alliance for securing democracy

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Policy Paper

August 2019 | No.21

AVOIDING THE BAND-AID EFFECT IN INSTITUTIONAL RESPONSES TO DISINFORMATION AND HYBRID THREATS

NINA JANKOWICZ

Executive Summary

Since 2014, a variety of initiatives have been created in response to the rise of Russian interference in democracies. Some of the organizations, while created as answers to a real and increasingly exigent danger, began their work without a clear mandate or political will behind them. As a result, their work has not always been fully effective, falling subject to "Band-Aid Effect" in which the creation of new bodies to address the complex problem of foreign interference in democracies is viewed—whether by the convening institution, the media, or the public—in itself as a panacea.

Through a study of six key unilateral and multilateral efforts in Europe to counter disinformation and hybrid threats, this paper identifies best practices and pitfalls in establishing such bodies. It assesses the extent to which they are integrated into meaningful policy- and decision-making processes, the extent to which they coordinate across government and with each other, and the extent to which they are meeting public-facing program objectives.

The six efforts profiled in this paper are diverse in form and approaches, and they have achieved success in building awareness about the problem among the public and policymakers. They have also faced a variety of obstacles. Attempts to set up similar efforts can extrapolate from their experience the following best practices so as to avoid "The Band-Aid Effect" in building up new institutions.

Secure vertical and horizontal buy-in to policies and objectives

Organizations that face criticism or lack vocal public support from high-level officials face a variety of administrative challenges. Their financial and human resources are precarious, making long-term strategic planning difficult. Horizontal coalition building across government and bodies is also integral; organizations or efforts that have a wide membership or supporter base are more effective in the coordination and amplification of efforts, and face less risk of being stymied or siloed through turf wars.

Obtain medium-term funding commitments when possible

A lack of financial stability can stymie effective work. While the inclination of many donor bodies or budget stewards to measure success over the short-term is understandable, the Russian government's interference operations continue to be funded at levels far greater than Western efforts to counter them. The budget for the Russian state-run media organization RT, for example, was over $300 million in 2018–2019. The West need not attempt to match this spending, but funding should be allocated in the medium-term to allow bodies to mount a more strategic response to Russian actions. Efforts with meager budgets should aim to coordinate with other organizations wherever possible in order to maximize their resources and amplification of programming.

Utilize existing structures and policymaking processes to avoid administrative obstacles

Creating a new body from scratch is challenging; securing a budget, recruiting qualified staff, and solidifying objectives take more time when starting from the ground level. Organizations and efforts that utilize existing structures can deliver an agile and wide-reaching response in a short time, compared with new organizations, which spend much of their first years standing up their efforts.

Define a clear mission and goals against which to measure success

Organizations should focus their energies on a clear mission. Given that most counter-disinformation and counter-hybrid threat efforts draw upon meager resources, it is important to identify the explicit objectives

against which new ones will deliver so that resources can be best allocated. However, organizations and governments should avoid the lure of linking their efforts to a single event. Russian government attempts to influence societies through disinformation and hybrid threats are built up over years, aiming to increase chaos and confusion. They are not pegged to one election or referendum; neither should the goals of organizations responding to them.

Manage the expectations of the press and the public by prioritizing communication

Most of the organizations studied suffer from a gap in understanding or expectations from the public or the media. It is important for them to conduct transparent, truthful, and regular outreach in order to raise awareness of the threat and increase resilience to it, but also to maintain a clear understanding of the expectations and limits of the organizations countering them. Neglecting to prioritize communications as a key part of the national security response to Russian disinformation and hybrid threats in democracies can undermine efforts before they even begin.

Most importantly, as the United States and others continue to institutionalize their responses to Russian government—and, increasingly, other countries'—disinformation and hybrid threats, they need not reinvent the wheel. There is much to be learned from years of work toward similar goals already underway. Ignoring these experiences could lead states toward adopting Band-Aid solutions that may address parts of the problem temporarily, but in the long-term will fail to heal deeper wounds.

Avoiding the Band-Aid Effect in Institutional Responses to Disinformation and Hybrid Threats

NINA JANKOWICZ

In 2014, national-security priorities across Europe shifted as a result of Russia's illegal annexation of Ukraine's Crimean peninsula, the shooting down of passenger airliner MH17 by Russian-backed separatists over eastern Ukraine, and the firestorm of Kremlin-propagated disinformation surrounding the subsequent war. Over the following years, Russian interference in electoral processes in the United Kingdom, the United States, Germany, and other Western countries have brought the issues of countering disinformation, and more broadly, the Russian hybrid toolkit to the forefront of national-security strategies across the Euro-Atlantic space. These issues have become a priority for hundreds of governmental and civil society organizations throughout and beyond the transatlantic community.

A variety of unilateral and multilateral initiatives have been created in direct response to the threat. While created as answers to a real and increasingly exigent danger, some have been stood up without a clear mandate or political will from the government or the multilateral institution in which they are housed. As a result, their work can be stymied or dampened for fear of attracting unwanted attention from internal political adversaries.

The resulting phenomenon can be dubbed the "Band-Aid Effect." This reflects the creation of new bodies to address the complex problem of foreign interference in democracies is viewed—whether by the convening institution, the media, or the public view—in itself as a panacea. Reports of a lack of cooperation between institutions, funding delays, and narrow or misguided foci have rendered some of these initiatives less effective, as a Band-Aid would be less effective at healing a deep cut than stitches.

Through an inventory of six key unilateral and multilateral effort in Europe to counter disinformation and hybrid threats, this paper identifies best practices and pitfalls in establishing such bodies. It assesses the extent to which they are integrated into meaningful policy- and decision-making processes, the extent to which they coordinate across government and with each other, and the extent to which they are meeting public-facing program objectives. Finally, it makes recommendations for the further development of government programs and policies aimed at countering disinformation and hybrid threats.

Methodology

The six case studies for this paper were chosen as a sample of national (U.K., Czech, and Swedish) efforts and multilateral (under EU and NATO umbrellas) initiatives. They represent a range of approaches to the problem, as well as a variety of obstacles. Four of the organizations are new efforts: NATO's Strategic Communications Center of Excellence, the EU vs Disinfo initiative based in the European External Action Service's East StratCom Task Force, the European Center of Excellence for Countering Hybrid Threats, and the Center Against Terrorism and Hybrid Threats of the Czech Republic's Ministry of Interior. The Civil Contingencies Agency in Sweden and the cross-governmental U.K. "Fusion Doctrine" efforts use existing structures to approach the problem.

The case studies have been analyzed and evaluated based on publicly available official documents and communications. While this paper attempts to assess cross-governmental and cross-organizational coordination, doing so on the basis of open-source information was often difficult, as much of the relevant material remains classified. English-language press coverage from reputable sources was also reviewed in order to ascertain the expectations for each effort, and how the coverage may or may not have affected the assessment of the organizations' achievements or created gaps in expectation. Finally, the paper is also based on the author's own observations and interviews on background with staff of four of the organizations. Two organizations declined interview requests.

NATO Strategic Communications Center of Excellence

The NATO Strategic Communications Center of Excellence (StratCom COE), in Riga, Latvia was established in 2014. As of this writing, NATO has accredited 25 centers of excellence that "specialize in one functional area and act as subject-matter experts in their field. They distribute their in-depth knowledge through training, conferences, seminars, concepts, doctrine, lessons learned and papers,"[1] of which the StratCom COE is one. COEs are "multi-nationally constituted and NATO-accredited international military organization[s], which [are] not part of the NATO Command Structure, nor subordinate to any other NATO entity."[2] The overall concept for NATO COEs was introduced after the Prague summit in 2002, when Allied Command Transformation was created to "[transform] the Alliance into a leaner, more efficient organization."[3]

The StratCom COE was established to assist the alliance in addressing the evolving challenge of strategic communications in the age of disinformation and hybrid threats. When it was launched in 2014, "the greatest perceived security threat to the alliance was the rapid spread of the Islamic State's brand of terrorism."[4] Soon after, with Russia's illegal annexation of Ukraine's Crimean peninsula and the beginning of its proxy war in eastern Ukraine, the center's focus shifted to Russia.

On its website, the StratCom COE describes the challenges of its field: "Today's information environment, characterized by a 24/7 news cycle, the rise of social networking sites, and the interconnectedness of audiences in and beyond NATO nations territory, directly affects how NATO actions are perceived by key audiences."[5] The center brings together experts in public diplomacy, public affairs, military public affairs, information operations, and psychological operations to increase the alliance's collective ability to carry out more effective strategic communications. Activities in support of this goal include "comprehensive analysis, timely advice, practical support [and] training for governments on strategic communication."[6]

The center's member countries[7] contribute to its budget and staff, and determine its lines of effort. Along with NATO itself, members can request specific research projects, request trainings on strategic communications for components of their domestic apparatus, and solicit the COE's operational support. As the center's director, Janis Sarts, stated in 2017, "We try to give the knowledge to the governments and probably from that understanding, some ideas which we say are best to counter these kinds of situations."[8] As of early 2019,

1 NATO. 2019. "Centres of Excellence." Last modified 24 January 2019. https://www.nato.int/cps/en/natohq/topics_68372.htm#

2 NATO StratCom COE. 2019. "FAQ." https://www.StratComcoe.org/faq

3 NATO 2019.

4 Sander, Gordon F. 2017. "Latvia's Fortress Think Tank." Politico. March 16, 2017. https://www.politico.eu/article/latvias-fortress-think-tank/

5 NATO StratCom COE. 2019. "About Strategic Communications." https://www.StratComcoe.org/about-strategic-communications

6 NATO StratCom COE. 2019. "About Us." https://www.StratComcoe.org/about-us-0

7 Latvia, Estonia, Germany, Italy, Lithuania, Poland, and the United Kingdom were founding members; Canada, Finland, the Netherlands, and Sweden joined later. At the time of writing, France and Slovakia were finalizing their membership. The United States has yet to join the COE and to second staff, but it sent a researcher to the center under the Fulbright program in 2019.

8 National Public Radio. 2017. "NATO Takes Aim at Disinformation Campaigns." https://www.npr.org/2017/05/10/527720078/nato-takes-aim-at-disinformation-campaigns

the COE consisted of five operational branches: doctrine, concept, and experimentation; education and training; operational support; technical and scientific development; and framework nation support.[9]

Activities

The NATO StratCom COE claims a variety of achievements related to Russian disinformation and hybrid warfare in its public reports.[10] In launching and publishing an annual peer-reviewed academic journal, *Defense Strategic Communications*, it contributes to the body of public research in this area. The COE conducted key studies on topics including the use of robotrolling; Russian disinformation narratives across the Baltic states, Ukraine, and most recently, the Balkans; and the use of humor in countering disinformation. Along with partners such as the U.K. Ministry of Defense Joint Activities Team, it has conducted training activities for NATO members and allies, as well as in Georgia, Moldova, and Ukraine, which are aspiring members and victims of Russian disinformation. The center also convenes public events and organizes outreach activities in the transatlantic arena.

Obstacles

Fully staffing the NATO StratCom COE was a slow process, as most employees are funded and seconded by the center's members and finding individuals with the necessary backgrounds can be challenging. In 2015, the center noted in its annual report that "the Operational Support Branch and the Education and Training Branch were understaffed for the better part of the year."[11] The center saw an uptick in its staffing in subsequent years as member states joined it.

Coordination

Since its inception, the NATO StratCom COE has actively sought to coordinate with other centers of excellence within and outside of the structures of regular multinational cyber and military exercises. Additionally, at the request of Allied Command Transformation and the COE Directors, it helped develop a common strategic communications directive for NATO. It also coordinates with structures in allied governments, including the U.K. Ministry of Defense, with several Latvian organizations, and with governments in NATO's periphery, including those of Georgia, Moldova, and Ukraine.[12]

However, based on public reports and interviews with staff, there appears to be less public coordination and cooperation between the StratCom COE and its counterparts in the European Union, including the European External Action Service's StratCom East Task Force, which houses the EU vs. Disinfo initiative, and the joint NATO-EU European Centre of Excellence for Countering Hybrid Threats in Helsinki, which was launched in 2017.

> *"Since its inception, the NATO StratCom COE has actively sought to coordinate with other centers of excellence.*

Press Coverage and Public Awareness

Most of the coverage of the NATO Stratcom COE's efforts by reputable news sources has been positive, based on articles in several large English-language outlets. However, some of the coverage lacks depth of understanding about the center's mission and activities, painting it as NATO's weapon in the

9 NATO StratCom COE. 2019. "Structure." https://www.StratComcoe.org/structure

10 At the time of writing, reports for 2018 have not been released.

11 NATO StratCom COE. 2016. "NATO Strategic Communications Center of Excellence, Annual Report (1 January 2015—31 December 2015). 31 March 2016. https://www.StratComcoe.org/audited-annual-report-2015

12 NATO StratCom COE. 2016.

fight against Russian disinformation.[13] The COE's presence among descriptions of counter-intelligence activities gives the impression that it is engaged in the front lines of information warfare, when its mission is academic in nature. In reality, the center informs and equips NATO to be more effective in fighting disinformation, with a secondary mission of building public awareness about the tools and tactics of Russia and other malign actors in the transatlantic space. To its credit, the COE has always maintained clarity in interviews with the press about its mission and remit, a practice that helps protect against unfulfilled expectations in the broader public.

Analysis

The NATO StratCom COE maintains research partnerships with academic institutions including Kings College London, which hosts a Centre on Strategic Communications and several degree programs in the field, situating it at the forefront of thinking on the topic of disinformation. The body of reputable academic research that it has produced since its inception is formidable and well regarded by experts. The COE also appears to be well-integrated in NATO and Allied Command Transformation structures, supporting the creation and updates of NATO doctrine related to strategic communications and assisting the alliance and its partners in war games, exercises, and trainings each year.

The center's successes are due in part to its genesis; it would not exist without buy-in from NATO leadership and a group of members invested in advancing its mission. This multinational model is exemplary, but also not necessarily attainable for other bodies for which membership is not self-selecting. What is more, NATO members that are more skeptical of Russian disinformation and hybrid threats such as Greece or Hungary, are not COE members. The center is a coalition of the willing, and therefore the breadth of its potential impact is somewhat reduced. That said, its network of supporting nations has increased each year and is on track to continue to do so, amplifying its efficacy and impact.

On a similar note, the COE should aim to strengthen coordination outside of the NATO community, and in particular the European Union in order to amplify both organizations' meager resources.

EEAS East StratCom Task Force—EU vs. Disinfo

A year after Russia's illegal annexation of Ukraine's Crimean peninsula, European Union leaders stressed at a meeting of the European Council:

> the need to challenge Russia's ongoing disinformation campaigns and invited the High Representative, in cooperation with Member States and EU institutions, to prepare by June an action plan on strategic communication. The establishment of a communication team is a first step in this regard.[14]

Later that year, the European Union External Action Service (EEAS) established its East StratCom Task Force to meet this need. Its objectives, as outlined in the June 2015 Action Plan on Strategic Communication, are:

- Effective communication and promotion of EU policies towards the Eastern Neighbourhood;
- Strengthening the overall media environment in the Eastern Neighbourhood and in EU Member States, including support for media freedom and strengthening independent media;

13 See Anna Nemtsova, "The Baltics Try to Wall Out Russian Agents, but Moscow's Message Still Comes Through," *The Daily Beast* (https://www.thedailybeast.com/russias-fear-abroad-the-baltics-try-to-wall-out-russian-agents-but-moscows-message-still-comes-through).

14 European Council. 2015. "European Council meeting (19 and 20 March 2015)—Conclusions." 20 March 2015. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

- Improved EU capacity to forecast, address and respond to disinformation activities by external actors.[15]

The task force team is composed of one unit focused on better communicating EU priorities and policies to the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine) as well as providing media programming, and the EU vs. Disinfo unit, where a small group works to track Russian government-sponsored disinformation.[16]

> *"EU vs Disinfo's research and documentation efforts were instrumental in changing the debate about Russian disinformation and hybrid threats.*

The latter's main product is a weekly newsletter of crowdsourced pieces of Russian-aligned disinformation from across the EU and Eastern Partnership. These instances are catalogued in a publicly accessible database and categorized by date, topic, outlet, and countries concerned.[17] Members of the team also "brief and train EU institutions, Member State governments, journalists and researchers on this topic, and participate regularly in conferences to share [their] experience."[18]

All team members are seconded from EU member states or recruited from within EU institutions. The East StratCom Task Force received a dedicated operating budget of €1.1 million only in 2018.[19] An additional €800,000 were moved from other parts of the EEAS budget to the Task Force the same year.[20] In late 2018, the European Commission released an updated *Action Plan against Disinformation* ahead of the European Parliament elections in May 2019.[21] In addition to increased human resources, the plan allocates €5 million to the task force in 2019. Among other objectives, the increased funds are envisaged to contract additional media-monitoring services and data-mining software to assist in tracking disinformation during the election period.

Activities

According to the *Action Plan on Disinformation*, EU vs. Disinfo "has catalogued, analysed and raised awareness of over 4,500 examples of pro-Kremlin disinformation, and significantly improved understanding of the tools, techniques and intentions of disinformation by Russian sources."[22] Its online database of Russian disinformation is a useful tool for researchers, practitioners, and educators as they work to further understand and track the threat.

EU vs Disinfo's research and documentation efforts were instrumental in changing the debate about Russian disinformation and hybrid threats within the European Parliament and EU institutions. This is evident in the adoption of the action plan, which clearly names Russia as a threat actor even though "some countries didn't really feel the threat," as an unnamed EU official said in 2017.[23]

15 EEAS. 2015. "Questions and Answers about the East StratCom Task Force." Last updated 5 December 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-StratCom-task-force_en

16 At this writing, the East StratCom team had 11 employees, and EU vs Disinfo had five.

17 EU vs. Disinfo. 2019. "Disinformation Cases." https://euvsdisinfo.eu/disinformation-cases/

18 EU vs. Disinfo. 2019. "About." https://euvsdisinfo.eu/about/

19 European Commission. 2018. "Questions and Answers—The EU steps up action against disinformation." 5 December 2018. http://europa.eu/rapid/press-release_MEMO-18-6648_en.htm

20 Boffey, Daniel and Jennifer Rankin. 2017. "EU Escalates its Campaign Against Russian Propaganda," *The Guardian*, 23 January 2017. https://www.theguardian.com/world/2017/jan/23/eu-escalates-campaign-russian-propaganda

21 EEAS. 2018. "Action Plan Against Disinformation." 5 December 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/54866/action-plan-against-disinformation_en

22 Ibid.

23 McDonald-Gibson, Charlotte. 2017. "The E.U. Agency Fighting Russia's Wildfire of Fake News with a Hosepipe." *Time*. 11 September 2017. http://time.com/4887297/europe-fake-news-east-stratcom-kremlin/

Obstacles

However, EU vs Disinfo and the wider East StratCom Task Force have faced several obstacles in the pursuit of their objectives. As noted above, funding and staffing the team has been a struggle since its inception. Laima Andrikiene, a member of the European Parliament from Lithuania, drew attention to this in 2018: "In 2015 East StratCom had only one officer working to fight the Russian information war, now there are 14 people doing this job, but their positions are temporary and may not be renewed this summer. While I admire their work, they are the EU's David to Russia's Goliath in this fight."[24]

> *"EU vs Disinfo and the wider East StratCom Task Force have faced several obstacles in the pursuit of their objectives.*

Even considering the increase in resources allocated to the team ahead of the European Parliament elections, the team is underfunded when considering that the EU represents the world's second-largest economy. Comparatively, a single part of the task force's adversary, the Russian government's propaganda network RT, has an operating budget that runs in the hundreds of millions of dollars.[25]

EU vs. Disinfo also had to contend with legal obstacles in 2018, when three Dutch websites that published articles the team had labeled as "disinformation" brought a suit against the EU, claiming that their stories had been mislabeled. They argued the site should "remove those accusations from all of their publications and publish a correction, under penalty of a €20,000 fine per day the content remains online."[26] The three articles were found to have been wrongly included in the disinformation database and were removed. EU vs. Disinfo issued a retraction and the legal suit was dropped.[27] The Dutch parliament, however, took issue with the errors and even passed a resolution demanding the task force be shuttered. Others said that the program's fact-checking methodology was not transparent and should be amended if it was to be allowed to continue operating at the EU level.[28]

Coordination

The EU vs Disinfo staff make regular appearances at conferences on disinformation across the region. The wider task force claims to work "closely with the EU institutions, EU Delegations, Member States, and a wide range of other partners, both governmental and non-governmental, within the EU, in the Eastern Neighbourhood, and beyond."[29] Its fact-checking work, crowdsourced by independent volunteers, is by its nature cooperative, and is amplified by several civil society organizations throughout the EU and Eastern Partnership.

Press Coverage

Given that until recently the EU was reluctant to publicly recognize the threat of Russian disinformation, press coverage of East StratCom Task Force and EU vs. Disinfo has been mixed. Specifically, after the Dutch legal suit and subsequent parliamentary resolution, commentators questioned whether a multilateral institution such as the EU should be engaged in fact-checking work at all. According to Peter Burger, the coordinator of a news-checking initiative at Leiden University, the

24 Andrikiene, Laima. 2018. "We still need East StratCom against Kremlin Trolls." *EUObserver*. 7 June 2018. https://euobserver.com/opinion/142022

25 The Moscow Times. 2014. "Looking West, Russia Beefs Up Spending on Global Media Giants." 23 September 2014. https://themoscowtimes.com/articles/looking-west-russia-beefs-up-spending-on-global-media-giants-39708

26 Funke, Daniel. 2018. "Three publications are suing the EU over fake news allegations." Poynter. 28 February 2018. https://www.poynter.org/fact-checking/2018/three-publications-are-suing-the-eu-over-fake-news-allegations/

27 EU vs. Disinfo. 2018. "Removal of three cases further to complaints by Dutch media." 8 March 2018. https://euvsdisinfo.eu/removal-of-three-cases-further-to-complaints-by-dutch-media/

28 Schulz, Teri. 2018. "EU counter-disinformation efforts in disarray." *Deustche Welle*. 11 April 2018. https://www.dw.com/en/eu-counter-disinformation-efforts-in-disarray/a-43285144

29 EEAS 2018.

Task Force is "much too close to the policymakers to come across as independent. We should be prepared for disinformation campaigns … so we need disinformation watchers to inform the public, preferably independent from—but, if necessary, funded by—governments."[30] In 2018, the academic and activist Alberto Alemanno filed an administrative complaint claiming that the task force's methodology was not transparent. He recommends that "the EEAS should develop and make public (1) a methodology for selecting partnerships and reviewing fact-checks in line with international standards and (2) a notice and response mechanism for journalists, publishers and citizens whose content is being reviewed."[31]

Analysis

The East StratCom Task Force's shoestring budget—and the fraction of that dedicated to EU vs Disinfo—hamper its effectiveness. The EU will never choose to match the Russian government's information operations budget, but neither should it run the East StratCom Task Force on fumes, relying on reports from a network of volunteers to fuel its disinformation review. The sum of €5 million over the course of a year is a low price to put on the protection of democratic discourse. The EU should consider increasing its investment over a several-year period so that the team might better implement a strategic plan focused not only on communicating EU goals, media resilience, and EU vs. Disinfo's work of cataloguing, fact-checking, and awareness-raising, but a broader scope of programming and output focused on its own citizens.

This sort of outreach is currently impossible because, as a part of the EEAS, the East StratCom Task Force focuses on communicating with non-EU citizens. But, as Laima Andrikiene wrote, "its primary goal is to address misinformation within the EU, not to liaise with external actors."[32] The new *Action Plan on Disinformation* contains more of a proactive approach in communicating with EU citizens, highlighting "raising awareness and improving societal resilience" as one of the four pillars of the EU's response. These activities are placed at the level of the European Commission and member states, though, and do not seem to include coordination with or support from the East StratCom Task Force.[33] The EU would do well to better integrate these efforts with the expertise in the EU vs. Disinfo Unit.

The Czech Republic's Center Against Terrorism and Hybrid Threats

The Czech Republic was among the first countries to launch a domestic effort to counter Russian disinformation and other hybrid threats, opening the Center Against Terrorism and Hybrid Threats (CTHT) within the Ministry of Interior in January 2017.

The CTHT was created in response to a 2016 National Security Audit in which hybrid threats were listed as one of the primary national security concerns.[34] The audit's focus, however, was less on Russian disinformation than internal problems in Czech society; five of its ten chapters are directly related to Islamophobia and extremism in the country. The report asserts that these societal fissures are weaponized by foreign powers, including Russia, as part of a hybrid warfare toolkit, the deployment of which may result in the "radicalization of the public" and "rise of extremist and anti-system attitudes (threatening Czech interests) within society and among political representatives."[35] In addition to training programs for potential targets of foreign influence, such as diplomats and other government officials serving abroad, and a short section on media literacy programs in elementary

30 Funke 2018.

31 Alemanno, Alberto, Justine Brogi, Maxime Fischer-Zernin, and Paige Morrow. 2018. "Is the EU Disinformation Review Compliant with EU Law? Complaint to the European Ombudsman About the EU Anti-Fake News Initiative." HEC Paris Research Paper No. LAW-2018-1273. 28 March 2018. https://ssrn.com/abstract=3151424

32 Andrikiene 2018.

33 EEAS 2018. Page 12.

34 Ministry of Interior of the Czech Republic. 2016. "National Security Audit." http://www.mvcr.cz/cthh/clanek/audit-narodni-bezpecnosti.aspx

35 Ministry of Interior of the Czech Republic. 2016.

and secondary schools, the audit recommended the establishment of "departments within relevant government institutions for the evaluation of disinformation campaigns and other manifestations of foreign power influence."[36]

Beginning in 2015, disinformation in the Czech media space concerned the European migration crisis, an issue directly within the Ministry of Interior's portfolio. As such, the ministry houses the CTHT. The center's mission statement states:

> given the competencies of the Ministry of the Interior, the Center not only monitors threats directly related to internal security…but also disinformation campaigns related to internal security. Based on its monitoring work, the Centre evaluates detected challenges and comes up with proposals for operational and legislative solutions that it also implements where needed. It also disseminates information and spreads awareness about the given issues among the general and professional public.[37]

It operates with a staff of about 20 and acts as neither a law enforcement agency nor an intelligence service; it has only the authority to observe, analyze, and communicate. It uses its Twitter account to communicate about debunked disinformation narratives and also conducts research and training.

Activities

Among its achievements during its first year of existence,[38] the CTHT claims to have "actively used its Twitter account to address current events relating to hybrid threats in both Czech and English, and debunked 20 cases of serious disinformation relating to Czech internal security." It underlines, however, that "90% of [its] work remained non-public," including the production of internal analytical materials.[39]

The CTHT also underlines its contribution to public discourse through direct responses to citizen inquiries, participation in conferences, and contributions to foreign and domestic media. It supported four conferences on strategic communications, organized with a local think tank. The conferences brought together transatlantic experts on the topic and served to increase cooperation and consultation among attendees.

> *"The CTHT's major obstacle is an ongoing crisis of political will that began before its official launch.*

Obstacles

The CTHT's major obstacle is an ongoing crisis of political will that began before its official launch. Despite signing CTHT into existence, President Milos Zeman singled it out in his annual Christmas address in 2017, days before it was set to open. Drawing on sensitivities from the not-so-distant communist era, he said: "We do not need censorship, we do not need idea police," despite the fact that censorship was not in the center's mandate.[40] Zeman's comment invited criticism of the center from his party's ranks and the press, and the CTHT spent much of its first year defending itself from uninformed criticism, even posting in its online FAQ that it does not possess a button to "shut off the Internet."[41] Political sensitivities make it difficult

36 Ibid.

37 Center Against Terrorism and Hybrid Threats. 2016. "FAQ." Updated 2019. https://www.mvcr.cz/cthh/clanek/specialni-dokumenty-faq.aspx

38 The annual report for 2018 is not publicly available as of this writing.

39 Czech Ministry of Interior. 2018. "Situation Report on Internal Security and Public Order in the Czech Republic in 2017." https://www.mvcr.cz/soubor/report-2017-en-pdf.aspx

40 Lopatka, Jan. 2017. "Czech 'hybrid threats' center under fire from country's own president." *Reuters.* 4 January 2017. https://www.reuters.com/article/us-czech-security-hybrid/czech-hybrid-threats-center-under-fire-from-countrys-own-president-idKBN140227

41 Center Against Terrorism and Hybrid Threats. 2016.

for the CTHT to publicly weigh in on the delicate issues in its portfolio, such as migration.

At odds with this criticism was the foreign media's reaction to the CTHT's launch. It was lauded as "a specialist unit to fight fake news" in *The Guardian*[42] and "a SWAT team for truth…armed with computers and smart phones" in *The Washington Post*.[43] Such press coverage created a gap between expectations and the center's remit.

Coordination and Impact on Policy

As the Czech Republic prepared for elections in late 2017, the CTHT "organized a [cybersecurity] workshop for representatives of political parties running in the parliamentary and presidential elections" in coordination with the National Cyber and Information Security Agency, Google, and Facebook. Furthermore, it attended meetings of the cross-governmental Expert Working Group on Hybrid Threats at the Government Office.[44] It remains the only non-military or intelligence structure within the government dedicated to the problem of hybrid threats.

Press Coverage

As outlined above, the CTHT received a great deal of positive foreign press coverage in the lead-up to its launch. The resulting expectations gap, compounded with the domestic political situation and the center's high proportion of classified work, led observers later to be critical of its output. "The center's public inactivity and accusations that it is claiming a 'monopoly on truth' show how difficult it is for governmental institutions to fight fake news publicly, without being perceived as biased," reported *The Washington Post* in late 2017.[45] Another article in *Foreign Policy* worried that the Center might not survive the country's presidential and parliamentary elections.[46] The CTHT did survive into 2018 and continues to fulfill its mandate.

Analysis

The experience of the CTHT holds several lessons for building institutions in response to hybrid threats. Its limited mandate—concerning the specific disinformation and hybrid threats under the remit of the Interior Ministry—means that it is a small piece of a much larger network of responses that have yet to be fully developed within the country. As such, media depictions to the center as a panacea to the Czech Republic's disinformation problem were overblown. In reality, a small part of its resources is dedicated to the public debunking of disinformation via its Twitter account. This is a curious choice for communication as only 11.5 percent of Czechs use the platform, while the center does not maintain a presence on Facebook, which 45 percent use.[47] The resonance of the CTHT's public messages is difficult to measure. Similarly, given that so much of its activity is classified, it is similarly difficult to ascertain its effect within the government. However, the experience of center's rollout still underlines the need to manage expectations of a new initiative's

> *"The experience of the CTHT holds several lessons for building institutions in response to hybrid threats.*

42 Tait, Robert. 2016. "Czech Republic to Fight 'Fake News' with Specialist Unit." *The Guardian*. 28 December 2016. https://www.theguardian.com/media/2016/dec/28/czech-republic-to-fight-fake-news-with-specialist-unit

43 Faiola, Anthony. 2017. "As Cold War turns to Information War, a new fake news police combats disinformation." *The Washington Post*. 22 January 2017. https://www.washingtonpost.com/world/europe/as-cold-war-turns-to-information-war-a-new-fake-news-police/2017/01/18/9bf49ff6-d80e-11e6-a0e6-d502d6751bc8_story.html

44 Czech Ministry of Interior. 2018.

45 Noack, Rick. 2017. "Czech elections show how difficult it is to fix the fake news problem." 20 October 2017. https://www.washingtonpost.com/news/worldviews/wp/2017/10/20/czech-elections-show-how-difficult-it-is-to-fix-the-fake-news-problem/

46 Colborne, Michael. 2017. "The Brief Life, and Looming Death, of Europe's 'SWAT Team for Truth'," 20 September 2017. https://foreignpolicy.com/2017/09/20/the-brief-life-and-looming-death-of-europes-swat-team-for-truth-fake-news/

47 StatCounter. 2019. "Social Media Stats Czech Republic." January 2019. http://gs.statcounter.com/social-media-stats/all/czech-republic

mandate and capacity in the wider press as well as in the government or structure of which it is a part.

Further, the center's lack of political support among the country's political leadership at the highest levels is instructive for several countries facing similarly politicized internal situations, where the existence of foreign interference is still a question up for debate. The CTHT's experience—with its public-facing fact-checking activities bringing it under fire despite accounting for a small portion of its programming—suggests that pursuing activities other than direct debunking may be more productive when high-level political support is lacking.

European Centre of Excellence for Countering Hybrid Threats

The EU and NATO announced the establishment of a new joint European Center of Excellence for Countering Hybrid Threats (Hybrid COE) in April 2017. The center, led by Finland, a non-militarily aligned member of the EU, is housed in Helsinki. It was inaugurated in October 2017. As of February 2019, participating nations were Austria, Canada, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Italy, Germany, Latvia, Lithuania, Netherlands, Norway, Poland, Romania, Spain, Sweden, the United Kingdom, and the United States. Participation is open to all EU and NATO members. Though the EU and NATO themselves as institutions are not participants in the Hybrid COE, they "participate actively in the Center's activities and are invited to support the Steering Board with their expertise."[48] Its initial budget was €1.5 million, funded by participation fees and contributions of participating countries, and Finland supplies its offices. [49]

Similar in structure and mission to the NATO StratCom COE in Riga, the Hybrid COE is "an international hub for practitioners and experts" that "aim[s] to assist member states and institutions in understanding and defending against hybrid threats."[50] It defines its core functions as:

- "To be a platform for nations to come together to share best practices, build capability, test new ideas and exercise defence against hybrid threats.
- To be a neutral facilitator between the EU and NATO through strategic discussions and exercises.
- To lead the conversation on countering hybrid [threats] through research and sharing of best practices."[51]

Its work is organized around three communities of interest (COIs) composed of practitioners from participating states and the EU and NATO. These focus on influence (led by the United Kingdom), vulnerabilities and resilience (led by Finland), and strategy and defense (led by Germany). The Hybrid COE's research division helps inform the work of the COIs, while the training division equips them to deliver on their objectives.

Finland's mission to NATO sought to manage expectations about the Hybrid COE's role in a press release upon its inauguration, stating: "the Center is not an ´operational center for anti-hybrid warfare´ or a ´cyber bomb disposal unit'…Instead, its aim is to contribute to a better understanding of hybrid influencing by state and non-state actors and how to counter hybrid threats."[52]

Activities

In its first full operational year, the Hybrid COE worked to broaden the networks of its COIs through

48 Hybrid COE. 2017. "EU and NATO Welcome Hybrid COE." 1 September 2017. https://www.hybridcoe.fi/news/eu-and-nato-welcome-hybrid-coe/

49 Finlex Data Bank. 2017. "Act on the European Centre of Excellence for Countering Hybrid Threats 417/2017" 28 June 2017. http://www.finlex.fi/fi/laki/alkup/2017/20170417

50 Hybrid COE. 2019. "What is Hybrid COE?" https://www.hybridcoe.fi/what-is-hybridcoe/

51 Ibid.

52 Finnish Mission to NATO. 2017. "European Centre of Excellence for Countering Hybrid Threats starts operating in Helsinki." http://www.finlandnato.org/public/default.aspx?contentid=365896&nodeid=39170&culture=en-

several outreach events in the transatlantic space. The launch of the work of each of the three COIs included public workshops and symposia.[53] The COI on influence focused its work on "election interference, disinformation and open source intelligence, as well as organizing table-top exercises in order to build member states' capabilities for countering malign influencing." The vulnerabilities and resilience COI worked on issues related to legal and maritime vulnerabilities, drones, and energy. The strategy and defense COI was launched only in August 2018, and as such, as this paper was written it was undertaking its first activities and setting the basic parameters for its work.[54]

> *"The Hybrid COE's largest obstacle is the fact that its mission covers a wide range of vulnerabilities.*

Additionally, the Hybrid COE held several trainings. One, on open source research for "strategic communicators, diplomats and civil servants from more than 10 nations," was organized and implemented with support from the U.K. Foreign and Commonwealth Office's Open Source Unit.[55] The center also convened a "comprehensive security training event" for 30 North American and European participants. The course material was based on "the Finnish Comprehensive Security Concept and its implementation by authorities and other security actors" and was delivered together with the Finnish Defense Forces and supported by the Finnish Security Committee and the National Defense University.[56]

To date, the Hybrid COE has published 15 reports, strategic analyses, and working papers on a variety of topics. In early 2019, it began work on a grant from the U.S. Department of State's Global Engagement Center to build capacity in NATO and EU member states to counter electoral interference and disinformation.[57]

Obstacles

Unlike some other efforts to counter hybrid threats, the Hybrid COE has enjoyed wide and enthusiastic support since its launch. Its kickoff event included remarks from High Representative of the European Union for Foreign Affairs and Security Policy Federica Mogherini and NATO Secretary General Jens Stoltenberg, as well as Finland's President Sauli Niinistö and Prime Minister Juha Sipilä.

The Hybrid COE's largest obstacle is the fact that its mission covers a wide range of vulnerabilities in information ecosystems, infrastructure, elections, legal matters, the defense sector, and beyond. It has attempted to break down this mandate into more manageable issue areas through its Communities of Interest, but even these portfolios are quite broad and varied. Rather than clarifying the idea of "hybrid warfare," often used as a policy catchall, the Hybrid COE's approach makes it difficult to distill its main lines of effort and further muddies an already contested and confusing concept.

Coordination and Impact on Policy

The nature of the joint EU-NATO support for the Hybrid COE means that it is an ideal structure for cross-institutional coordination and cooperation. In addition to the coordinated training activities described above, as well the COIs themselves, which are led by individual participating states, the Hybrid COE also facilitates EU-NATO coordination. In September 2018, it "supported a hybrid scenario-based discussion for an informal meeting between

53 Hybrid COE. 2019. "News." https://www.hybridcoe.fi/news/

54 Hybrid COE. 2018. "Hybrid COE Presents the First Year Results in Brussels." 21 November 2018. https://www.hybridcoe.fi/news/hybrid-coe-presents-the-first-year-results-in-brussels/

55 Hybrid COE. 2018. "Trainings on Open Source Material." 10 October 2018. https://www.hybridcoe.fi/news/trainings-on-open-source-material/

56 Hybrid COE. 2017. "Hybrid COE Co-Hosted Comprehensive Security Training Event." 26 October 2017. https://www.hybridcoe.fi/news/hybrid-coe-co-hosted-comprehensive-security-training-event/

57 Hybrid COE. 2018. "United States Grant to the European Center of Excellence for Countering Hybrid Threats." 12 December 2018. https://www.hybridcoe.fi/news/united-states-grant-to-the-european-center-of-excellence-for-countering-hybrid-threats/

the EU's Political and Security Committee (PSC), the EU's body to oversee the Common Foreign and Security Policy, and the North Atlantic Council (NAC), NATO's principal political decision-making body."[58] The Hybrid COE developed the scenario presented at the discussion, and attending ambassadors discussed how they would implement a coordinated response.

The Hybrid COE also briefed ambassadors and other officials from EU and NATO structures, but the extent of its coordination with the COEs in Tallinn and Riga, as well as organizations with similar mandates, such as the East StratCom Task Force, is as of yet unclear. As the Hybrid COE implements its "road show" training program with a grant from the U.S. State Department's Global Engagement Center in 2019, its effect on policymaking processes may become more visible to the public.

Press Coverage

The opening and ongoing operations of the Hybrid COE have enjoyed less press coverage than other similar efforts. However, as in their case, its launch was also mischaracterized by some media outlets as a direct Western response to Russia's hybrid warfare, rather than a research and training institution created to help the West better understand the threat.[59] *The Telegraph* described the center in the style of an espionage novel.[60] The Hybrid COE also drew some criticism for its wide mandate and "bureaucratic approach to a nonbureaucratic problem."[61]

Analysis

The Hybrid COE is an ideal structure through which to facilitate multilateral coordination and cooperation on the institutional- and state-level, with high-level buy-in from EU and NATO leaders and an enthusiastic and growing membership. Its challenge is tackling an amorphous mandate and meeting the high expectations set by press coverage and with a small staff and budget.

Sweden's Civil Contingencies Agency

Sweden's Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB) has a much wider mandate than the other organizations profiled in this paper, having been created from the combination of the country's Rescue Services Agency, Emergency Management Agency, and National Board of Psychological Defense in 2009. It is housed within the Ministry of Defense, and "is responsible for issues concerning civil protection, public safety, emergency management and civil defense," from forest fires to disinformation and hybrid threats.[62]

The MSB "supports and coordinates" preventative work around information security "to avoid disruptions and to enable the management of crises."[63] Its information security portfolio encompasses several strands of work, including research and analysis,[64] consultative work with national, regional, and local authorities, and coordination with the media around "preparedness planning."[65] In particular, the MSB has worked "actively since 2014 to develop Sweden's capacity to identify, understand and counter hostile information influence campaigns." This includes "increasing […] public awareness, [which] is central

58 Hybrid COE. 2018. "Hybrid COE Supports Informal NAC-PSC Discussion." 28 September 2018. https://www.hybridcoe.fi/news/hybrid-coe-supports-informal-nac-psc-discussion/

59 Standish, Reid. 2017. "Finland opens new center to fight 'hybrid threats' from Russia." *U.S.A Today*. 4 October 2017. https://www.usatoday.com/story/news/world/2017/10/04/finland-opens-new-center-fight-hybrid-threats-russia/730498001/

60 Rothwell, James. 2018. "Inside Europe's secret weapon against Russian 'hybrid threats'" 26 January 2019. *The Telegraph*. https://www.telegraph.co.uk/news/2018/01/26/inside-europes-top-secret-weapon-against-russian-hybrid-threats/

61 Standish, Reid. 2018. "Inside a European Center to Combat Russia's Hybrid Warfare." *Foreign Policy*. 18 January 2018. https://foreignpolicy.com/2018/01/18/inside-a-european-center-to-combat-russias-hybrid-warfare/

62 MSB. 2019. "About MSB." https://www.msb.se/en/About-MSB/

63 MSB. 2012. "The MSB and Societal Information Security." February 2012. https://www.msb.se/Upload/English/About_MSB_fact/Societal%20information%20security.pdf

64 The agency's total research budget is over $12 million. See: MSB. 2019. "Research for a Safer Society." https://www.msb.se/en/About-MSB/Research/

65 MSB. 2012.

to countering information influence campaigns."[66] The MSB's budget was increased in 2017 and it began to invest more in countering foreign influence ahead of the 2018 parliamentary elections.[67]

Activities

Ahead of the 2018 elections, the MSB's "election-related tasks […] included continuous engagements with the mass media, cybersecurity briefings and seminars for public administrators, and cyber support via its CERT (Computer Emergency Response Team)."[68] It also coordinated an interagency election working group (see below), briefed campaigns and other election actors on important cyber security measures, and trained 10,000 local election administrators on information influence activities ahead of the election.[69]

> *"A sustained investment over time is necessary to fight disinformation and hybrid activities outside of election periods.*

Further, the MSB issued a pamphlet to every household in Sweden, titled *If Crisis or War Comes*. It explains proper emergency preparedness, Sweden's "total defense" doctrine, and the country's emergency alert system. It also dedicates one page to false information and encourages critical thinking. "States and organisations are already using misleading information in order to try and influence our values and how we act. The aim may be to reduce our resilience and willingness to defend ourselves," the pamphlet states, before explaining the basics of media literacy in six short questions.[70]

Additionally, the MSB issued a handbook for communicators on "countering information influence activities" in collaboration with researchers at Lund University. The handbook, which was sent in hard-copy form to every household, aims to raise awareness of such activities and to assist communicators in the public sector in identifying and fighting them.[71] Finally, the MSB served as the point-of-contact for social media companies during the election period, in addition to convening its Media Preparedness Council with a special focus on information operations ahead of the 2018 elections.

MSB Director General Dan Eliasson noted last October that the agency "did not see any direct influence" from malign foreign actors during the parliamentary elections.[72]

Obstacles

While the MSB's efforts surrounding the 2018 elections were wide-ranging and well executed, the mandate and funding for much of this work was directly tied to the elections.[73] A sustained investment over time is necessary to fight disinformation and hybrid activities outside of election periods, which is when the groundwork for influence operations is being laid.

Coordination and Impact on Policy

According to the MSB, "the complexity and cross-sector nature of information security demands effective cooperation. This means cooperation between various entities in Sweden, such as

66 MSB. 2018. "Countering information influence activities: a handbook for communicators." 27 August 2018. https://www.msb.se/RibData/Filer/pdf/28698.pdf

67 Cederberg, Gabriel. 2018. "Catching Swedish Phish: How Sweden is Protecting its 2018 Elections." Belfer Center; Harvard Kennedy School. August 2018. Page 13. https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf

68 Ibid. Page 13.

69 Ibid. Pages 19 and 21.

70 MSB. 2018. "If Crisis or War Comes." 21 May 2018. https://www.msb.se/Upload/Forebyggande/Krisberedskap/Krisberedskapsveckan/Fakta%20om%20broschyren%20Om%20krisen%20eller%20Kriget%20kommer/om-krisen-eller-kriget-kommer---engelska.pdf

71 MSB. 2018. "Countering information influence: a handbook for communicators." 27 August 2018. https://www.msb.se/RibData/Filer/pdf/28698.pdf

72 Wemer, David A. 2018. "Here's how to fight disinformation." Atlantic Council. 2 October 2018. https://www.atlanticcouncil.org/blogs/new-atlanticist/here-s-how-to-fight-disinformation

73 Cederberg. 2018. Page 31.

government authorities, municipalities, county councils, the private sector, and organisations; but also international cooperation."[74]

In the lead-up to the 2018 elections, the MSB together with Sweden's Election Authority and Security Service established a high-level national working group on election security. The organizations worked together on "comprehensive threat analysis and election administrator briefings," and created a space for cross-governmental dialogue.[75] Mikael Tofvesson, who headed the MSB's 2018 elections efforts, said: "Our all-hazards approach has given us an advantage to tie different actors and vulnerabilities together in our monitoring, assessment and cooperation activities."[76]

In the international arena, the MSB signed a cooperation agreement with NATO StratCom COE in early 2017.[77] It is an active participant in academic and think tank dialogues on disinformation and sponsors cross-border research on the issue, including a paper on the 2018 elections published through the London School of Economics' Arena Project.[78]

Press Coverage

Most of the English-language press coverage of the MSB's anti-disinformation efforts ahead of the 2018 elections coincided with the release of the pamphlet *If Crisis or War Comes*. While some articles presented the pamphlet as a one-stop shop to fighting disinformation, many highlighted Sweden's whole-of-government efforts to protect the upcoming election as a potential blueprint for the United States ahead of the 2018 midterm elections.[79]

74 MSB. 2012.

75 Cederberg. 2018. Page 15.

76 Ibid.

77 StratCom COE. 2017. "Sweden and NATO StratCom COE sign cooperation agreement." 10 January 2017. https://www.stratcomcoe.org/sweden-and-nato-stratcom-coe-sign-cooperation-agreement

78 Colliver, Chloe et al. 2018. "Smearing Sweden." LSE Arena Project. http://www.lse.ac.uk/iga/assets/documents/arena/2018/Sweden-Report-October-2018.pdf

79 Birnbaum, Michael. 2018. "Sweden is taking on Russian meddling ahead of fall elections. The White House might take note." *The Washington Post*. 22 February 2018. https://www.washingtonpost.com/world/europe/sweden-looks-at-russias-electoral-interference-in-the-us-and-takes-steps-not-to-be-another-victim/2018/02/21/9e58ee48-0768-11e8-aa61-f3391373867e_story.html

Analysis

The MSB presents a whole-of-government model for countering hybrid threats that other institutions can seek to replicate. In particular, it served as the convening force behind the Swedish government's 2018 efforts to protect the country's elections, bringing together actors across and outside of national-level government, including political parties, election administrators, media, and social media platforms. Outside of focusing on infrastructure and good cyber hygiene, the MSB's programming also aimed to build public awareness of the threat of disinformation through the nationwide distribution of its pamphlet and work with the media sector. While some outlets pushed back on the MSB's media coordination efforts for fear of appearing too conspiratorial,[80] these efforts are an example of well-meaning proactive communication that other governments—particularly those on the front lines of Russian disinformation and other forms of interference—could adopt in place of current models, which are inherently reactive.

Cross-Governmental U.K. Efforts

The U.K. government's efforts to counter Russian hybrid threats are a unique case in this paper because they are not housed or led by a single office. Governed by what the 2018 National Security Capability Review (NSCR) calls the "Fusion Doctrine," the efforts draw on all parts of government connected to a given policy challenge to preserve national security.

In her foreword to the NSCR framing the Fusion Doctrine, Prime Minister Theresa May referred to "a brazen and reckless act of aggression on the streets of Salisbury: attempted murder using an illegal chemical weapon, amounting to an unlawful use of force against the UK."[81] Though the development of

80 Cederberg. 2018. Page 24.

81 UK Cabinet Office. 2018. "National Security Capability Review." 28 March 2018. Page 2. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf

Fusion Doctrine predated the attempted murder of former Russian intelligence officer Sergei Skripal in Salisbury, the NSCR argues that the ability to respond effectively to challenges including Russian disinformation and hybrid warfare rests on the degree to which the United Kingdom can mobilize all its available resources. "This approach will ensure that in defending our national security we make better use of all of our capabilities: from economic levers, through cutting-edge military resources to our wider diplomatic and cultural influence on the world's stage," May wrote. "Every part of our government and every one of our agencies has its part to play."[82]

The Fusion Doctrine is applicable to the entirety of the government's national security activities, but the focus here is on its efforts to fight Russian disinformation and counter hybrid threats, which, like other countries' efforts, began abroad after Russia's illegal annexation of Crimea. Through its Russian Language and Counter Disinformation and Media Development Programs, which include activities delivered by the Foreign and Commonwealth Office and supported

> *"Crucially, the Fusion Doctrine enshrines a place for strategic communications at the heart of national security issues*

by the Department for International Development, the Ministry of Defense, and the Cabinet Office, the government seeks to engage audiences vulnerable to disinformation and to support independent media in Russia's neighborhood. The approaches used abroad were adapted for the United Kingdom's domestic context, in which the government identifies and exposes disinformation and hybrid tactics, works to improve the domestic information environment, and builds societal resilience. Having built a strong network of allies also working to counter Russian efforts prior to beginning this work, the United Kingdom's efforts are amplified beyond its own borders.

Crucially, the Fusion Doctrine enshrines a place for strategic communications at the heart of national security issues. According to Alex Aiken, the head of the Government Communication Service (GCS), in the Fusion Doctrine "strategic communications are to be considered with the same seriousness as financial or military options."[83] This is made clear in government structure; Aiken now has a seat at the National Security Council. Further, in April 2018, the GCS launched a Rapid Response Unit (RRU) to work alongside the expanded National Security Communications Team (NSCT) in order to meet the challenges of the new information environment, including Russian disinformation as a high priority. The RRU "monitors news and information being shared and engaged with online to identify emerging issues with speed, accuracy and with integrity [but it] is neither a 'rebuttal' unit, nor is it a 'fake news' unit."[84] Rather, the unit's monitoring efforts allow the government to quickly gain a handle on misleading narratives as they spread. The RRU then works with other arms of the GCS, including the NSCT, to "rebalance the narrative" and provide more trustworthy sources of information.[85]

Activities

U.K. officials cite their response to the Skripal poisoning as the best example of the Fusion Doctrine in practice, even though its official unveiling occurred after the event occurred. As the news of the Salisbury incident broke, the Russian disinformation machine pushed out more than 40 false narratives about the attack. The government focused "on building respect and winning the trust of [its] audiences rather than rebutting every false

82 Ibid.

83 Aiken, Alex. 2018. "Disinformation is a continuing threat to our values and our democracy." UK Government Communication Service. 12 June 2018. https://gcs.civilservice.gov.uk/disinformation/

84 Aiken, Alex. 2018. "Alex Aiken introduces the Rapid Response Unit." UK Government Communication Service. 19 July 2018. https://gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/

85 Ibid.

Russian narrative. [It was] clear about [the] case—the Russian state had the means, method and motivation to undertake this attack."[86]

The response included regular updates from the government to the parliament and the public, and tied together all relevant arms of government, from bodies responsible for public safety and health to the Foreign and Commonwealth Office and Defense Ministry. By repeatedly underscoring the breadth of false and contradictory claims the Russian government used to attempt to explain the Salisbury attack, as well as Russia's history of similarly aggressive actions, the U.K. government highlighted Russia's flagrant disregard for the rules-based international order.

Coordination

In addition to coordination within the U.K. government itself, the response to the Skripal incident was coordinated with international partners. The U.K. government worked in concert with over 20

> *"The Fusion Doctrine is government policy with high-level buy-in and is not tied to a single event or issue area.*

other governments to expel more than 100 Russian diplomats believed to be intelligence assets, in addition to equipping journalists and experts with an ongoing flow of information about the crime and subsequent investigation. In sum, the response was "the Fusion doctrine in practice—covering economic, diplomatic, communication and other action designed to reassure the U.K. public, deter […] adversar[ies] and build an international coalition."[87] It proved that a whole-of-government, cooperative model to responding to disinformation and hybrid threats is possible even in times of crisis.

86 Aiken. 2018. "Disinformation is a continuing threat…"

87 Ibid.

Obstacles

The Fusion Doctrine is government policy with high-level buy-in and is not tied to a single event or issue area. As such, the U.K. government faced fewer administrative hurdles to its implementation than similar efforts, such as the EU's East Stratcom Task Force or the Czech Republic's Center Against Terrorism and Hybrid Threats, which lacked high-level directives. The doctrine required the creation of several new bodies and coordination mechanisms, and while the act of standing up any new governmental body is complex, these efforts did not face the existential struggles related to missions, budgets, and staffing faced by other organizations.

Press Coverage

The media response to the release of the Fusion Doctrine was by and large neutral.[88] One opinion column worried that the inclusion of soft power—including media and communications—within it would undermine the nation's power and influence if it crossed into the realm of counter-propaganda.[89] Unlike with the other cases, the coverage appears not to have affected expectations or implementation of the effort.

Analysis

The Fusion Doctrine is just over a year old and beyond the NSCR and publications related to the Skripal poisoning, little public information exists about its implementation. However, in its short existence, it did not experience the growing pains of some other policy efforts. It enjoyed high-level political buy-in from the prime minister and ministers. Rather than attempting to carve out a niche policy area from the portfolios of other efforts, the Fusion Doctrine coordinates a cross-

88 See, for instance: Perkins, Anne. 2018. "UK to remain on high terror alert for at least two years, sources say." *The Guardian*. 27 March 2018. https://www.theguardian.com/uk-news/2018/mar/27/uk-remain-high-terror-alert-two-years-whitehall-sources-say

89 Bershidsky, Leonid. 2018. "The UK's New Warfare Doctrine Looks Familiar." *Bloomberg*. 29 March 2018. https://www.bloomberg.com/opinion/articles/2018-03-29/the-u-k-s-new-fusion-strategy-looks-familiar

government approach to issues that are not limited to Russian hybrid warfare. Because it is official policy for all of the government, departments are obligated to realign their activities and resources to produce agile, flexible responses to national security concerns. The Fusion Doctrine attempts to tear down walls between geographical and functional strands of work across government, and, importantly, emphasizes communication with the public. It is a truly whole-of-government approach with a focus on societal resilience that can be used to respond to the developing challenges of Russian disinformation, hybrid threats, and beyond.

Conclusion and Recommendations

The six European efforts to counter Russian disinformation and hybrid threats outlined in this paper are diverse in their forms and approaches, and they have made progress in building awareness about the problem among the public and policymakers. They have also faced a variety of obstacles from which similar nascent efforts, and those in the United States in particular, can extrapolate best practices and avoid the "Band-Aid Effect" in their own institution-building processes. Key lessons are outlined below.

Secure vertical and horizontal buy-in to policies and objectives.

Organizations that face criticism or lack vocal public support from high-level officials, such as the Czech Center Against Terrorism and Hybrid Threats and the EEAS East StratCom Task Force, face a variety of administrative challenges. Their financial and human resources are precarious, making long-term strategic planning difficult. Conversely, organizations and efforts with enthusiastic high-level buy-in, such as the European Centre of Excellence for Countering Hybrid Threats, and the Swedish and U.K. national efforts, face fewer such roadblocks. Further, the vocal public support of high-level officials is important as a tool to raise public awareness.

Similarly, horizontal coalition building across government and bodies is also integral to success. Initiatives that have a wide swath of members or supporters—such as both COEs and the U.K. efforts in support of the Fusion Doctrine—are examples of more effective coordination and amplification of efforts, and face less of a risk of being stymied or siloed through turf wars.

Obtain medium-term funding commitments where possible.

The case studies demonstrate the need for reliable funding, and how financial uncertainty can stymie effective work. The example of the EEAS East StratCom Task Force is perhaps the starkest in this regard; after years of spending time simply justifying its existence and subsisting on very limited finances, it finally received a markedly increased, if still small, budget in the lead-up the European Parliament elections. Ideally, a medium-term budget of at least three years would have been allocated to the team so they could plan for upcoming key events, strategically allocate human resources, and create a longer-term strategy for success before, during, and after the election period.

While the inclination of many donor bodies or budget stewards to measure success over the short term is understandable, the Russian government's interference operations continue to be funded at levels far greater than Western efforts to counter them. The West need not replicate this spending; instead, funding should be allocated for the medium-term to allow bodies to mount a more strategic response to Russian actions. Furthermore, efforts with meager budgets should aim to coordinate with other organizations wherever possible in order to maximize their resources and amplify their impact.

Utilize existing structures and policymaking processes to avoid administrative obstacles.

Creating a new body entirely from scratch is challenging; securing a budget, recruiting qualified staff, solidifying objectives, and a host of other

challenges take more time when starting from the ground level. Organizations and efforts such as Sweden's Civil Contingencies Agency and the cross-governmental U.K. efforts that utilized existing structures to respond to foreign interference threats were able to deliver an agile and wide-reaching response in a short time, compared with the new organizations that spend much of their first years standing up their efforts.

> *"As the United States and others continue to institutionalize their responses to Russian government—and, increasingly, other countries'—interference efforts, they need not reinvent the wheel.*

Define a clear mission and goals against which to measure success.

Hybrid threats are often extremely broadly defined. However, given that most new efforts draw upon limited resources, it is important to identify the explicit objectives against which they will deliver so that resources can be best allocated. However, organizations and governments should avoid linking their efforts to a single event; Russian attempts to influence society through disinformation and other hybrid tools are built up over years, aiming to increase chaos and confusion in society. They are not pegged to one election or referendum, and neither should the goals of organizations responding to such threats.

Manage the expectations of the press and the public by prioritizing communication.

For the organizations profiled in this paper, communication is too often an afterthought. Particularly in the charged political atmosphere that Russian influence operations exploit, it is important to conduct transparent, truthful, and regular outreach to the press and public in order to raise awareness of the threat and increase resilience against it. But it is also important to maintain a clear understanding of the expectations and limits of the organizations countering them. Neglecting to prioritize communication as a key part of the national security response to Russian hybrid threats can undermine efforts before they even begin.

Most importantly, as the United States and others continue to institutionalize their responses to Russian government—and, increasingly, other countries'—interference efforts, they need not reinvent the wheel. There is much to be learned from the years of work toward similar goals already underway. Ignoring these experiences could lead states toward adopting Band-Aid solutions that may address parts the problem temporarily, but in the long term will fail to heal deeper wounds.

Please direct inquiries to:

The German Marshall Fund of the United States
1744 R Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@gmfus.org

This publication can be downloaded for free at http://www.gmfus.org/listings/research/type/publication.
The views expressed in GMF publications and commentary are the views of the authors alone.

Cover photo credit: Shutterstock.com / Gorodenkoff

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF contributes research and analysis and convenes leaders on transatlantic issues relevant to policymakers. GMF offers rising leaders opportunities to develop their skills and networks through transatlantic exchange, and supports civil society in the Balkans and Black Sea regions by fostering democratic initiatives, rule of law, and regional cooperation. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

About ASD

The Alliance for Securing Democracy is a bipartisan, transatlantic initiative housed at The German Marshall Fund of the United States (GMF) that is committed to developing comprehensive strategies to defend against, deter, and raise the costs on Russian and other state actors' efforts to undermine democracy and democratic institutions. The Alliance is informed by a bipartisan, transatlantic advisory council composed of former senior officials with experience in politics, foreign policy, intelligence, Russia, and Europe — bringing deep expertise across a range of issues and political perspectives.

About the Author(s)

Nina Jankowicz is a global fellow at the Woodrow Wilson International Center for Scholars' Kennan Institute, where she studies Russian disinformation and the democratic challenges of the technology age. Her first book, How to Lose the Information War, will be published by Bloomsbury's IBTauris in Summer 2020. She was a Fulbright public policy fellow in 2016-2017, a role in which she provided strategic communications guidance to the Foreign Ministry of Ukraine. She holds an MA in Russian, Eurasian, and East European studies from Georgetown University and a BA in Russian and political science from Bryn Mawr College.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org