] including in Slovenia. Russian state media organizations invested millions of dollars in Central and Eastern European countries, such as Slovenia, to influence domestic politics and exacerbate political polarization through state-run media channels, government proxies, and other systems. Many of Slovenia's top proliferators of disinformation and other falsehoods have significant inroads and connections to Russian state-media organizations.[25]

Several websites that maintain strong linkages to Russia and the Kremlin—including RBTH Daily, NewsFront, and Katehon—operate or are available in Slovenia and consistently post dangerous rhetoric on the EU, NATO, and the United States. Russia launched RBTH Daily, a mobile app version of its Russia Beyond service operated by the Russian state news agency that regularly publishes content in Slovenian.[26]

In early 2023, the Russian Ministry of Foreign Affairs claimed on Twitter that Ukraine was secretly building a dirty bomb and


Slovenian Government
@govSlovenia

Photo, used by the Russian Foreign Ministry in its Twitter post (twitter.com/mfa_russia/sta...) is an ARAO photo from 2010.

Ukraine's capacities to create the 'dirty bomb'
5
Source of radioactive substances
Storage pools for spent nuclear fuel at the n... ...r plant
Radioactive waste storage sites
Scientific research reactors
Development of 'dirty bomb'
...aterials used: Uranium-235, Plutonium-239
Radionuclides' decay periods
Annual limit on intake, Bq per year
Permissible annual volumetric activity, Bq per m³
Cobal...
Strontium-9...
Uranium-235
Uranium-238
Plutonium-239
4.47*10⁹
2.41*10⁴
2.1*10⁶
8.3*10⁵
2.7*10⁴
6*10³
7.8
8.3*10²
3.3*10²
11
2.4
3.2

Radioactive waste in Slovenia is stored safely and is under supervision. It is not used for making of any dirty bombs.

Sandi Viršek,
Director, Slovenian Radioactive Waste Management Agency (ARAO)

Figure 3: The Slovenian government's response to Russian disinformation about radioactive weapons being used in Ukraine. ARAO stands for Agency for Radwaste Management, which is responsible for managing all radioactive waste in Slovenia. Image: Twitter/govslovenia, https://twitter.com/govSlovenia/status/1584936237806206976.

[24] Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, August 28, 2016, https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html.

[25] Doman Savič, "Publicly Funded Hate in Slovenia: A Blueprint for Disaster," Heinrich-Böll-Stiftung (foundation), June 7, 2021, https://eu.boell.org/en/2021/06/07/publicly-funded-hate-slovenia-blueprint-disaster.

[26] Paul Stronski and Annie Himes, "Russia's Game in the Balkans," Carnegie Endowment for International Peace, February 6, 2019, https://carnegieendowment.org/2019/02/06/russia-s-game-in-balkans-pub-78235.

included a series of photos as evidence.[27] One of the photos was taken directly from a 2010 public education campaign on the Slovenian Agency for Radioactive Waste's website. In response, the Slovenian government quickly published a statement on its official website and on social media that denied Russia's claims and stressed that nuclear waste was stored safely in the country (see Figure 3).[28] Slovenian government authorities responded to these Russian campaigns and attempts to undermine its credibility with facts, data, and truthful information.[29]

SLOVAKIA

Russia also has frequently targeted Slovakia with IIA. Within Slovakia, pro-Russia propagandists are actively working to discredit Slovakia's allies,[30] including the United States, the EU, and other NATO allies to downplay Russian aggression in Ukraine, deflect blame from historical conflicts, and denigrate responses from across the Alliance. These campaigns also attempt to erode trust in and the credibility of nonproliferation norms and regimes.

For example, in May 2023, Russia spread disinformation in Slovakia regarding an alleged radiation leak as a result of an explosion of the ammunition warehouse in the Ukrainian city of Khmelnytskyi.[31] Through its claims circulated on social media channels and with support from the Russian embassy in Slovakia, the Kremlin attempted to incite fear within targeted communities that there was a significant airborne risk of radiation spilling over into Slovakia from Ukraine.[32]

In 2022, the Russian embassy in Bratislava issued several posts that claimed the United States and Ukraine were developing biological agents. The embassy—which was named by the International Republican Institute's Beacon Project as the most virulent in circulating disinformation across Moscow's network of diplomatic missions—alleged that the United States and Ukraine were developing biological weapons that could target specific ethnic groups, including Slavs.[33]

Similar to Slovenia's experience, the Kremlin injects pro-Russian messaging within Slovakia to amplify its geopolitical goals. One recurring target of Russian information manipulation is the bilateral defense cooperation agreement (DCA) that Slovakia signed with the United States in 2022.[34] After it was signed, Russian operatives began to inject falsified information that the DCA would include the deployment of nuclear weapons in Slovakia.[35]

[27] Ministry of Foreign Affairs of Russia (@MFA_Russia), "Russia Defence Ministry: According to the information at hand, two organizations of Ukraine have been directly ordered to create the so-called #dirtybomb," Twitter (now X), October 24, 2022, https://twitter.com/mfa_russia/status/1584547788335251462; and Sebastijan R. Maček, "Slovenia Inadvertently Dragged into Russian 'Dirty Bomb' Campaign," *Euractiv*, October 27, 2022, https://www.euractiv.com/section/all/short_news/slovenia-inadvertently-dragged-into-russian-dirty-bomb-campaign.

[28] For example, see: Slovenian government (@govSlovenia), "Photo, used by the Russian Foreign Ministry in its Twitter post (https://twitter.com/mfa_russia/status/1584547788335251462) is an ARAO photo from 2010," Twitter (now X), October 25, 2022, 11:53 AM, https://twitter.com/govSlovenia/status/1584936237806206976; and Joscha Weber, "Fact Check: Russia's False Case for a Dirty Bomb in Ukraine," *Deutsche Welle* (DW), October 18, 2022, https://www.dw.com/en/fact-check-russias-false-case-for-a-dirty-bomb-in-ukraine/a-63590306.

[29] Statement by Ambassador Barbara Žvokelj, Permanent Representative of Slovenia to the International Atomic Energy Agency (IAEA) at the meeting of the IAEA Board of Governors, on the safety, security, and safeguards implications of the situation in Ukraine (agenda item one), Vienna, Austria, March 2, 2022, https://www.gov.si/assets/predstavnistva/OVSE-Dunaj/dokumenti/izjave/2022/Slovenia-Statement-BoG-2-March-Ukraine.pdf.

[30] Peter Dubóczi and Dávid Dinič, "Disinformers in Slovakia Are Trying to Downplay Russian Activities in Ukraine by Discrediting the U.S. and NATO," Friedrich Naumann Foundation, June 14, 2022, https://www.freiheit.org/central-europe-and-baltic-states/disinformers-slovakia-are-trying-downplay-russian-activities.

[31] For example, see: "DISINFO: Radiation from Depleted Uranium Ammo in Ukraine Approaches Europe," EUvsDisinfo website, East Stratcom Task Force, European External Action Service, May 23, 2022, https://euvsdisinfo.eu/report/radiation-from-depleted-uranium-ammo-in-ukraine-approaches-europe; "Meteorologist Service Debunks Radiation Hoax," *Slovak Spectator* (newspaper), May 19, 2023, https://spectator.sme.sk/c/23171008/shmu-debunks-radiation-hoax.html; and Yevgeny Kuklychev, "Huge 'Mushroom' Blast in Khmelnytskyi Reignites 'Depleted Uranium' Claims," *Newsweek*, May 15, 2023, https://www.newsweek.com/huge-mushroom-blast-khmelnytskyi-reignites-depleted-uranium-claims-1800443.

[32] Marek Biró, "Šíria Sa Hoaxy o Rádioaktívnom Mraku Po Výbuchu v Meste Chmeľnyckyj. Nie je to Pravda (Hoaxes are Spreading About the Radioactive Cloud after the Explosion in the City of Khmeľnyckyj. It is not truth)," *Aktuality* (Slovak news site), May 18, 2023, https://www.aktuality.sk/clanok/9KfrgkG/siria-sa-hoaxy-o-radioaktivnom-mraku-po-vybuchu-v-meste-chmelnyckyj-nie-je-to-pravda/.

[33] Samuel Bista, "Správu o Zničení Muničného Skladu Pri Obci Chmeľnyckyj Využili Prokremeľské účty na šírenie Hoaxu o Uniknutej Radiácii (Pro-Kremlin Accounts Used the News About the Destruction of a Munitions Warehouse Near the Village of Khmeľnyckyj to Spread a Hoax About Leaked Radiation," *Infosecurity* (Slovak website), May 24, 2023, https://infosecurity.sk/domace/spravu-o-zniceni-municneho-skladu-pri-obci-chmelnyckyj-vyuzili-prokremelske-ucty-na-sirenie-hoaxu-o-uniknutej-radiacii/; and Una Hajdari, "Russian Embassy in Slovakia Uses Facebook to Push Propaganda. Why Are So Many Slovaks Buying It?" Euronews (television news network), March 29, 2023, https://www.euronews.com/2023/03/29/russian-embassy-in-slovakia-uses-facebook-to-push-propaganda-why-are-so-many-slovaks-buyin.

[34] "Slovak Republic (22-401)–Defense Cooperation Agreement," US Department of State, April 1, 2022, https://www.state.gov/slovakia-22-401.

[35] Martin Brezina et al., "Communicating Defence in Slovakia and the Czech Republic: Mapping Actors and Narratives Online," NATO Strategic Communications Centre of Excellence, November 11, 2022, https://stratcomcoe.org/publications/communicating-defence-in-slovakia-and-the-czech-republic-mapping-actors-and-narratives-online/252.

Supporters of the opposition 'Serbia Against Violence' (SPN) coalition protest in front of the Radio Television of Serbia (RTS) building amid opposition claims of major election law violations in the Belgrade city and parliament races, which were the subjct of frequent information influence campaigns, in Belgrade, Serbia. Source: REUTERS/Marko Djurica

Slovakia's elections in September 2023 were preceded by an influx of false and misleading messages, including those from Russia. The London-based nonprofit organization Reset recorded more than 365,000 election-related disinformation messages on Slovak social networks in the first two weeks of September, with estimates that the number would grow.[36] Their research found messages that violated social network terms of use and featured disinformation generated more than five times as much exposure as the average message. More than 15 percent of such content was posted by pro-Kremlin accounts.

SERBIA

Serbia is one of Russia's top targets in Eastern Europe for IIA. Serbia is deeply affected by Russian information operations that attempt to undermine perceptions of the EU, NATO, and other multilateral institutions in the region. With respect to CBRN weapons and nonproliferation, Russia has established a number of fake profiles, proxy pages, and state-run media (including Belgrade-based offices of Russia Today and Sputnik) in Serbia to share and amplify favorable stories on these issues.[37] Both Russia Today and Sputnik publish a constant flow of articles

[36] "Pro-Russian Disinformation Floods Slovakia Ahead of Crucial Parliamentary Election," Euronews with Agence France-Presse, September 29, 2023, https://www.euronews.com/2023/09/29/pro-russia-disinformation-floods-slovakia-ahead-of-crucial-parliamentary-elections.

[37] Leyla Latypova, "From Yandex to RT: Russia Expands Presence in Serbia Amid Ukraine War," *Moscow Times*, September 6, 2022, https://www.themoscowtimes.com/2022/09/06/from-yandex-to-rt-russia-expands-presence-in-serbia-amid-ukraine-war-a78638.

A general view of the "Foreign Ministers of Partners at Risk of Russian Disinformation and Destabilization" session at the NATO foreign ministers' meeting in Bucharest, Romania, November 2022. Source: Stoyan Nenov/REUTERS

that relate to CBRN weapons and nonproliferation. Russia has invested resources and funds into ensuring that narratives gain a broader audience, especially in the Western Balkans, given Serbia's relationship with Russia.[38] Several Russian state-sponsored or state-connected media organizations publish Serbian-language content in support of the Kremlin,[39] including News Front, SouthFront, Geopolitica.ru, and Katehon. For example, SouthFront has circulated several false claims, including that the OPCW neglected to share key details in their investigation on Syria's chemical weapons program or that US accusations of Russia's involvement in chemical attacks in Syria were an act of "whitewashing."[40]

However, even as Russian state-run media organizations maintain presences in Serbia, their most frequent tactic involves flooding the information space to see what resonates the most within local communities. Through these tactics, local media outlets in Serbia frequently repost and amplify Moscow's claims laid out in state-run media, which has much more impact in reaching the public because many individuals in Serbia have greater trust in local media outlets. For example, on Serbian platforms, false claims include the story of the United States and Ukraine developing bats as biological weapons to attack Russians.[41] These platforms include local media organizations, television broadcasters, radio stations, and others in Serbia that amplify, give credibility to, or create their own narratives that mirror the Kremlin's priorities.

These narratives circulate beyond Serbia throughout the Western Balkans. Given the reach of Serbian media and historical connections with other nations in the region, many of the narratives related to CBRN weapons and nonproliferation

[38] Maxim Samorukov and Vuk Vuksanovic, "Untarnished by War: Why Russia's Soft Power Is So Resilient in Serbia," Carnegie Endowment for International Peace, January 18, 2023, https://carnegieendowment.org/politika/88828.

[39] "GEC Special Report: Russia's Pillars of Disinformation and Propaganda," Global Engagement Center, US Department of State, August 2020, https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/.

[40] "GEC Special Report," US Department of State.

[41] Julian Borger, Jennifer Rankin, and Martin Farrer, "Russia Makes Claims of US-Backed Biological Weapon Plot at U.N.," Guardian, March 11, 2022, https://www.theguardian.com/world/2022/mar/11/russia-un-claims-us-backed-biological-weapon-plot-kremlin-foreign-fighters-ukraine.

that are shared in Serbia are picked up by other media organizations—including in Bosnia and Herzegovina, Montenegro, and North Macedonia—with great effect. Russia benefits significantly from destabilization in the Western Balkans, especially when Serbia and its neighbors do not condemn Russia's actions within the international community. As part of its broader geopolitical strategy, Russia uses Serbian media organizations as proxies to create distrust in nonproliferation regimes while degrading broader support for global nonproliferation norms.[42]

A STRATEGIC FRAMEWORK TO COUNTER RUSSIAN INFORMATION INFLUENCE ACTIVITIES

Given the scope and severity of Russian threats to nonproliferation norms in Slovenia, Slovakia, and Serbia, the project team developed a strategic framework for countering Russian IIA with the Department of State's Office of Cooperative Threat Reduction. We convened private, small-group workshops with representatives from government, civil society, academia, media, think tanks, business groups, law enforcement, and other sectors in Ljubljana, Bratislava, and Belgrade in 2023.[43] The first series of workshops, conducted in all three cities, was designed to educate personnel who were familiar with the challenges of IIA but less knowledgeable about nonproliferation topics, especially as it relates to the risks IIA pose to the stability of nonproliferation norms and potential use of CBRN weapons. These workshops included a scenario-based exercise where attendees were asked to create a counter-messaging strategy to respond to a hypothetical disinformation campaign from an adversary that involved an anthrax leak at a secure government laboratory.[44]

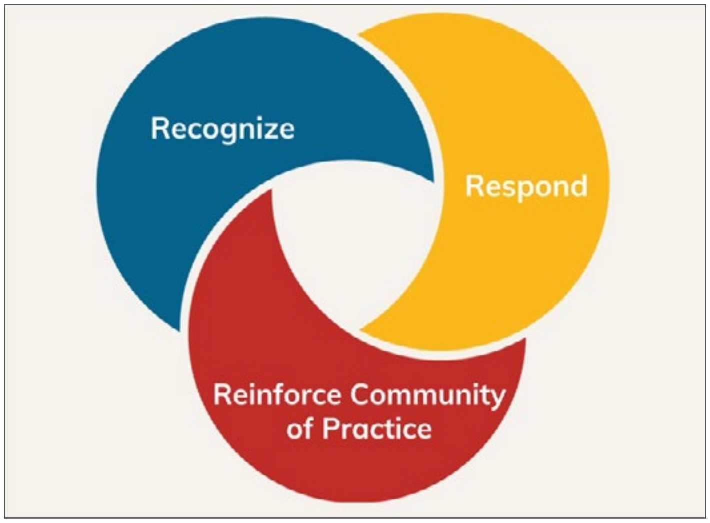


Figure 4: The Atlantic Council's strategic framework for countering Russian information influence activities.

After these workshops were completed, the project team used the results of the discussions, our extensive research, and consultations with experts in the region to create a draft strategic framework for countering IIA. The framework is comprised of three critical elements, or pillars. As depicted in Figure 4, the three pillars are *recognize, respond*, and *reinforce a community of practice*. For the next series of workshops, the project team returned to Bratislava and Belgrade to present the draft strategic framework to similar groups of experts, both those who were present at the first workshops and new stakeholders. Participants shared their views related to the three pillars, as well as the threat of Russian IIA more generally in their countries. Their feedback was critical to finalize the strategic framework presented in this report.

These pillars reflect the central elements of establishing resilience against disinformation, misinformation, and other forms of IIA. As Figure 4 demonstrates, the pillars are mutually reinforcing. For example, members of a community of practice can help each other recognize possible Russian IIA and devise effective response strategies. Response options can be studied by the community of practice to understand strengths and identify areas for improvement. The next three chapters describe each pillar of the strategic framework in greater detail.

[42] "Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them," European Parliament, February 23, 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf.

[43] Participants were selected for their subject matter knowledge on CBRN capabilities, disinformation and other forms of information influence, or other specialized expertise. The selected group of participants was intentionally designed to include a diverse range of backgrounds and perspectives.

[44] For more on the hypothetical scenario exercise, see Appendix II.

CHAPTER 2:
Recognizing information influence activities

Through its IIA, Russia attempts to distract from its own harmful actions and noncompliance with nonproliferation norms and regimes. These actions include Russia's use of chemical agents as weapons, its support for other regimes who have deployed chemical weapons, and its threats of nuclear escalation in Ukraine. Russia's long history of sowing doubt and confusion in public discourse by manipulating information goes beyond its borders. In Slovenia, Slovakia, and Serbia, Russia has perpetuated narratives designed to undermine nonproliferation norms, including those about the development and use of CBRN weapons. The first pillar in our strategic framework is *recognize*, which covers strategies, methods, and tools to identify IIA. This pillar is critical to promoting public awareness of—and resilience against—Russian influence.

KEY PRINCIPLES OF RECOGNIZING INFORMATION INFLUENCE ACTIVITIES

Effective tools and methods to recognize IIA are critical to fostering greater resilience and promoting critical thinking. Many governments and organizations have prepared guidelines for how to recognize disinformation, misinformation, and other types of IIA.[45] Several of these guidelines discuss the importance of verifying, authenticating, and scrutinizing information. Some tools are tailored for academic settings or for government and multilateral institution representatives.[46] However, the wider public can use many of the same tools. Common elements include the following principles:

Check the sources of the content and authenticate legitimacy

Understanding the source of a social media post or article is a critical first step in determining whether the information is reliable. Media consumers should assess whether a source is a reputable and well-established individual, organization, media outlet, or other legitimate entity. This is especially important when considering responses to nonproliferation-related information manipulation.

The US Cybersecurity and Infrastructure Security Agency (CISA) produced a guide titled "Disinformation Stops with You," which recommends several useful tactics to evaluate content, including investigating the issue with other reliable sources of information and thinking before sharing the content online.[47] CISA's guide, built around the principles outlined in Figure 5, serves as an important tool for local communities to identify forms of foreign malign influence. Ensuring accuracy and conducting diligent fact-checking can help prevent the spread and impact of IIA.

Verify information within the article or publication

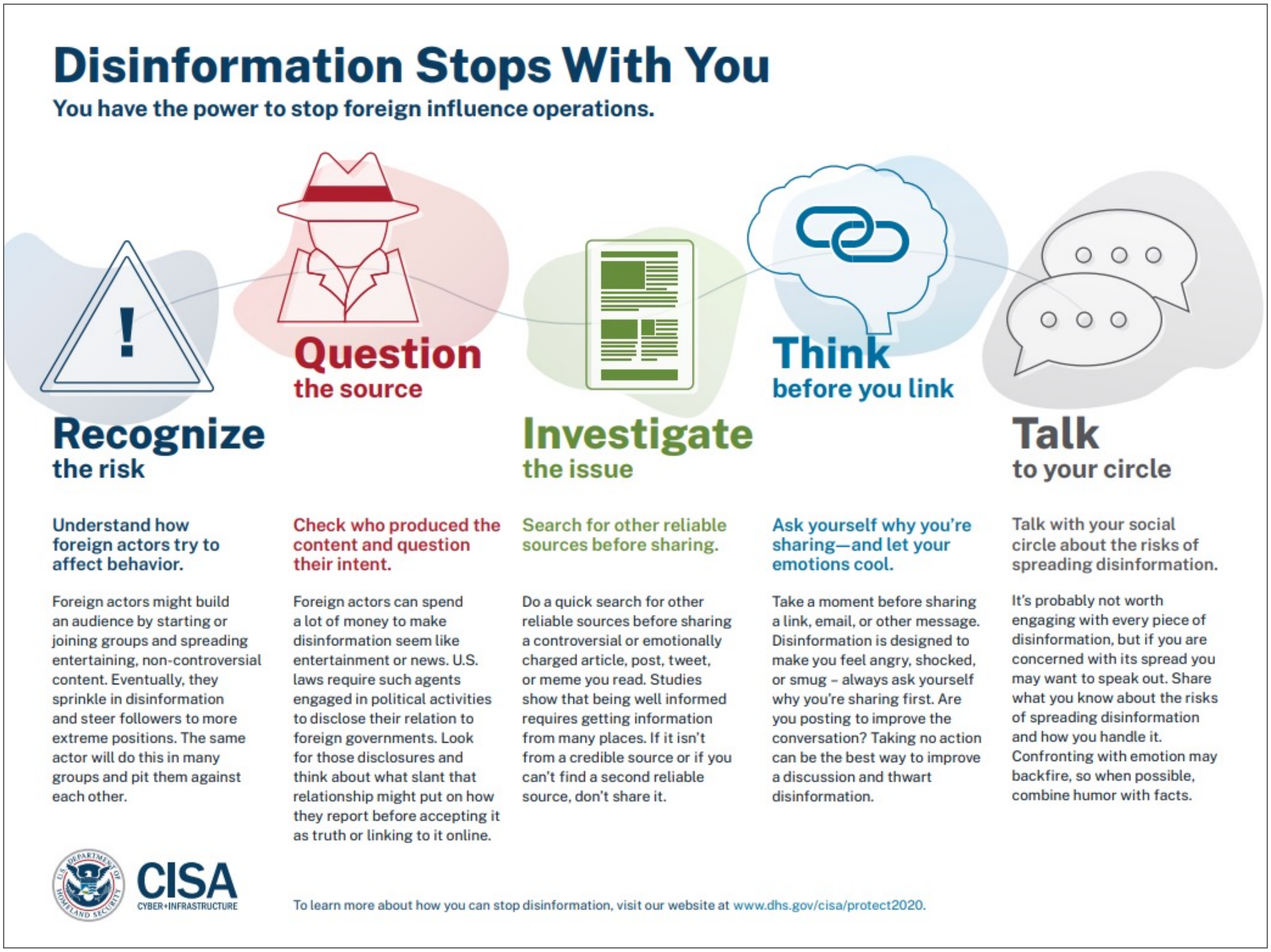
Cross-checking information through multiple reputable sources is instrumental in confirming the accuracy of content. Fact-checking websites and other digital literacy tools provide a methodical approach to validating the claims presented in an article. Fact-checking and verifying information also can serve as an important educational tool for individuals to learn how to critically assess information. Digital and media literacy exercises allow the public to make better-informed judgments on the credibility of content before sharing.

Apart from fact-checking websites, trusted networks can serve as another way to corroborate information before publishing or sharing content. During each workshop, participants frequently pointed to how often they rely on their own trusted relationships to screen information. Verifying content is an important

[45] Some examples include: "Resist 2 Counter Disinformation Toolkit," UK Government Communication Service, last updated November 2023, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/; "Disarming Disinformation: Our Shared Responsibility," Global Engagement Center, US Department of State, last updated October 20, 2023, https://www.state.gov/disarming-disinformation/; and "Detector Media," Detector Media (Ukrainian online publication), last updated September 2023, https://en.detector.media/.

[46] For academic-geared audiences, see: "'Fake News,' Disinformation, and Propaganda," Harvard Library, 2018, https://guides.library.harvard.edu/fake; "News: Fake News, Misinformation & Disinformation," Campus Library, University of Washington Bothell and Cascadia College, last updated November 2023, https://guides.lib.uw.edu/c.php?g=345925&p=7772376. For government-oriented guides, see: "Countering Disinformation," United Nations, last updated December 2023, https://www.un.org/en/countering-disinformation; and "Tackling Online Disinformation," European Commission, last updated December 2023, https://digital-strategy.ec.europa.eu/en/policies/online-disinformation.

[47] "Disinformation Stops With You," US Cybersecurity and Infrastructure Security Agency (CISA), 2022, https://www.cisa.gov/sites/default/files/publications/disinformation_stops_with_you_infographic_set_508.pdf.



Disinformation Stops With You

You have the power to stop foreign influence operations.

Recognize the risk

Understand how foreign actors try to affect behavior.

Foreign actors might build an audience by starting or joining groups and spreading entertaining, non-controversial content. Eventually, they sprinkle in disinformation and steer followers to more extreme positions. The same actor will do this in many groups and pit them against each other.

Question the source

Check who produced the content and question their intent.

Foreign actors can spend a lot of money to make disinformation seem like entertainment or news. U.S. laws require such agents engaged in political activities to disclose their relation to foreign governments. Look for those disclosures and think about what slant that relationship might put on how they report before accepting it as truth or linking to it online.

Investigate the issue

Search for other reliable sources before sharing.

Do a quick search for other reliable sources before sharing a controversial or emotionally charged article, post, tweet, or meme you read. Studies show that being well informed requires getting information from many places. If it isn't from a credible source or if you can't find a second reliable source, don't share it.

Think before you link

Ask yourself why you're sharing—and let your emotions cool.

Take a moment before sharing a link, email, or other message. Disinformation is designed to make you feel angry, shocked, or smug – always ask yourself why you're sharing first. Are you posting to improve the conversation? Taking no action can be the best way to improve a discussion and thwart disinformation.

Talk to your circle

Talk with your social circle about the risks of spreading disinformation.

It's probably not worth engaging with every piece of disinformation, but if you are concerned with its spread you may want to speak out. Share what you know about the risks of spreading disinformation and how you handle it. Confronting with emotion may backfire, so when possible, combine humor with facts.

CISA CYBER+INFRASTRUCTURE

To learn more about how you can stop disinformation, visit our website at www.dhs.gov/cisa/protect2020.

Figure 5: CISA's "Disinformation Stops With You" project, encouraging members of the community to recognize and combat disinformation and other forms of IIA. Image: CISA, https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_nrmc-Disinformation-Stops-With-You_0.pdf.

step in mitigating the spread of falsehoods and minimizing the impact of Russian IIA.

Review the date of the publication before sharing

Prior to circulating any media online, audiences should inspect and identify the publication date of an article or post. A frequent Russian tactic includes circulating outdated information with eye-catching headlines that mislead audiences. First Draft News published a guide to corroborating false information online that recommends examining a webpage's metadata to verify the date of the publication matches supporting sourcing elsewhere online and in print media.[48] Checking the publication date before sharing information can be a critical step in mitigating the spread of outdated, irrelevant, and sensationalized content.

Authenticate the authorship of content

Audiences should confirm the authorship of publications, especially as IIA can involve the impersonation of credible individuals or organizations.[49] Given that authors tend to publish within their area of responsibility and substantive focus, it is important to consider how the publication fits within the author's broader expertise. Establishing the author's identity by verifying their credentials contributes to the overall trustworthiness of the content.[50] Validating author identities

[48] "Verifying Online Information," *First Draft News*, October 19, 2019, https://firstdraftnews.org/wp-content/uploads/2019/10/Verifying_Online_Information_Digital_AW.pdf?x21167.

[49] "Tactics of Disinformation," CISA, September 2021, https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf.

[50] Darrell West, "How to Combat Fake News and Disinformation," Brookings Institution, December 18, 2017, https://www.brookings.edu/articles/how-to-combat-fake-news-and-disinformation/.

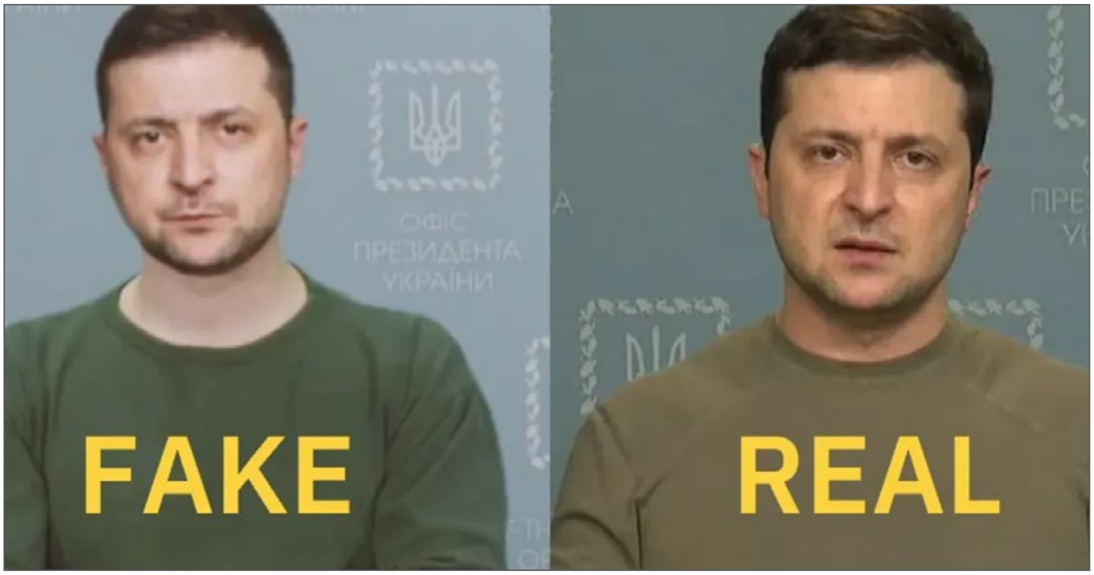


Figure 6: A side-by-side comparison of screenshots that claim to be Ukrainian President Volodymyr Zelenskyy. The photo on the right is real; the image on the left is a deepfake. Image comparison: Snopes, https://www.snopes.com/news/2022/03/16/zelenskyy-deepfake-shared/.

is a necessary component to combat disinformation, while building trust and support for legitimate reporting.

Inspect multimedia and other content included within the post

With the development of new and emerging technologies, fabricated and doctored multimedia content appear more frequently on various publications, including social media posts and fringe website pages.[51] To ensure manipulated content is properly verified, audiences should corroborate images and video to prevent manipulation through deepfakes, AI-generated photos and videos, deceptive editing, and other forms of online personalization.

Deepfake images in particular can mislead audiences to believe falsified content is real. For example, two seemingly authentic screenshots of Ukrainian President Volodymyr Zelenskyy speaking at a press conference appear in Figure 6. Both images appear to be authentic, but upon closer examination, there are indications that the image on the right was doctored. In this instance, the image on the right is an authentic photograph, while the image on the left is an AI-generated deepfake. However, for a user who is scrolling quickly on Facebook or X (formerly known as Twitter), the difference may not be easy to discern, creating an even more challenging information environment.

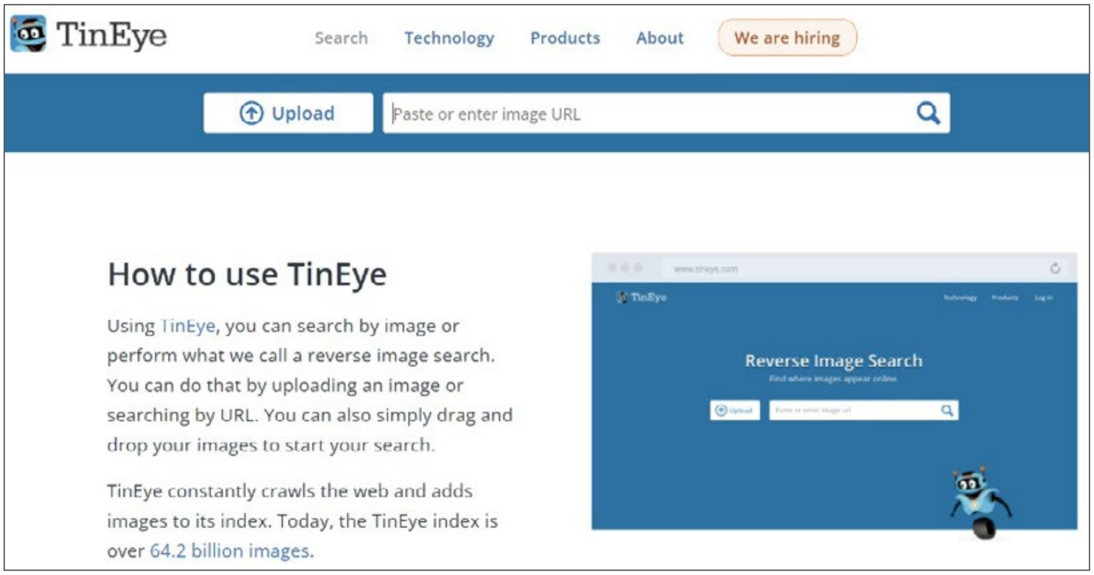
Similarly, IIA rely on visually compelling or sensational images and video to evoke extreme reactions from audiences. This holds especially true for CBRN-related disinformation, which can grab attention and spread rapidly online, in print and broadcast media, and through word of mouth.[52] As new methods for misleading audiences are developed, it is imperative for the public to ensure content has not been altered, taken out of context, or misconstrued to serve ulterior interests.

TOOLS TO DETECT INFORMATION INFLUENCE ACTIVITIES

In many cases, it can be difficult to detect and identify IIA as they arise, especially as Russia deploys several kinds of narratives. As local media outlets frequently parrot Russian IIA and communities battle the constant influx of propaganda, people can unintentionally share misinformation. Several tools and methods exist to help identify and verify the accuracy of information shared online.

[51] Rachel Baig, "Fact Check: How Do I Spot Manipulated Images?" *DW*, January 5, 2022, https://www.dw.com/en/fact-check-how-do-i-spot-manipulated-images/a-60001842.

[52] Lisa Fazio, "Out-of-context Photos Are a Powerful Low-tech Form of Misinformation," PBS *NewsHour*, February 18, 2020, https://www.pbs.org/newshour/science/out-of-context-photos-are-a-powerful-low-tech-form-of-misinformation.



How to use TinEye

Using TinEye, you can search by image or perform what we call a reverse image search. You can do that by uploading an image or searching by URL. You can also simply drag and drop your images to start your search.

TinEye constantly crawls the web and adds images to its index. Today, the TinEye index is over 64.2 billion images.

Figure 7: TinEye's reverse image search platform can help users identify existing uses of images online. Image: https://tineye.com/.

Fact-checking and debunking websites

Fact-checking sites and debunking organizations play an important role in assessing the accuracy of information shared online. Fact-checkers often investigate and corroborate claims made in news articles, social media posts, and official government documents.

In Europe, EUvsDisinfo,[53] Snopes,[54] and PolitiFact are good examples of fact-checking and debunking websites.[55] In Slovenia, Oštro[56] and its fact-checking arm, Razkrinkavanje,[57] play an important role in vetting truthful information within the public domain. In Slovakia, fact-checking and debunking webpages—including Demagog.sk[58] and Infosecurity.sk[59]—frequently fact-checked the statements of candidates during the September 2023 parliamentary elections. Similar organizations also exist in Serbia, including the Center for Research, Transparency and Accountability (CRTA),[60] FakeNews Tragač,[61] and the Crime and Corruption Reporting Network (KRIK).[62] Finally, Radio Free Europe/Radio Liberty[63] plays an important regional role throughout Central and Eastern Europe through its mission of sharing truthful information and independent analysis.

Reverse image search methods

Reverse image search tools are another important tactic in verifying online information. These platforms allow users to corroborate and verify the original uses and sources of images. Many reserve image search tools also provide tracing capabilities for audiences to track where the image has been circulated and whether the photos have previously been used in different contexts. In addition, reverse image search tools can determine whether questionable content has previously been used in other contexts. Similarly, in instances where images have been created and manipulated using deepfake technology, reverse image search tools are able to uncover the original sources of images and reveal inconsistencies, such as facial features, landscape backgrounds, and other details.

[53] "EUvsDisinfo," EUvsDisinfo, last updated December 2023, https://euvsdisinfo.eu/.

[54] "Snopes," Snopes, last updated December 2023, https://www.snopes.com/.

[55] "Politifact," Politifact, last updated December 2023, https://www.politifact.com/.

[56] "Ostro," Ostro, last updated December 2023, https://www.ostro.si/.

[57] Raskrinkavanje (@raskrinkavanje), "Koje Vijesti o koronavirusu su lazne," Twitter (now X), March 18, 2020, 2:35 pm, https://twitter.com/raskrinkavanje/status/1240346134922399744.

[58] "Factcheck on Political Discussion," Demagog, last updated December 2023, https://demagog.sk/.

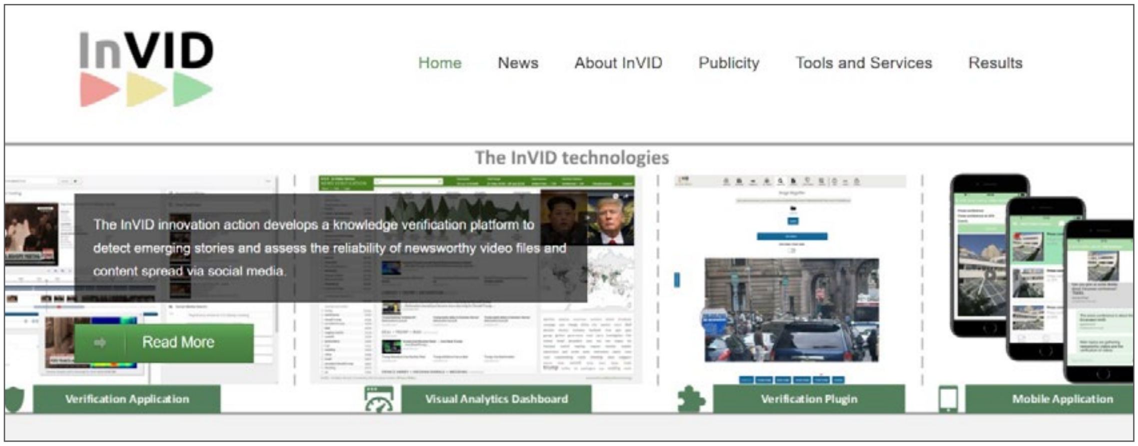
[59] "Infosecurity," Infosecurity, last updated December 2023, https://infosecurity.sk/.

[60] "CTRA," CTRA, last updated December 2023, https://crta.rs/.

[61] "Fake News Tragač," Fake News Tragac, last updated December 2023, https://fakenews.rs/.

[62] "KRIK," KRIK, last updated December 2023, https://www.krik.rs/en/.

[63] "Radio Free Europe/Radio Liberty," *Radio Free Europe/Radio Liberty*, last updated December 2023, https://www.rferl.org/.



The InVID innovation action develops a knowledge verification platform to detect emerging stories and assess the reliability of newsworthy video files and content spread via social media.

Figure 8: InVID is a useful digital forensics tool that can help analyze video footage that is spread online. Image: https://www.invid-project.eu/description/.

Several platforms including Google Images,[64] TinEye,[65] and ImageRaider[66] are examples of systems that can help individuals confirm the authenticity of visual content online. TinEye, as displayed in Figure 7, uses a database of over sixty-four billion images for users to cross-reference when photos have been used in other contexts. Given how technical CBRN-related topics can be for audiences, these tools are important to support efforts in debunking and combating the spread of Russian IIA related to nonproliferation.

Web browser extensions

As search engines become more sophisticated, browser extensions can be useful tools to help identify false and misleading information, especially on webpages that tend to share disinformation. Many extensions can analyze links and sources in real time, which provides important details on the trustworthiness of information online.

One example of a browser extension is NewsGuard, which provides ratings and detailed information about the news sites that users visit as they read through various webpages.[67] SurfSafe is another example that can help identify disinformation and other forms of IIA through highlighting tools on content posts.[68] TinEye, the aforementioned reverse image search tool, also offers a browser extension for verifying visual content in real time when visiting webpages.

Digital forensics tools

Digital forensics tools are more specialized software that can investigate and analyze sophisticated IIA. Many of these tools can comb through the metadata of websites, which can reveal important details of webpages and their creation, modification, and origins, especially in tracing links to other pages. Other tools, such as social media forensics technologies, can assist investigators in tracking the spread of disinformation, identifying key actors within information influence networks, and analyzing the extent of Russian IIA's reach and impact.

One sample tool is InVID, a browser extension that can verify the authenticity of videos and information shared on social media.[69] The tool, as seen in Figure 8, can be used in a variety of different formats, including a browser extension

[64] "Google Images," Google, last updated December 2023, https://images.google.com/.

[65] "Reverse Image Search," TinEye, December 2023, https://tineye.com/.

[66] "Image Raider Reverse Image Search," Infringement Report, last updated December 2023, https://infringement.report/api/raider-reverse-image-search/.

[67] "Transparent Tools to Counter Misinformation for Readers, Brands, and Democracies," NewsGuard, last updated December 2023, https://www.newsguardtech.com/.

[68] Issie Lapowsky, "This Browser Extension Is Like an AntiVirus for Fake Photos," *Wired*, August 20, 2018, https://www.wired.com/story/surfsafe-browser-extension-save-you-from-fake-photos/.

[69] "InVID Verification Plugin," InVID, December 2018, https://www.invid-project.eu/tools-and-services/invid-verification-plugin/.

and mobile phone application. Forensically is another suite of digital tools for digital forensics, including image analysis and other forms of authenticating content.[70] Both forensics analysis systems are useful in identifying manipulated content and deepfake technology.

AUGMENTING METHODS TO RECOGNIZE INFORMATION INFLUENCE ACTIVITIES

Our discussions with representatives in Slovenia, Slovakia, and Serbia demonstrated that recognizing information influence activities is an important step to counter Russian influence efforts. However, these efforts need to be supported and complemented by effective responses to these campaigns. To counter Russian IIA, the recognize pillar of our strategic framework seeks to address some of the broader strategies that may be used in understanding the threat of disinformation and other forms of malign influence activity. In Chapter 3, we discuss our second pillar, responding to Russian information influence activities, which examines best practices and recent responses to Russian IIA.

[70] "Forensically Beta," Forensically Beta, last updated December 2023, https://29a.ch/photo-forensics/.

CHAPTER 3:
Responding to information influence activities

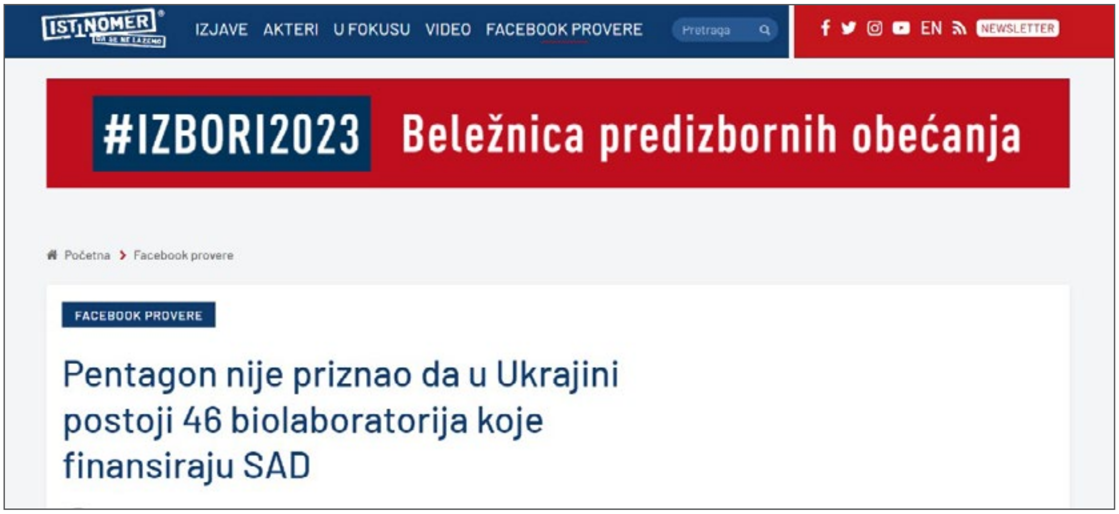
Through our research, we identified several key principles to consider when crafting a response to Russian IIA. These principles are reinforced by examples from the United States, as well as the experiences of individuals in Slovenia, Slovakia, Serbia, and elsewhere. The second pillar in our strategic framework is *respond*, which covers strategies and narratives used to counter Russian IIA. Workshop participants demonstrated these principles when asked to create a response to the anthrax exposure posited in our hypothetical scenario-based exercise described in Appendix II. Several attendees also shared insights from their experiences creating responses to real-world Russian IIA, which we discuss in this chapter.

KEY PRINCIPLES OF RESPONDING TO INFORMATION INFLUENCE ACTIVITIES

When crafting a response to Russian IIA, it is important to keep several key principles in mind: prioritize transparency and concise messaging, connect the ideas to the correct audience and platforms; and determine the best person to deliver the message.

Be transparent, clear, and concise

An effective counterresponse should be factual and clear, especially when addressing scientific and technical information that can be confusing to a nonspecialist audience. By using clear and concise information, complex topics such



#IZBORI2023 Beležnica predizbornih obećanja

Pentagon nije priznao da u Ukrajini postoji 46 biolaboratorija koje finansiraju SAD

Figure 9: Istinomer regularly fact-checks various forms of IIA on social media platforms using facts and transparency. Image: https://www.istinomer.rs/.

as nonproliferation or chemical weapons can be distilled into digestible language that is easy to understand. Russia recognizes that CBRN-related issues and WMD threats are often not well understood among the general community, which makes them popular topics for false narratives.

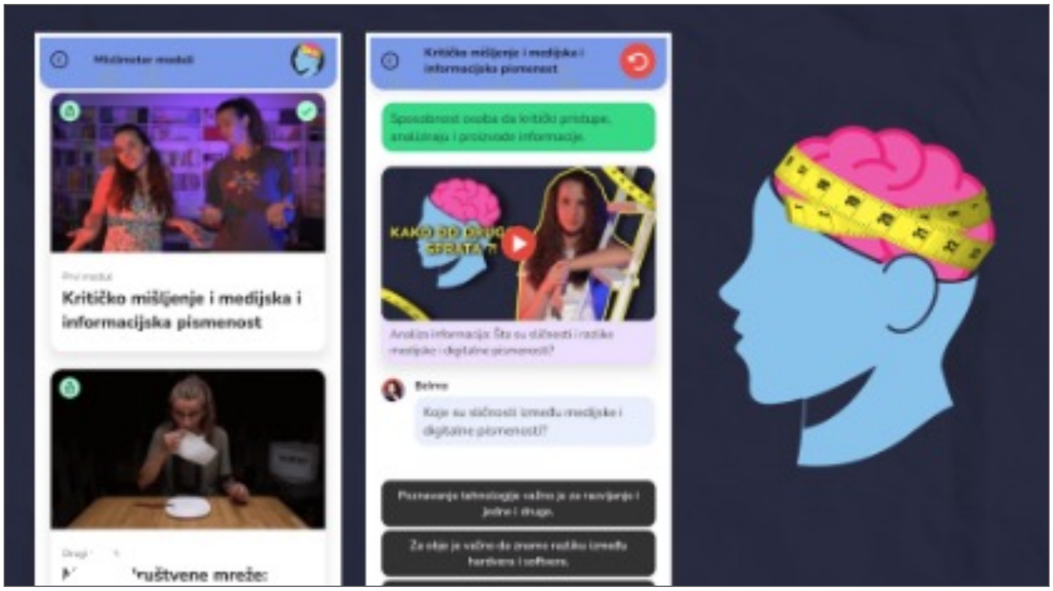
Russia's use of emotionally charged IIA has made the need for clear responses a priority. In Serbia, CRTA's Istinomer project is at the forefront of debunking, fact-checking, and countering Russian IIA.[71] Istinomer consistently monitors disinformation and misinformation on social media to determine which narratives are resonating the most within communities. Following their analysis, Istinomer staff publish short-form posts on their platform that debunk the various claims using facts. See Figure 9 for an example of how the Istinomer team debunked false and misleading claims that mischaracterized the work of US-supported research facilities in Ukraine. In each post, the Istinomer author refutes each false and misleading claim with citations, secondary sources, interviews, and further reading material, including US government reports.

It is important for counter-messaging strategies to include these characteristics to resonate with audiences and ensure effectiveness, especially when it relates to nonproliferation-related information manipulation tactics.

Match the message to the audience and platforms

Different audiences might require tailored messaging strategies, including via different platforms. Younger audiences that receive much of their information from social media platforms may view TikTok before watching a local news broadcast. Those who spend more time driving might listen to radio news than those who commute via other means. Therefore, it is important to consider whether a counternarrative should include more visuals than text based on the intended audience and platform. Messages designed for television will require compelling audio and visual components, but messages designed for print media should focus on attention-grabbing graphics and text that clearly convey the main messages. However, all messages should include the same basic facts to promote consistency and accuracy.

Counter-messaging strategies must consider both the medium for sharing responses as well as the social media platforms themselves. For example, TikTok prioritizes short-form videos, while Instagram focuses more on photographs and other forms



Mislimetar moduli

Prvi modul
Kritičko mišljenje i medijska i informacijska pismenost

Drugi
[illegible] ruštvene mreže:

Kritičko mišljenje i medijska i informacijska pismenost

Sposobnost osoba da kritički pristupe, analiziraju i proizvode informacije.

Analiza informacija: Šta su sličnosti i razlike medijske i digitalne pismenosti?

Belma
Koje su sličnosti između medijske i digitalne pismenosti?

Poznavanje tehnologije važno je za razvijanje i jedne i druge.

Za nas je važno da znamo razliku između hardvera i softvera.

Figure 10: A screenshot of the Danes je nov dan mobile application, Mislimetar, which serves as an important media literacy tool in Slovenia. Image: https://danesjenovdan.si/en/campaigns.

[71] "Istinomer," Istinomer, last updated December 2023, https://www.istinomer.rs/.

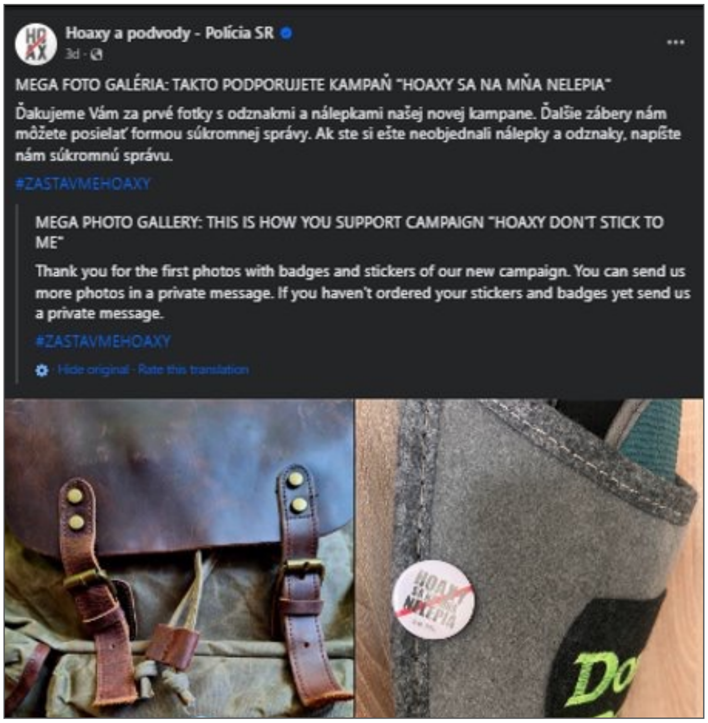
of visually appealing content. The combination of message and medium is especially important when considering which kinds of counter-messaging campaigns will resonate with different audiences. Two organizations in Slovenia—Danes je nov dan (Today is a new day) and Pod črto (The Bottom Line)—developed innovative methods of using storytelling to debunk false information in Slovenia using trusted voices and captivating forms of visual media. These efforts deepen the impact and reach of their organizations.[72] One initiative, which Danes je nov dan termed Mislimetar (Figure 10), serves as an educational and entertainment mobile application that promotes media literacy and critical thinking in younger audiences.

Regional differences also are important to consider. For example, in Slovakia, workshop participants said that Facebook and Telegram are more popular than Instagram or TikTok.[73] In Serbia, Telegram is the most frequently used social media platform, while Facebook remains a popular platform in Slovenia. Regardless of platform, it is essential to make sure credible information is available in regional dialects in addition to the main language spoken in a country to reach the broadest possible audience.

Consider who is best positioned to deliver the message

The best person, organization, or outlet to deliver a counternarrative will depend on the country, city, or local area that the message is intended to reach as well as the specific target audience. When asked who the trusted messengers are within their communities, workshop participants in our three countries had varying answers. In Slovakia, the police and armed forces were cited as effective messengers, whereas in Slovenia, participants said a response led by the armed forces would not be well received.

The Slovak Police Force leads a popular community-centered Facebook campaign titled "Hoaxy a Podvody" ("Hoaxes and Frauds"), which began in 2018. Through its platform, the Police Force leads public engagement to debunk false narratives circulating online and develop an informed and resilient citizenry.[74] In 2023, the Police Force, part of the Department of Interior, kicked off a campaign called "Hoaxy Sa Na Mňa Nelepia" ("Hoaxes Don't Stick to Me"). To move the campaign beyond the digital world, members of the community displayed buttons and stickers in public spaces in support of counter-disinformation efforts, as seen in Figure 11. The project's community-centric focus could be a potential model to replicate in the future.[75]


Hoaxy a podvody - Polícia SR
3d ·

MEGA FOTO GALÉRIA: TAKTO PODPORUJETE KAMPAŇ "HOAXY SA NA MŇA NELEPIA"

Ďakujeme Vám za prvé fotky s odznakmi a nálepkami našej novej kampane. Ďalšie zábery nám môžete posielať formou súkromnej správy. Ak ste si ešte neobjednali nálepky a odznaky, napíšte nám súkromnú správu.

#ZASTAVMEHOAXY

MEGA PHOTO GALLERY: THIS IS HOW YOU SUPPORT CAMPAIGN "HOAXY DON'T STICK TO ME"

Thank you for the first photos with badges and stickers of our new campaign. You can send us more photos in a private message. If you haven't ordered your stickers and badges yet send us a private message.

#ZASTAVMEHOAXY

Figure 11: A photo from the Slovak Police Force Facebook page, which describes the "Hoaxes Don't Stick to Me" campaign. Image: Facebook, https://www.facebook.com/hoaxPZ/.

BEYOND RESPONDING: PROACTIVE MEASURES TO PREVENT RUSSIAN INFORMATION INFLUENCE ACTIVITIES

Our discussions with representatives in all three countries demonstrated that responding alone is not enough to stop Russian IIA. Countries need to get ahead of possible Russian

[72] "Campaigns," Danes je nov dan (Today is a new day), last updated December 2023, https://danesjenovdan.si/en; and "CTRO Podcast," Pod črto, last updated December 2023, https://podcrto.si/.

[73] "Social Media Stats Slovakia," Statcounter, last updated November 2023, https://gs.statcounter.com/social-media-stats/all/slovakia-(slovak-republic).

[74] "Report of the Police Force on Disinformation in Slovakia in 2022," Department of Communication and Prevention of the Presidium of the Police Force, 2023, https://www.minv.sk/swift_data/source/images/sprava-o-dezinformaciach-sr-2022eng.pdf.

[75] This publication was originally written in December 2023, before the Ministry of Interior's decision to terminate "Hoaxy a Podvody" as a state-run project in early 2024. The platform has now been reshaped as a citizen-led initiative that still maintains popular support in Slovakia.

IIA campaigns, an observation shared by US government officials. For example, the US Defense Threat Reduction Agency (DTRA) established a dedicated information resilience office in 2022 to better understand the scope of information manipulation against its worldwide countering-WMD presence.[76] This includes prebunking,[77] a term that encompasses efforts to anticipate or identify IIA early and encourage resilience among citizens to inoculate them from IIA.[78] Additionally, the Department of State's Global Engagement Center (GEC) has issued numerous reports about Russia's attempts to spread disinformation about US and Ukrainian biosafety and biosecurity initiatives.[79] The GEC was established in 2017, but has more recently begun to explore whether sharing limited details about sensitive missions in advance can limit the effect of Russian attempts to twist facts after a mission has occurred.[80]

To effectively counter Russian IIA, the respond pillar of our strategic framework takes a broad approach that incorporates elements of prebunking and early identification to promote a holistic view of response. In this way, response can be proactive or reactive, which is essential to limiting the effects of false narratives Russia spreads worldwide. In the next chapter, we describe our third pillar, *reinforcing a community of practice*, which encapsulates elements of the first two pillars to augment their importance to a broader audience.

[76] "Director's Strategic Intent: 2022-2027," US Defense Threat Reduction Agency, 2022, https://www.dtra.mil/Portals/125/Documents/Leadership/Director-Strategic-Intent-FINAL.pdf.

[77] Mikey Biddlestone et al., "A Practical Guide to Prebunking Misinformation," University of Cambridge, BBC Media Action, and Jigsaw, 2022, https://interventions.withgoogle.com/static/pdf/A_Practical_Guide_to_Prebunking_Misinformation.pdf.

[78] "Adapt to the Information Environment," Defense Threat Reduction Agency, last updated December 2023, https://www.dtra.mil/About/Strategic-Initiatives/Adapt-to-the-Information-Environment/; and Alberto-Horst Neidhardt and Paul Butcher, "From Debunking to Prebunking: How to Get Ahead of Disinformation on Migration in the EU," European Policy Centre, November 29, 2011, https://www.epc.eu/en/Publications/From-debunking-to-prebunking-How-to-get-ahead-of-disinformation-on-mi~446f88.

[79] "The Kremlin's Never-Ending Attempt to Spread Disinformation About Biological Weapons," Global Engagement Center, US Department of State, March 14, 2023, https://www.state.gov/the-kremlins-never-ending-attempt-to-spread-disinformation-about-biological-weapons/; and "Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War," Global Engagement Center, US Department of State, February 23, 2023, https://www.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war/.

[80] Steven Lee Meyers, "U.S. Tries New Tack on Russian Disinformation: Pre-Empting It," *New York Times*, October 27, 2023, https://www.nytimes.com/2023/10/26/technology/russian-disinformation-us-state-department-campaign.html.

CHAPTER 4: Reinforcing a community of practice

A community of practice committed to identifying and countering Russian IIA is a critical component to limiting the effectiveness of Russia's efforts to spread false messages in Slovenia, Slovakia, and Serbia. For our project, this community is defined broadly to ensure that all stakeholders are represented. Members of the public and private sectors, including government, military, law enforcement, academia, think tanks, nongovernmental organizations, and the media all have a role to play in recognizing and responding to Russian IIA. This third pillar in our strategic framework is *reinforcing a community of practice*, which covers opportunities to expand the multistakeholder community dedicated to responding to Russian IIA. In this chapter, we describe the general roles that a community of practice should serve in addition to country-specific considerations discussed throughout our workshops.

COMMUNITY OF PRACTICE ROLES

Members of the community play an important role in promoting resilience among the populations most frequently targeted by Russia's false messages. These roles include reinforcing consistent communication, expanding social resilience, prioritizing multistakeholder engagement, and identifying methods to expand the overall community dedicated to countering Russian information influence activities.

Resource and reinforce

A vital role for the community of practice is to ensure that efforts to counter Russian IIA reach the broadest possible audience, both within a country and among its regional neighbors, when appropriate. Community members from academia and think tanks can amplify messages from government and law enforcement sources to add legitimacy to their campaigns. This cooperation requires consistent communication among the community to understand Russia's IIA, how it affects the broader public, and what stakeholders can do to counter false narratives.

In March 2022, the Russian Defense Ministry circulated claims about US-backed Ukrainian bioweapons production efforts to justify Russia's then-recent invasion of Ukraine.[81] Officials from the People's Republic of China and incendiary US media figures amplified these claims on a popular social media platform, Weibo.[82] In response, prominent US officials testified before Congress about the legitimacy of US-backed research facilities in Ukraine—including those established with CTR resources—and organizations like DTRA and the GEC issued fact sheets and statements that bolstered the legitimacy of CTR's work. Former US officials and private-sector experts wrote editorials, social media posts, and made media appearances decrying Russia's claims, providing important alternative perspectives that bolstered official government messages. The reinforcement of the key message that the United States and Ukraine were not producing biological weapons was critical to reaching as broad an audience as possible.

Reinforcing capacity-building efforts focused on countering Russian influence efforts is a priority among stakeholders in Slovenia, Slovakia, and Serbia. However, interest in these issues must be matched by resources to maintain and create new counternarratives. Many of the workshop participants shoulder numerous work responsibilities in addition to tracking Russian IIA. One benefit of an engaged community of practice is the ability to cooperate on messaging strategies and share the resource burden, including the time it takes to craft engaging, informative narratives and discern the best platform(s) on which to disseminate these narratives. When new approaches are needed to respond to new or evolving Russian falsehoods, an active community can also ensure

[81] Nika Aleksejeva and Andy Carvin, *Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression Against Ukraine*, Atlantic Council, February 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/.

[82] The Washington Post Editorial Board, "How Russia Turned America's Helping Hand to Ukraine into a Vast Lie," *Washington Post*, March 29, 2023, https://www.washingtonpost.com/opinions/2023/03/29/russia-disinformation-ukraine-bio-labs/.

that key messages from past campaigns are carried over to promote consistency. Furthermore, a coordinated approach among stakeholders to amplify key messages and reduce duplication in messaging is important to reduce confusion and promote clarity.

Enhance social resilience

The community of practice should also focus on enhancing social resilience through public messaging and public education campaigns. While it is more difficult to reach people who espouse aggressively favorable views of false claims, evidence-based messages can influence those who are more open-minded.[83] Though it might not be possible to stop Russia's IIA, a resilient public might be less susceptible to believing or spreading false claims.

Enhancing social resilience emphasizes whole of society responses to counter Russian malign influence activities. This is a deliberately broad goal, but given the complexity of the media landscape, it is difficult to achieve.[84] A good starting point is by working through trusted messengers to understand whether false narratives have achieved support in specific parts of the community, and why those narratives were persuasive. Local journalists are especially critical because they are in closer contact with parts of the community that national outlets might not understand as well. In this way, local journalists can both contribute to an understanding of the pervasiveness of false messages and what could be effective in changing minds.

Media literacy is another critical component of enhancing resilience. Critical thinking skills that teach students to question everything they read can promote longer-term outcomes than identifying correct and incorrect statements.[85] Furthermore, engaging the public early and often can promote trust in the output of government data.[86] Such an approach has demonstrated benefits in countering public health-related disinformation and misinformation, and also applies to Russian IIA about biological and radiological weapons that prey on the health effects of exposure to toxic substances.

Employ multisectoral and multidisciplinary approaches

An important role of the community of practice is to promote effective methods to combat IIA through multisectoral and multidisciplinary approaches. For a complicated and technical subject such as biological weapons—a frequent target of Russia's IIA efforts—it is critical to include scientists, public health experts, academics, and other experts in the development of responses. Communications experts should seek to translate scientific and technical information into digestible information suitable for a general audience. The Bioweapons Disinformation Monitor, a partnership between King's College London and the Canadian government, publishes videos, fact sheets, and short reports that concisely explain false Russian narratives about biological weapons and the reasons why these claims are untrue.[87] In addition to producing concise, factual counternarratives, the website also promotes articles from other sources, such as the Bulletin of the Atomic Scientists and foreign news sites to amplify the work of like-minded organizations in multiple sectors.[88]

Identify opportunities for expansion

When considering other elements of society to incorporate into a community of practice, it is important to cast a wide net. In international relations theory, the concept of latent power refers to the broad range of resources available to a state that could contribute to greater military power.[89] Russia calls this the correlation of forces and means, which explains how Russia views its military expansion potential, but also incorporates elements of alliance relations, social cohesion, and economic stability that involve broader parts of society.[90] Although these theories have primarily military implications, the principle that all elements of a society can bolster one critical function applies directly to the fight against Russian IIA. For example, Estonia has used a multisectoral approach to countering disinformation and misinformation since 2007, when it was subject to destructive

[83] Cristina Pulido et al., "A New Application of Social Impact in Social Media for Overcoming Fake News in Health," *Journal Environmental Research and Public Health* 17, no. 7 (2020): 2430-2435, accessed, November 17, 2023, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7177765/.

[84] Julian McDougall, "Media Literacy versus Fake News: Critical Thinking, Resilience, and Civic Engagement," Media Studies 10, no. 19 (2019), https://hrcak.srce.hr/ojs/index.php/medijske-studije/article/view/8786.

[85] McDougall, "Media Literacy versus Fake News."

[86] Nathan Myers, "Information Sharing and Community Resilience: Toward a Whole Community Approach to Surveillance and Combatting the 'Infodemic,' " *World Medical & Health Policy* 13, no. 3 (2021): 581-592, accessed November 22, 2023, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8250699/.

[87] "Bioweapons Disinformation Library," Bioweapons Disinformation Monitor, King's College London initiative in partnership with the Canadian government, last updated December 2023, https://www.bioweaponsdisinformationmonitor.com/.

[88] "Bioweapons Disinformation Library," Bioweapons Disinformation Monitor.

[89] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W.W. Norton and Company, 2014), 60.

[90] Clint Reach, Vikram Kilambi, and Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means*, Santa Monica, Calif.: RAND Corporation (2020), 11, https://www.rand.org/pubs/research_reports/RR4235.html.

cyberattacks that continue to present day.[91] Media literacy is a core component of the curriculum in Estonian schools, and leaders from across Europe visit Estonia to learn more about their broad approach to establishing resilience to IIA.[92] The need to go beyond traditional organizations tasked with identifying and stopping IIA also is understood in Slovakia. Participants at our second workshop in Bratislava suggested that engaging religious leaders and local labor officials to amplify counternarratives against false Russian claims could be effective because these leaders maintain the trust of their members.

Expansion also applies to promoting resilience across countries, not just in large population centers. In Slovakia and Serbia, political polarization and distrust of institutions hamper counter-messaging strategies and keep people with disparate views siloed from one another. Geographic differences exacerbate these silos. Participants in both countries noted that going beyond the capital allows one to reach disadvantaged communities that might be more affected by Russian information warfare preying on their existing views that the state does not look after their interests.

As the third pillar of our strategic framework, the community of practice plays an important role in reinforcing the efforts of the first two pillars to recognize and respond to Russian IIA. The linkages between the three pillars are important to ensure thoughtful, effective responses to false narratives that damage government credibility and trust in institutions. In the next chapter, we discuss considerations for implementing the strategic framework, as well as areas for investment to continue the fight against Russian IIA that target nonproliferation.

[91] Rain Ottis, “Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective,” Cooperative Cyber Defence Centre of Excellence, January 2008, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[92] Amy Yee, “The Country Inoculating against Disinformation,” BBC, January 30, 2022, https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation.

CHAPTER 5:
Considerations for implementation and the way ahead

Our research and discussions with stakeholders in Slovenia, Slovakia, and Serbia illuminated several important considerations for implementing initiatives to counter Russian IIA as they relate to nonproliferation. In this chapter, we describe these considerations and include recommendations for investment, while discussing the way ahead for this project.

IMPLEMENTATION CONSIDERATIONS

There are many opportunities for stakeholders within the region to design successful responses to Russian IIA. These include opportunities to strengthen transparency and access to information, expand cooperation within multistakeholder groups, and broaden existing networks to include international partners.

Maximize transparency and safeguard access to information

To improve trust in public institutions and political processes, government entities should strive to be as transparent as possible with information related to false Russian claims about CBRN weapons. Providing truthful and accurate information with proper citations and evidence can play an important role in prebunking Russian narratives. Maximizing transparency on social media platforms with respect to the activity of Russian information networks also can play an important role, especially as civil society and other organizations prioritize how to respond to Russian IIA.

Enhance cooperation with a multistakeholder community

Involving the private sector in government-led responses to Russian IIA can strengthen relationships and improve information sharing with partners outside of government. Members of the private sector can support a healthy information environment, including through their support for independent investigative journalism and objective reporting.

Another opportunity to strengthen responses to combat Russian IIA includes connecting civil society organizations and government entities with their counterparts in scientific and academic communities. Research-oriented professionals bring a wealth of expertise on technical topics, such as CBRN weapons and nonproliferation, which can augment counter-messaging strategies with data-driven information.

Similarly, youth organizations can play an important role in mitigating disinformation. Dedicated engagement and educational initiatives with younger audiences can build broader resilience against Russian IIA. Youth organizations serve as an opportunity to reach unengaged youth who are not necessarily involved in countering Russian IIA more broadly. Increasing investment within younger generations also helps mitigate the brain drain phenomenon of young, highly educated people leaving Central and Eastern Europe.[93] This phenomenon leaves fewer in the next generation that are able to study disinformation and nonproliferation, resulting in a significant gap in substantive expertise on these issues. It will be critical to reinvest in the next generation of experts, which will allow for greater potential for locally driven development of policy solutions, especially around nonproliferation and information warfare.

Expand the community of practice to include international partners

Members of the community of practices within Slovenia, Slovakia, and Serbia should enforce stronger multistakeholder engagement with international partners, including neighboring countries, international organizations, and the United States. Maintaining consistent close cooperation with international partners provides opportunities to learn about other countries that might experience similar challenges with respect to Russian IIA and discuss best practices for response. These opportunities to learn from a broader range of stakeholders can build stronger alliances to coordinate responses against threats of information warfare on a larger scale.

[93] Marjan Icoski, "Reversing the Brain Drain in the Western Balkans," German Marshall Fund, October 27, 2022, https://www.gmfus.org/news/reversing-brain-drain-western-balkans.

Through its CTR programs across Europe, the US government is uniquely positioned to share insights between countries. International organizations also can facilitate learning across countries, in addition to sharing education tools and reports that codify lessons for countering Russian IIA.

AREAS FOR INVESTMENT

To expand societal resilience to counter Russian IIA, key stakeholders and organizations need to prioritize investing in programs to confront information manipulation in Europe. Several opportunities play an important role in building resilience and effectiveness in the long term, including: augmenting proactive measures, strengthening media literacy efforts and fact-checking programs, supporting independent media and community journalism, and prioritizing capacity-building efforts.

Augment proactive measures

Attempts to more proactively counter malign influence campaigns are an important area for additional resourcing so counter-messaging strategies are not primarily reactive. The United States and NATO are exploring ways to be more proactive in sharing research and information, including exploration of prebunking initiatives, but continued cooperation will benefit NATO allies such as Slovenia and Slovakia.[94] For Serbia, cooperation with the EU, regional partners, or nongovernmental organizations could provide insights on how to incorporate proactive measures into their counter-messaging strategies.

Strengthen media literacy efforts and fact-checking programs

Greater cooperation between journalists and government representatives can improve public awareness about the threats of Russian IIA and enhance resilience. Instituting media literacy curriculum in education systems is also important to improve resilience among younger citizens, especially those who are more active on social media and exposed to a wider variety of messaging. Additionally, fact-checking programs to promote critical engagement with information from news, television broadcasts, and social media platforms can be expanded beyond education systems to workplaces, government offices, and other environments that would benefit from increased awareness.

Support independent media and community journalism initiatives

Independent media and community journalism can play important roles in combating IIA, especially through the prioritization of localized reporting, transparency, and accountability. Through strong connections to the communities around them, media and community journalism initiatives' active engagement and collaboration with local organizations and trusted officials enhances the overall credibility of responses to Russian IIA. These organizations can highlight local solutions and positive stories that can play a role in bolstering broader support for institutions, minimizing polarization, and blunting the negative effects of disinformation.

Consider ways to measure success

Across the three countries considered for this project and in the United States, members of the communities of practice struggle with how to measure the success of responses to Russian IIA. It is impossible to isolate the effects of one message or campaign within the entire media landscape, given how much content is produced and how quickly it is distributed. It also is difficult to predict what could influence Russia to change its tactics. However, there are resources available to guide the development of attention-grabbing, impactful messages that can garner support, such as EUvsDisinfo and the Bioweapons Disinformation Monitor. Additionally, greater engagement with academia and journalism professionals can assist in developing messages backed by industry best practices and standards.

Review adequacy of cybersecurity infrastructure

In addition to concerns over false Russian narratives, Slovenia, Slovakia, and Serbia should consider whether existing cybersecurity measures are adequate to prevent cyberattacks. In the event prevention measures fail, each country should also review whether current defenses are up to date. For Slovenia and Slovakia, NATO's Strategic Communications Centre of Excellence could be a good resource to support or inform these reviews.[95]

Focus on capacity building efforts to increase effectiveness and viability across sectors

Leveraging programs to build capacity within organizations can sustain efforts, increase effectiveness, and build long-term resilience. For civil society organizations, think tanks, media

[94] "NATO's Approach to Countering Disinformation," NATO, last updated November, 8, 2023, https://www.nato.int/cps/en/natohq/topics_219728.htm; and "Countering Disinformation: Improving the Alliance's Digital Resilience," NATO, August 12, 2021, https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.

[95] "NATO Strategic Communications Centre of Excellence," NATO, 2023, https://stratcomcoe.org/.

entities, and others that are involved in countering Russian IIA, it is important to prioritize efforts that strengthen their overall ability to achieve success. To counter Russian IIA, educational programs—both within and outside of formal educational institutions—allow stakeholders to obtain important skills in digital literacy, cybersecurity, and critical thinking abilities. Professional development opportunities for analysts and journalists alike can strengthen the ability to use technologies and other tools to combat Russian IIA. For public diplomacy officials, training sessions that focus on strategic communications and crisis management provide important opportunities to implement standard operating procedures within their organizations. These kinds of programs play an important role in developing the necessary skills and experience to counter Russian IIA on nonproliferation.

Additionally, community engagement programs serve an important role in capacity building within the public. Organized workshops, outreach programs, and structured dialogues contribute to a broader sense of involvement among the community, which can increase buy-in and participation when combating Russian IIA. Community engagement programs can also empower local leaders and educators to play a role in disseminating truthful information and countering Russian IIA within the public.

PROJECT NEXT STEPS

For the next iteration of this project, the Atlantic Council's Transatlantic Security Initiative and the Department of State's Office of Cooperative Threat Reduction will continue to examine the threat of Russian malign influence efforts that target nonproliferation norms in Eastern Europe and the responses to these threats. The Atlantic Council will monitor developments in Russia's IIA for topics related to nonproliferation and CBRN weapons that might emerge in our focus countries to tailor the content of our private workshops accordingly. In addition, we will also support the organizations, experts, and entities on the frontlines of Russia's information warfare to enable implementation and sustainment of the project's overall goals.

In the next phase of our project, the Atlantic Council will continue to refine the three pillars of our strategic framework to ensure they capture the current challenges to recognizing and responding to IIA within Central and Eastern Europe, as well as any challenges to reinforcing a healthy community of practice committed to countering IIA in the region.

Finally, we will work closely with our partners at the Department of State to identify new countries that would benefit from engagement with our strategic framework.

About the authors

Natasha Lander Finch is a senior fellow with the Scowcroft Center's Transatlantic Security Initiative. She previously worked as a senior policy analyst at the RAND Corporation, where she led research on a range of issues, including chemical, biological, and nuclear policy; counterterrorism; European security; and military and civilian workforce policy. Lander Finch also served as an adviser within the Office of the Undersecretary of Defense for Policy. In this capacity, she aided the development of policy guidance influencing diplomatic, operational, and technical aspects of the international mission to remove and destroy Syria's declared chemical weapons. During her assignment at the Pentagon, Lander Finch was also the principal adviser for NATO's Committee on Proliferation in the Defense Format, where she fostered implementation of policies to protect NATO allies against threats posed by weapons of mass destruction and strengthen NATO's chemical, biological, radiological, and nuclear preparedness. For her efforts, she was twice awarded the Office of the Secretary of Defense Medal for Exceptional Public Service.

Prior to joining RAND, Lander Finch was a senior analyst and deputy program manager at BAE Systems, where she authored a variety of analytic products for US government policymakers.

Lander Finch holds a master of science in psychology and the neuroscience of mental health with distinction from King's College London, a master of public policy from George Mason University, and a bachelor's degree in journalism with a dual major in political science from Bowling Green State University. Her commentaries have been published in the Cipher Brief, National Interest, Real Clear Defense, and US News and World Report.

Ryan Arick is an associate director with the Transatlantic Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security. In this capacity, he supports the Transatlantic Security Initiative's work to strengthen the transatlantic alliance against emerging security threats from around the world. His research interests include NATO defense policy and transatlantic security; arms control, disarmament, and nonproliferation; democratic resilience from foreign malign influence; and state fragility and conflict prevention.

Previously, he served as an assistant program officer with the International Forum for Democratic Studies at the National Endowment for Democracy (NED), where he supported NED's transnational kleptocracy and democratic resilience portfolios. Earlier, he worked with the National Democratic Institute's Central and Eastern Europe division, where he supported democracy programs in the Western Balkans as well as cross-regional grants to promote pluralism and good governance. He graduated from Indiana University with a bachelor of science in public affairs.

Appendix I: Acronyms and key definitions

ACRONYM LIST

BWC	Biological weapons convention
CBRN	Chemical, biological, radiological, and nuclear
CTR	Cooperative threat reduction
CWMD	Countering weapons of mass destruction
DCA	Defense cooperation agreement
DTRA	Defense Threat Reduction Agency
GEC	Global Engagement Center (US Department of State)
EU	European Union
IIA	Information influence activities
ISN	Bureau of International Security and Nonproliferation (US Department of State)
OPCW	Organization for the Prohibition of Chemical Weapons
OSCE	Organization for Security and Cooperation in Europe
TSI	Transatlantic Security Initiative
WMD	Weapons of mass destruction

KEY DEFINITIONS

NONPROLIFERATION:

All efforts to prevent proliferation from occurring, or should it occur, to reverse it by any other means than the use of military force. Nonproliferation applies to weapons of mass destruction (WMD), including chemical, biological, radiological, and nuclear (CBRN) weapons and conventional capabilities (e.g., missiles and small arms).[96]

NONPROLIFERATION NORMS:

Shared values against the development and use of WMD. Established by a global network of treaties and international organizations against WMD proliferation, bolstered by bilateral and multilateral diplomacy.[97]

NONPROLIFERATION REGIMES:

The broad international framework of agreements and organizations aimed at preventing the spread of CBRN weapons and contributing to arms control and disarmament progress.[98]

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR WEAPONS:

Include materials, articles, or devices explicitly banned by the Non-Proliferation Treaty, Chemical Weapons Convention, Biological Weapons Convention, or other international treaty.[99]

DISINFORMATION:

False or misleading information that is intentionally created, presented, and disseminated to deceive or mislead the public.[100]

[96] "Arms Control, Disarmament, and Non-proliferation in NATO," NATO, last updated February 27, 2023, https://www.nato.int/cps/en/natohq/topics_48895.htm.

[97] US Department of State, *Functional Bureau Strategy*, Bureau of International Security and Nonproliferation, Department of State, February 2, 2022, https://www.state.gov/wp-content/uploads/2022/08/FBS_ISN_Public.pdf.

[98] "Nonproliferation Regime," Nuclear Threat Initiative, last updated December 2023, https://tutorials.nti.org/nonproliferation-regime-tutorial/.

[99] "NATO's Chemical, Biological, Radiological, and Nuclear (CBRN) Defence Policy," NATO, last updated July 5, 2022, https://www.nato.int/cps/en/natohq/official_texts_197768.htm.

[100] "Technology and Innovation: Disinformation," Atlantic Council, last updated December 2023, https://www.atlanticcouncil.org/issue/disinformation/.

MISINFORMATION:

False or misleading information that is spread unintentionally.[101]

MALINFORMATION:

Information built around truth and facts but taken out of context or otherwise misleading to inflict harm.[102]

PROPAGANDA:

Information, especially of a biased or misleading nature, used to promote or publicize a particular political cause or point of view.[103]

INFORMATION INFLUENCE ACTIVITIES:

Culmination of information tactics (including disinformation, misinformation, malinformation, and propaganda) intended to sow confusion in public dialogue, exacerbate political polarization, and promote distrust in political systems and democratic institutions.[104]

[101] James Pamment, "A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference," NATO Strategic Communications Centre of Excellence, December 5, 2022, https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255.

[102] How to Identify Misinformation, Disinformation, and Malinformation," Canadian Centre for Cyber Security, February 2022, https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.

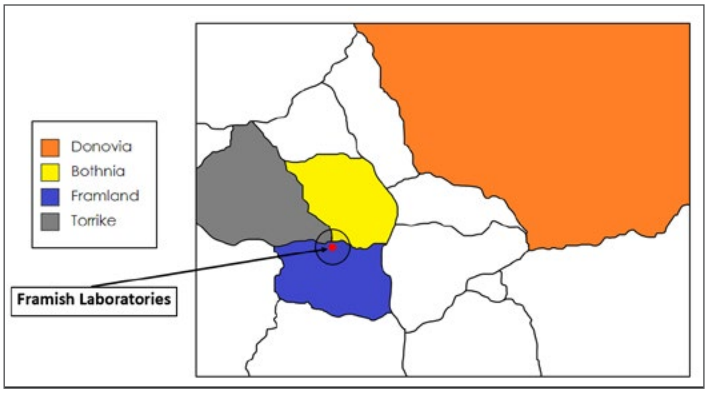
[103] Dean W. Jackson, "Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News,' " National Endowment for Democracy, October 17, 2017, https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/; and "Understanding Propaganda and Disinformation,“ European Parliament, November 2015, https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2015)571332.

[104] The Atlantic Council's Transatlantic Security Initiative used a combination of definitions in reference to Russian information influence activities, including the following sources: "Technology and Innovation: Disinformation," Atlantic Council, last updated December 2023, https://www.atlanticcouncil.org/issue/disinformation/; Pamment, "A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference"; "How to Identify Misinformation, Disinformation, and Malinformation," Canadian Centre for Cyber Security; Jackson, "Issue Brief: Distinguishing Disinformation"; "Understanding Propaganda and Disinformation,“ European Parliament.

Appendix II: Hypothetical scenario-based exercise details

The Atlantic Council's Transatlantic Security Initiative developed a hypothetical, scenario-based exercise for the first series of workshops in this project. The scenario is based on actual events, but uses fake countries and locations adapted from US Army training materials to promote openness and creative thinking. The goal was to remove cognitive constraints on participants that would limit their responses to their own experiences or country borders. Workshop participants were provided with the following description and discussion questions to guide their small-group deliberations.

SCENARIO EXERCISE BACKGROUND INFORMATION



Framland is a small country in Central Europe with a stable economy led by a constitutional monarchy, with a prime minister appointed to lead the country.[105] Its all-volunteer force is small but well regarded for its professionalism by UN missions it has supported. Framland is not a member of the European Union or NATO, but it enjoys good relations with its neighboring countries, including Torrike and Bothnia. Framland also engages in diplomacy with the United States and NATO. Donovia, a resurgent former regional power, is attempting to reassert itself through a combination of military, diplomatic, and information influence activities.[106] These efforts include disinformation attempts in Central Europe, including in Framland. Donovia's information influence activities seek to incite confusion in public dialogue, exacerbate social polarization, and promote distrust within Framland's political systems and democratic institutions.

Framland has a biosafety level three (BSL-3) laboratory near its borders with Torrike and Bothnia called Framish Laboratories.[107] BSL-3 laboratories are used to study agents that can be transmitted through air. These agents can cause lethal infection. The Framish entity maintains a secure stockpile of one of these agents, live anthrax spores, for peaceful research purposes.[108] Anthrax derives from a naturally occurring bacteria that is spread through air to humans or animals but is not contagious.

Framish Laboratories' scientists participate in regional conferences and publish reports on their research to promote information sharing about infectious diseases and other concerns in their region. As part of a regional biological cooperation project, Framland has received US training and support since 2010 to improve their laboratory capabilities and enhance biosecurity at Framish Laboratories. Torrike and Bothnia also receive US assistance through this project.

Recently, Donovia has published news articles and social media posts that falsely claim the United States is funding bioweapons research at Framish Laboratories. These reports are part of Donovia's strategy to undermine public confidence in legitimate institutions within countries Donovia perceives are being controlled by the United States, including Framland. Donovia also claims that the anthrax samples are improperly stored and at risk of infecting local populations. Although the claims are unsupported, Donovia's false messages have prompted fears within the population, especially among those who were previously unaware of Framish Laboratories and are only now learning about its research activities. The information influence

[105] "Framland," OE Data Integration Network (ODIN), US Army Training and Doctrine Command, 2023, https://odin.tradoc.army.mil/DATE/Europe/Framland.

[106] "Donovia," ODIN, 2023, https://odin.tradoc.army.mil/DATE/Caucasus/Donovia.

[107] "Biosafety Labs," National Institute of Allergy and Infectious Diseases, US National Institutes of Health (NIH), last updated May 12, 2011, https://www.niaid.nih.gov/research/biodefense-biosafety-labs; and "Disease and Laboratory Networks," European Centre for Disease Prevention and Control, 2023, https://www.ecdc.europa.eu/en/about-ecdc/what-we-do/partners-and-networks/disease-and-laboratory-networks.

[108] "What Is Anthrax?" US Centers for Disease Control and Prevention, last updated February 15, 2022, https://www.cdc.gov/anthrax/basics/index.html.

activities have become a serious concern to officials in Torrike and Bothnia as well; these countries are seeking reassurance that Framish Laboratories are following necessary safety protocols given the laboratories' location in the triborder area.

Donovia's information influence activities in Framland related to Framish Laboratories build off preexisting disinformation efforts to undermine Framland. These narratives include false news articles and social media posts about Framish government institutions and civil society groups. In addition, Donovia also frequently targets Framland's cooperation with its neighboring states as well as with multilateral alliances and institutions.

Framish authorities have been working on public messaging efforts to counter Donovia's false claims about Framish Laboratories. These messages emphasize Framish Laboratories' long history of safety and the transparency they demonstrate by publishing peer-reviewed articles about their work. Their approach to countermessaging is based on previous efforts to develop counternarratives against other Donovian disinformation efforts. However, many Framish citizens get their news from internet sources and use social media to communicate and share ideas, which has made it difficult for Framish authorities to control the spread of Donovia's false claims and their own counternarratives.

Part I

One perpetual claim from Donovia is that researchers at Framish Laboratories are developing biological weapons, despite a lack of credible evidence to support this claim. Your strategic communications firm has been asked by the Framish government to develop a messaging strategy to counter these narratives. Questions to consider include:

- What information about Framish Laboratories' activities do you want to convey to reassure public trust?
- How do you bring in various stakeholders from across Framland (e.g., think tanks, nongovernmental organizations, government ministries, media organizations, academia) to promote greater cooperation to combat Donovia's information influence activities?
- What medium(s) are best suited for your messaging campaign (e.g., social media, online newspapers, via spokespeople, fact sheets)? How might you reach audiences that may be more susceptible to Donovia's efforts?

Part II

Your counter-messaging strategy to debunk Donovia's false claims about bioweapons development at Framish Laboratories appears to have stopped additional Donovian attacks for now. However, two laboratory technicians have recently sought treatment at a local hospital for exposure to a substance at Framish Laboratories. The technicians were found to have been exposed to anthrax due to poor laboratory safety procedures. They were the only two people involved in the exposure and the incident was contained inside the BSL-3 laboratory. The technicians were treated for their symptoms and released from the hospital.

Framish Laboratories closed for two days following the incident for mandatory safety training for all employees. However, this is the first instance of exposure to a dangerous pathogen at Framish Laboratories, which has worried some. The neighbor of one of the technicians created a social media post that stoked fears about possible exposure to anthrax. This post was picked up by Donovia and recirculated as "evidence" to renew its efforts to discredit Framish Laboratories.

Framish Laboratories has asked your firm to assist with a messaging strategy to assure the public they are not in danger. Questions to consider include:

- Are there elements of your first messaging strategy that you can adapt to address this incident? How does the anthrax exposure incident affect Framland's response to the new information influence activities?
- How do you view the recent developments changing the collaboration needed from across Framland in the previous scenario to combat Donovia's information influence activities?
- Given Framish Laboratories' proximity to Bothnia and Torrike, how can your messaging reassure Framland's neighbors that Framish Laboratories is committed to safety? Does your strategy change when addressing your message to the US, European Union, or NATO officials?

Atlantic Council

Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org