ASSESSING THE WESTERN RESPONSE TO RUSSIAN DISINFORMATION IN EUROPE: HOW CAN WE DO BETTER?

NINA JANKOWICZ
Fulbright-Clinton Public Policy Fellow, Ukraine, 2016-2017

The views in this report are the author's own and do not represent the Fulbright Program or the U.S. Department of State.

Executive Summary

Russia's disinformation campaign against the West takes on many forms: outright fake news stories, attacks by troll armies, funding local disinformation outlets and groups, and other, more surreptitious provocations. But no matter which of the many information environments the Kremlin's campaigns touch or the form they take, its activities across Europe have one thing in common: they exploit the trust gap between citizens and their governments, as well as the gap between citizens and the media, in order to undermine the cohesion of the transatlantic order.

The West is beginning to acknowledge the disinformation threat. Fact-checking operations are proliferating, the U.S. Congress passed a bill in December 2016 to fight disinformation, and several NATO and EU countries recently announced the establishment of a new center to counter hybrid threats. These are steps in the right direction, to be sure, but most anti-disinformation programming targets expert communities rather than addressing the populations most susceptible to Russian efforts. Without addressing citizens' overall lack of trust by supporting local media and helping populations learn to recognize what constitutes quality coverage, other investments will fail to yield results.

Recommendations

1. Our first priority must be to **bridge the trust gap through long-term investments in skills-building programs, campaigns in media literacy and support of independent local journalism**. These programs could also be replicated in the United States, Germany, France, and other countries outside of Russia's former sphere of influence.
2. We must **continue strategically funding analytical, fact-checking, consciousness-raising work** by offering long-term support to organizations that are experienced and produce quality analysis. Offer training to help these organizations achieve sustainability before redirecting funding. Prioritize programming that requires working-level cooperation between organizations in this category, not only to encourage the sharing of best practices, but also to avoid duplication of efforts.
3. We must **rethink the foreign assistance funding paradigm**. Across the board, we should invest in longer programs with more flexible deliverables and consider expanding the list of assistance beneficiaries to countries that have "graduated" from foreign assistance but influence the cohesion of the transatlantic community.

Table of Contents

Introduction

In the wake of the 2016 U.S. Presidential Election and ensuing revelations about Russian interference in the American democratic process, the West seems to have finally woken up to the threat of "fake news" emanating from Russia. Central and Eastern European states, however, have been aware of the threat for years. Many of them, sometimes with Western support, have set out to combat the threat and prevent its further encroachment into their societies. While some projects have naturally had more impact than others, the increased recognition of the disinformation threat means that the already-crowded landscape of anti-disinformation initiatives is becoming further populated by hastily-conceived programs meant to defend the Western democratic order as Europe heads into several critical elections in 2017 and beyond.

This paper endeavors to provide a digestible snapshot of the European information environment and ongoing programming in four main sectors in the anti-disinformation space: non-governmental organizations, think tanks, cooperative multilateral bodies, and domestic initiatives run by government institutions. It draws on over 25 interviews with experts in six European countries (Belgium/the greater European Union, the Czech Republic, Latvia, Poland, Ukraine, and the United Kingdom) and implementers of anti-disinformation programming in four types of information spaces: marginally pro-Kremlin (Czech Republic), anti-Kremlin (Poland), anti-Kremlin with a large pro-Kremlin minority (Latvia), and multilateral spaces (EU External Action Service, NATO).

Using these interviews and existing literature, the paper assesses the current situation and makes recommendations for ways the foreign assistance community can more efficiently, strategically, and successfully respond to the disinformation threat. Though the focus of the research is foreign assistance programming and policies in the traditional sense (that is, programming conducted through implementing partners and grantmaking) its conclusions should also be employed domestically by current targets of Kremlin disinformation campaigns, including Germany, France, and the United States.

Despite seemingly disparate political and information environments in which the examined programming operates, the paper identifies a common circumstance between them: citizens in all societies in which disinformation finds fertile ground harbor an extreme distrust in both media and government. While Russia's disinformation activities exploit this trust gap, most anti-disinformation programming targets expert communities rather than addressing the populations most susceptible to Russian efforts. The programs seek to combat the top-level, easily-measurable weapons of the disinformation phenomenon

by debunking or fact-checking fakes, but too few efforts address the fissures in society that make Russian disinformation campaigns so successful. Without addressing citizens' overall lack of trust by supporting local media and helping populations learn to recognize what constitutes quality coverage, other investments will fail to yield results.

The European disinformation landscape

Russia's disinformation campaign, also known as its "information-psychological war," has been active throughout Vladimir Putin's administration, but has increased and gained currency with the advent of new media and social networks that facilitate the spread of "alternative" viewpoints. Propaganda in the Soviet sense is only one component of the disinformation landscape. As Edward Lucas and Ben Nimmo write:

> Russian techniques employ a mixture of media, psychological, economic and cultural means, as well as espionage, cyberattacks (seen in Estonia in 2007, alongside another Kremlin-inspired outburst of local protests), subversion, corruption, and targeted kidnapping and assassination. Sometimes these elements are paired with covert military intervention, as in the case of Ukraine. Most times, however, it represents a "contact-less" conflict that is fought in the realms of perception and the human mind. It continues through both official peace and wartime.[1]

This paper will not seek to further repackage the extensive analysis of primary sources and data over the more than three years of active Russian information warfare in Ukraine and the wider Eastern European region regarding the tools, techniques, and coordinated implementation tactics of Russian disinformation. More important for the focus of this research is an understanding of the ultimate goal of Russia's disinformation campaign in the West. In contrast with Soviet propaganda, "[Russian disinformation's] aim is not to convince or persuade, but to undermine. Instead of agitating audiences into action, it seeks to keep them hooked and distracted, passive and paranoid."[2] In short, Russia exploits fissures in target societies to sow doubt, distrust, discontent and further divide populations and their governments. Ultimately, Russia aims to disrupt the synergies in Western democracies and undermine the Western liberal order as a whole.

The Growing Trust Gap

Around the globe, and particularly in the countries examined for this paper, citizens' trust in public institutions is at its lowest levels in recent memory. The Edelman Trust Barometer recorded "an implosion of trust" in public institutions in 2017.[3] A 2015 study by the European Endowment for Democracy noted that "one of the strongest themes to emerge from [its] audience research [was] a consistent lack of trust in most media outlets regardless of genres and affiliations."[4] The public also harbors a strong distrust in government, throughout the European information space, even in so-called consolidated democracies (Fig. 1).
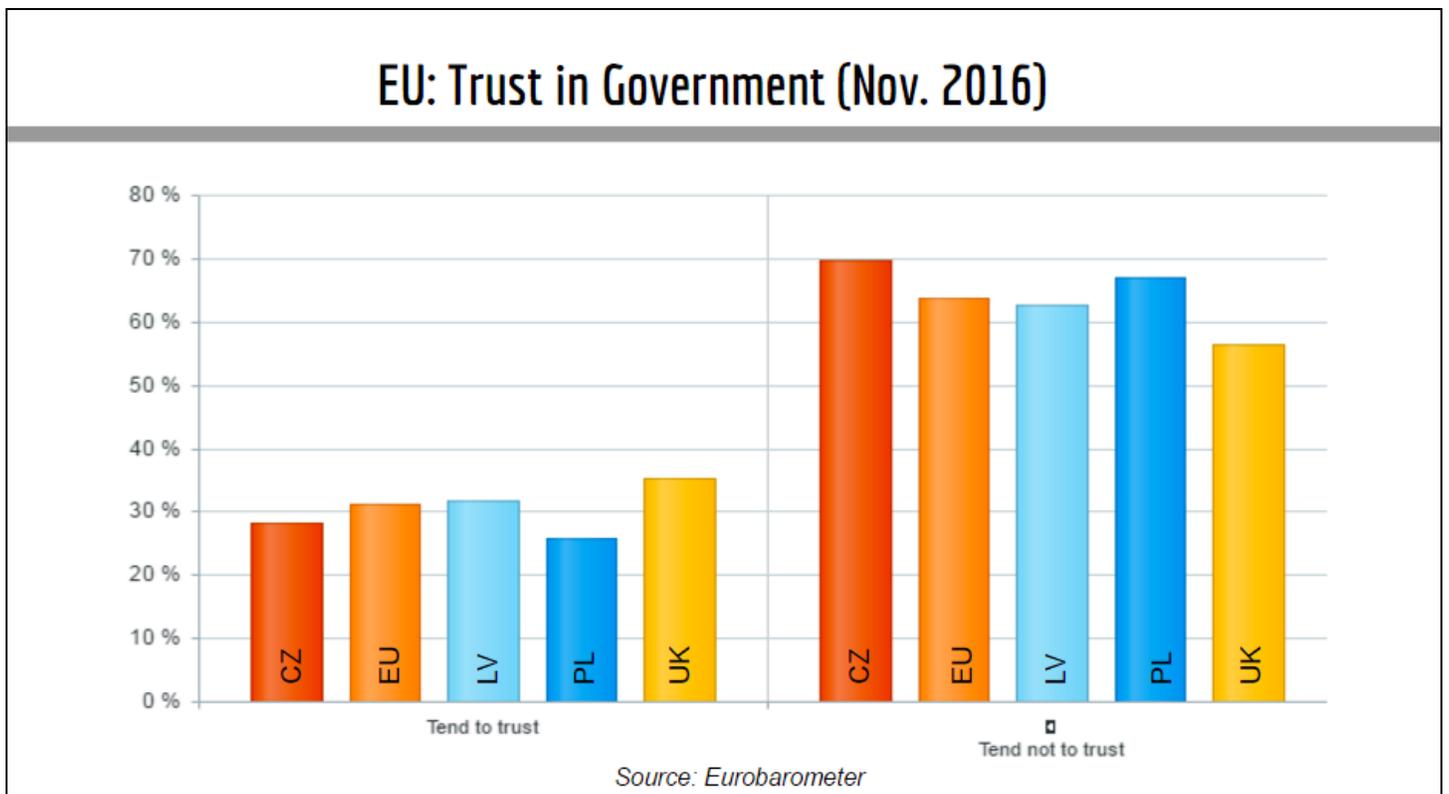

Fig. 1: Eurobarometer survey question: "I would like to ask you about the trust you have in certain institutions. For the national government, please tell me if you tend to trust it or tend not to trust it?" EU results show EU-28 average.[5]

Outside of EU member states, Ukraine also is experiencing a widening trust gap between citizens and both government and media. A 2015 Gallup poll found "one of the lowest trust levels Gallup recorded in Ukraine since 2006,"[6] with only eight *per cent* of those polled reporting confidence in their national government, while a 2016 poll by the Kyiv International Institute of Sociology found very few institutions enjoyed the public's trust in the post-Maidan era (Fig. 2).[7]

Russia's Exploitation of the Trust Gap

Russia is exploiting the widening trust gap across the West. Populations that feel disenfranchised and distant from their governments and underrepresented in the increasingly global media climate are searching for narratives that fit their worldview and address their fears. As Edward Lucas and Peter Pomeranzev write, "the aim [of Russian disinformation] is not so much to convince 'mainstream media' [of the Russian narrative's truth], but play to audiences who already mistrust their own systems, who believe, *a priori*, in conspiracy theories and are looking for any information, however ridiculous, which confirms their biases."[8]

Ukraine: Trust in Social Institutions

Social institutions	Trust	Mistrust	Trust-mistrust balance (difference)
Armed Forces of Ukraine	53.1	23.5	29.6
Non-governmental organizations	37	24.5	12.5
Ukrainian mass media	26.1	43.3	-17.2
Government of Ukraine	9.5	72.8	-63.3
Russian mass-media	2.4	76.3	-73.9
Verkhovna Rada of Ukraine	5.3	82.1	-76.8

Source: KIIS Survey, Dec 2016

(Fig. 2)

The examples of this type of exploitation are many and varied, with the Kremlin employing different techniques depending on the political and informational context. In Germany, Russia exploited growing unease about German Chancellor Angela Merkel's "open-door" refugee policy by propagating the infamous "Lisa" case, in which a 13-year old girl of Russian origin was reportedly raped by migrants. The story was first reported by a minor website for Russian expatriates living in Germany, then amplified by larger Russian domestic and international outlets as well as right-wing social media groups.[9] Eventually, international media picked up the story, and Russian Foreign Minister Sergei Lavrov "made two public

statements about...the inability of the German police and legal system to take such cases seriously because of political correctness."[10] Even after the rape allegations were proven to have been fabricated, demonstrations against migrants in response to the case still took place, beginning the shift away from a thoroughly pro-refugee climate in Germany and placing pressure on the German government.

In Ukraine, the Kremlin plays on citizens' impatience with the slow pace of reforms using a barrage of fake news about the purported ineptitude and illegitimacy of the Poroshenko administration, which it insists was installed by a Western-backed *coup d'etat*.[11] In the Czech Republic, where a 2012 recession left behind many in the Czech countryside and shored up support for an anti-establishment, anti-European, pro-Russian candidate, Russia filled the trust gap with messages that amplified citizen grievances and fears, through websites with proven financial ties to the Kremlin as well as those that simply augment its narratives.[12]

Poland represents perhaps the most adept and unexpected exploitation of the trust gap by Russia. Since it is famous for its ire toward its eastern cousin, many, including high-level Polish officials in the governing Law and Justice party, assume Poland is inoculated to Kremlin propaganda. However, Russia's intervention in the Polish information space, as in all others, seizes on Poland's internal weaknesses and jeopardizes its relationships with allies and neighbors. The political crisis that has plagued Poland since the Law and Justice party assumed power in November 2015 has hastened the deterioration of a culture of consensus in Poland, which Russia is using to its advantage.

The Kremlin is using several inflection points to deepen the trust gap in Poland. First, it has refused to return to Warsaw the wreckage of the 2010 airplane crash in the Russian city of Smolensk that killed former president Lech Kaczynski. Law and Justice, led by Kaczynski's twin brother, obsessively spreads the resulting conspiracy theories far and wide, inspiring doubt and sowing confusion. Moscow doesn't have to lift a finger, but is able to further divide the population in what has already been a contentious political period. Furthermore, Russia actively spreads anti-Lithuanian narratives regarding discrimination against the Polish minority in Lithuania. Ethnic Poles in Lithuania rarely speak Lithuanian and so rely on Russian channels available in the country for news, which amplifies their anti-Vilnius worldview and exacerbates relations between Vilnius and Warsaw. Finally, two attacks on Polish consulates and the desecration of monuments to victims of World-War-II era clashes in Western Ukraine and Eastern Poland are believed by both sides to be perpetrated not by either country's ultra-nationalist factions, but by a "third party," meaning Russia.[13]

Even Russia's interference in the 2016 U.S. presidential election utilized a similar model by leaking damaging information about Hillary Clinton and her surrogates through proxies, further dividing the American left from the right and even creating a chasm within the Democratic Party itself, all the while avoiding direct blame during the campaign. Meanwhile, as they prepare for their own upcoming elections, France and Germany have become Russia's latest targets.[14]

The Western Response

The West is beginning to acknowledge the disinformation threat. An annual mapping project by the Duke University Reporters Lab shows there are now at least 114 active fact-checking operations around the world, up from 44 since 2014.[15] The BBC,[16] Facebook[17] and others have set up their own debunking efforts. In late 2016, the Countering Information Warfare Act, better known as the "Portman-Murphy Disinformation Act" was signed into law by U.S. President Barack Obama.[18] The Act sets up an anti-disinformation coordination, research, and analysis center within the U.S. government and allocates $20 million yearly for two years to support its work. During the drafting of this paper, several NATO and EU countries announced the establishment of a new center to counter so-called "hybrid threats" and increase cooperation between the two multilateral bodies and individual sponsoring states.[19] These are steps in the right direction, to be sure, but as the cottage anti-disinformation industry continues to expand, the donor community must take into account the challenges that make the information war with Russia singularly hard to fight while planning its response.

Challenges in a Multi-Vector Donor Community

The largest policy challenge to the West in its fight against Russian disinformation is the nature of the Russian threat. Russia's disinformation offensive comes from a single country, with a single and expansive budget, and is ostensibly controlled by a single man. Conversely, the Western response is a patchwork of 30 sets of competing foreign policy priorities, different levels of recognition of the disinformation threat by national governments, as well as politically-driven disputes between Western nations leading the response. Even within the European Union, which has recognized the disinformation threat through multiple parliamentary resolutions and acts, the European External Action Service's East StratCom Task Force has not received the funding or personnel it needs to operate effectively, due to purported stonewalling by High Representative for Foreign Affairs and Security Frederica Mogherini.[20] As

Edward Lucas and Peter Pomeranzev observe: "If hybrid war is a joined-up threat, we in the West do not have a joined-up response."[21]

In addition to a lack of coordination among government structures, the information assets the West possesses are also "autonomous and uncoordinated actors in the information space. In Russia's centralized system, a single decision from the Kremlin ripples out to broadcasters, news agencies, social media, websites, and individual journalists."[22] These types of government-controlled narratives were even celebrated by the Kremlin when Putin honored over 300 Russian media workers after their "objective" coverage of Moscow's illegal annexation of Ukraine's Crimean peninsula in 2014.[23] Conversely, the West's strict moral standards regarding freedom of the press and of information leave it ill-equipped to respond to Russian propaganda. While Russia is unafraid to trample on editorial freedoms, "the West believes in categories and boundaries…The West believes in, and practices, the separation of powers. Its adversaries do not."[24]

Finally, many of the Kremlin's disinformation operations fall in large part under the shroud of secrecy encompassing the Russian security services' "active measures" playbook, while the West's media and information-related foreign assistance is open and transparent. Any activity funded by a Western government will be branded as such, presenting a practically insurmountable problem to reaching distrusting populations; no matter how slick, interesting, or well-researched the content, those who already harbor distrust towards the West are unlikely to trust any story or outlet funded through such seemingly-suspicious mechanisms.

Challenges in a Growing Industry

While many of the challenges the West faces in fighting Russian disinformation are endemic to the singularity of the Russian media machine, others are self-created and have arisen due to the growing anti-disinformation industry. As more efforts to stop the spread of disinformation are established across the domestic, multilateral, NGO, and think tank sectors, organizations that should be coordinating and amplifying each other's' work are instead competing for funding and attention.

In interviews, implementers across the information space echoed these concerns and also expressed frustration that the short-term funding cycle on which many Western donors operate leads to a lack of continuity in their activities. Rather than conduct programming based on long-term strategic priorities in the communities they serve, organizations spend much of their time and resources applying for

six-to-twelve-month grants based on priorities dictated months earlier by bureaucrats in Western capitals.

Furthermore, once a grant is won, organizations have no guarantee that their funding stream will be renewed in the next grant cycle. This has a paralyzing effect, particularly within independent media organizations, which incur high costs for technological and human resources. They are often unsure how many staff or what type of studio space they will be able to retain in the long term, which in turn affects the type of in-depth reporting projects they are able to undertake. Finally, interlocutors expressed frustration that the donor community seems to have a desire to "spread the wealth," that is, to stop funding one organization in favor of another that has not yet received Western assistance, without investing in building organizations' business skills to make their work sustainable after assistance evaporates.

The short-term nature of foreign assistance to combat Russian disinformation belies the donor community's focus on surface-level solutions such as fact-checking, awareness-raising campaigns, and other activities that address "low-hanging fruit" and are more likely to yield results over a short implementation period. Projects that require a larger or longer-term investment are either avoided or not funded to full commitment. When discussing the investment that would be required to produce a pan-Baltic or pan-European Russian language television channel, the Executive director of Riga's Centre for East European Policy Studies noted that despite the urgent need for a such an effort in Latvia, "it is hard to promote projects that lack a quick payoff."[25]

Is Fact Checking Effective?

Among surface-level solutions, the Western donor community places a particular emphasis on fact-checking efforts. In some ways, this is logical; fact-checking efforts do provide an important dataset for other analytical work that allows governments to track, identify, and predict trends in narratives and tools of Russian disinformation. Part of the $20 million budget for the U.S. center to address disinformation, approved as part of the Portman-Murphy Disinformation Act, is to be allocated "to support local independent media who are best placed to refute foreign disinformation and manipulation in their own communities."[26] The priority to support local independent media is commendable, but the law's focus on "refuting" propaganda is indicative of the lack of nuance in the overall debate about disinformation. The problem is not simply a lack of facts; it is a dearth of people who trust those facts and the media or governments communicating them.

Fact-checking, whether carried out by governments or media organizations, does not address the growing trust gap. In some cases, it does the opposite, further fueling and even legitimizing conspiracy theories and claims found on fringe websites. The "#Pizzagate" conspiracy theories that emerged during the 2016 U.S. Presidential Election are an excellent example of fact-checking gone wrong:

> Across the country, major news outlets went to great effort to challenge conspiracy reports that linked John Podesta and Hillary Clinton to a child trafficking ring supposedly run out of a pizza shop in Washington, DC. Most people never heard the conspiracy stories, but their ears perked up when the mainstream press went nuts trying to debunk these stories. For many people who distrust "liberal" media and were already primed not to trust Clinton, the abundant reporting suggested that there was something to investigate.[27]

Fact-checking efforts are also met with a particular connotation in the former communist space, where freedoms of information and speech are highly-regarded and recently-gained rights. Jaroslav Plesl, editor of *Dnes*, the second-largest Czech daily, believes that Western efforts to fact-check are misguided: "I don't believe in fighting information. That's what the communists did. If governments continue this behavior, it will divide society and cause mistrust in democracy," he said in an interview. "People think that fighting lies means fighting opinion."[28]

Organizations engaged in debunking have made few inroads in reaching the populations most susceptible to a belief in Russian disinformation. Several, including Ukraine's StopFake.org and the European External Action Service's Disinformation Review, have a fairly robust reach on social media, but "to some extent these websites are preaching to the converted. If you access a site called StopFake.org, you are likely to have an awareness that you may be exposed to propaganda."[29] Further, many of the most distrusting populations in Europe reside in areas with low internet penetration and are more likely to follow news on television rather than the Internet. Whether individuals from the broader population are engaged with these efforts, as well as ways to reach groups offline, is worth studying.

Most importantly, a focus on fact checking inherently cedes control over the Western narrative to Russia and other purveyors of disinformation. Where the West and the organizations it supports should be proactively connecting with distrusting populations, we are instead reacting to and trying to stem the flow of the "firehose of falsehoods" emanating from Russia.[30] Without a focus on repairing the trust gap, the

phenomenon that makes populations susceptible to Russian disinformation, and given the challenges laid out above, this is a losing strategy.

Recommendations

The threat of disinformation has sounded alarm bells across the West and there is, at last, a growing recognition of its impact, not only on discrete events such as elections, but on democratic systems and societies as a whole. It is high time for Western governments to make a long-term effort to ensure that their investments reach beyond gatherings of like-minded bureaucrats and activists in Washington, London, and Brussels. The implementation of such a strategy must come with the understanding that it may not fit neatly into existing metrics by which governments measure performance, and indeed, may take much longer than the typical grant lifecycle to yield results. But it is critical that anti-disinformation efforts prioritize reaching the mass population in order to bridge the trust gap.

Invest in Skills-Building Programs

The West must make long-term investments in skills-building programs and campaigns to begin the long and difficult work of repairing the trust gap. These investments should support two populations -- ordinary citizens and journalists -- through programs specifically designed to address the root cause of disinformation's resonance in the West.

Citizen Media Literacy

It can be difficult even for highly-educated media consumers to spot disinformation, so it is critical that we empower citizens to navigate the confusing 21st-century media market. Rather than develop clunky curricula implemented through the traditional NGO training model, Ondrej Soukoup, a Czech journalist, believes that we "need to do media literacy in terms people understand. How do you spot sensationalism? How do you realize when someone is deliberately targeting your emotions?"[31]

A Canadian-funded project implemented by IREX in Ukraine married a network of highly-skilled media trainers with an awareness-raising campaign to successfully "enhance citizen capacity to establish reliability of news sources and content...[and] increase public demand for truthful reporting."[32] IREX created a new curriculum for media consumption, drawing on StopFake.org's large database of debunked fake news stories for examples. The curriculum covered topics such as "avoiding emotional

manipulation," "verifying expert credentials" and "detecting censorship." It was used to train 400 trainers who trained 15,000 people in key oblasts around Ukraine. IREX also launched an [ad](#) [campaign](#) reminding citizens: "Information is a product: consume wisely." It reached "approximately 20 million TV viewers, 8 million radio listeners, 10,000 YouTube users, and countless Metro riders." In nine months and with $600,000 (CAN), the program recorded a 23% increase in those who cross-checked the news they consumed.

The IREX program shows what is possible when even a small investment of time and money is made to reach beyond the policymaking community to ordinary people. Admittedly, the 15,000 people trained by IREX represent only a small fraction of Ukraine's 45 million citizens, but a multi-year investment could have a much wider reach, particularly if the curriculum were rolled out in courses for students from primary school to university, government employees and even politicians. The Western donor community, as well as governments affected by disinformation and searching for domestic solutions, should also look beyond the traditional NGO implementation model to deliver whole-of-government programs. For example, while discussing the Czech Republic's newly-minted Hybrid Threats Center, housed within the Ministry of Interior and charged with countering domestic disinformation threats, Mark Galeotti posited that "arguably even more useful [than the establishment of the Hybrid Threats Center] would be task forces within the Ministry of Education, Youth & Sports and the Ministry of Culture, to train young Czechs to consume media wisely and skeptically and crack down on the purveyors of 'fake news,' respectively."

Supporting Journalists

Investing in journalism, particularly at the local level, is also paramount to bridging the trust gap. While the donor community has spent many years harnessing the resources and wherewithal to launch television networks meant to provide the Western answer to RT, supporting the continued existence, professional development, and proliferation of pre-existing local media organizations could be a less costly and more effective venture.

While pan-regional television networks or media organizations focus on problems on an international scale, a focus on local outlets that address local problems, whether in former communist countries or the West, can help reconnect citizens to the news. Public broadcasters and government-sponsored multilateral outlets often lack an understanding of the issues affecting the daily lives of local populations. Their editorial strategies are "crafted by European or North American men in suits [sitting] behind a

computer in an office. But one cannot help but wonder how that man in a suit knows what messages will resonate with…the miner in East Ukraine."[34] Furthermore, "although independent media exist throughout the region, many struggle on extremely limited resources. That, in turn, prevents them from acquiring or producing high-quality content and reaching critical mass audiences."[35] Rather than reinvent the wheel by creating new media outlets, the donor community should consider supporting and empowering outlets that already exist.

Free Press Unlimited's Russian Language News Exchange provides one sustainable model for local content creation and journalist training. The program supports privately-owned, independent local news initiatives in seven Eastern European countries to "increase access to balanced and reliable Russian-language information," with a focus on content that is resonant to local populations.[36] In addition to encouraging the production and exchange of high-quality reporting on all platforms (radio, television, print, digital), the Exchange aims to build business skills among its members so that they become self-sustaining. In one year and for less than $150,000 per country, it supported the production of over 500 stories viewed a minimum of 1 million times each across platforms.[37]

Continue Strategic Funding of Analytical, Fact-Checking, and Consciousness-Raising Work

Prioritizing the repair of the trust gap does not mean that the donor community or host governments should completely reorient their efforts away from analytical, fact-checking, and consciousness-raising work. As is evident from case studies conducted as part of this research (see Appendix), some of these programs have made a significant impact on governments' and policymakers' understanding and awareness of disinformation and provide valuable insight as we plan programs such as those described above. However, the donor community must still be more strategic about what is funded and why. We must also be realistic about the goals of such programs, recognizing that they have a much more narrow reach than ideal.

We should continue to support organizations that are experienced and produce quality analysis. If these organizations are grant-dependent, we should offer them training to help them achieve sustainability before redirecting funding. Additionally, we should prioritize programming that requires working-level cooperation between organizations in this category, not only to encourage the sharing of best practices, but also to avoid duplication of efforts.

Change the Funding Paradigm

Equipping people with media consumption skills and rebuilding a struggling industry from the local level are not and cannot be short-term investments. Just as Russia's disinformation campaigns have lasted for more than the lifecycle of a typical foreign assistance grant, so should our investments in bridging the trust gap. The current foreign assistance funding paradigm places a great burden on grantees, who spend an inordinate amount of time applying for and reporting on projects, rather than actually doing the work necessary to gain ground in the fight against Russian disinformation.

Across the board, we must invest in longer programs with more flexible, grantee-dictated deliverables, and, wherever possible, reduce reporting requirements on grantees. This will ensure that organizations fighting disinformation are able to respond nimbly to the rapidly-changing information environment, not waiting for their grant officer to authorize a shift in their program evaluation plan or worrying if they will be able to pay their office rent and staff in six months.

Western donors should also consider expanding the list of assistance beneficiaries eligible to receive support to fight disinformation. Countries like the Czech Republic and Poland that have "graduated" from foreign assistance are often ineligible to receive funding earmarked for "fighting Russian propaganda" in countries that are current assistance recipients, such as Ukraine, Moldova and Georgia. However, the goals of Russian disinformation in graduated countries often involve influencing public opinion both about relationships with the Eastern Partnership countries and towards the EU and NATO, accession to which current assistance beneficiaries are pursuing.

Conclusion

The solutions discussed in this paper will not yield results overnight. By and large, they represent change that will occur on a generational scale, and our foreign assistance paradigms should reflect this. Most of all, bridging the trust gap requires a global vision of what winning the information war looks like. If our efforts are successful, people will consume information responsibly, sampling a range of viewpoints to inform their daily lives and the criticism that is healthy for any democracy, while developing greater immunity to conspiratorial versions of the truth. Western democracies and the transatlantic community as a whole will be stronger if we work *with* people instead of simply talking to them. We live in an era in which labeling something "fake" is becoming synonymous with political inconvenience. Now, more than

ever, people need access to high-quality information and the ability to recognize it when they see it, enabling them to resist disinformation across the board, whoever the distributor.

Appendix

Case Studies

A snapshot of programming undertaken since experts began to sound alarm bells about Russia's disinformation activities can also aid in understanding the disinformation climate in Europe and the challenges the West faces in countering the disinformation threat.

The pullouts in this appendix are based on interviews conducted in January - March 2017 as well as open source information. Interlocutors for these programs were interviewed as representatives of each of the four main types of implementers of the response to disinformation: NGOs, think tanks, domestic and multilateral groups. They are working across several lines of effort: fact-checking, awareness-building, lobbying, and direct support programs to citizens or organizations, and are working in each of the representative information environments in Europe.

The following is by no means an exhaustive list or in-depth description of ongoing programming, but an attempt to characterize the current efforts and identify best practices in a digestible manner to assist governments as they begin to focus their responses to Russian disinformation.

StopFake.Org

Founded: 2 March 2014

Affiliation: National University of Kyiv-Mohyla Academy, School of Journalism

Location: Kyiv, Ukraine

Funding: Currently: crowdfunding donations, International Renaissance Foundation, Czech Foreign Ministry , the British Embassy in Ukraine, Sigrid Rausing Trust. Past donors include National Endowment for Democracy, U.S. Embassy Kyiv.

Type of organization: Media/Non-profit

Line(s) of effort: Fact-checking and analysis; also conducts fact-checking trainings for journalists and public officials in the Eastern Europe region.

Objectives: Verify and refute disinformation and propaganda about events in Ukraine being circulated in the media; examine and analyze all aspects of Kremlin propaganda.[38]

Audience: "Ukraine-watchers" throughout the West, as well as a growing audience within Russia itself. StopFake content is translated into 10 languages.

Reach: Twitter: 21,7k; Facebook: 6.1k

Evaluation: StopFake has amassed an impressive database of over 1,000 fakes, which allows researchers to identify and track trends in the implementation of Russian disinformation.

The team estimates that half of all StopFake's readers organically access the website from Russia, which means their message is achieving resonance in one of the most restrictive information environments, likely because of its high quality and availability in Russian language.

StopFake's journalist trainings have an effect beyond awareness-raising; Moldova's TV regulator took the decision to apply broadcasting standards to Russian language networks after a StopFake training.

European Values Think Tank - Kremlin Watch Monitor

Founded: 2015

Funding: Private donors, Open Society Foundation, National Endowment for Democracy, US Embassy Prague, UK Embassy Prague, Konrad Adenauer Stiftung, Czech MFA, International Visegrad Group, European Parliament, and others cited in the organization's annual report.

Location: Prague, Czech Republic

Type of organization: Operates as a think tank; registered as a civic association.

Line(s) of effort: Fact-checking/analysis

Objectives: 1) Operational analysis of disinformation efforts
2) Weekly reports on disinformation trends in CZ and in EU
3) Specific case studies on disinformation cases
4) Development & advising for democratic policy responses on tactical and strategic level
5) Educational activities for general public & trainings for practitioners
6) Public and behind-close door advocacy for awareness of disinformation efforts in media and on policy-makers level

Audience: European / Western Policymaking community

Reach: 12.8k, FB: 8.6k

Evaluation: Extensive research and lobbying conducted by the European Values Think Tank led to the creation of the Czech Hybrid Threats Center.

"Name and shame" strategy using research connecting Czech publications with disinformation outlets led to the largest Czech bank (*Ceska sporitelna*) removing its advertisements from over 40 publications towing the Kremlin line.

EEAS East StratCom Task Force - Disinfo Review

Founded: September 2015

Affiliation: European Union

Location: Brussels, Belgium

Funding: "The East StratCom Task Force draws on existing resources within the EU institutions and the Member States, including staff from institutions and seconded national experts from Member States. The Task Force works within the existing budget for EU Strategic Communication – both at headquarters and delegation level."[39]

Type of organization: Multilateral

Line(s) of effort: Fact-checking; awareness-raising; strategic communications

Objectives: The Disinformation Review "analyzes disinformation trends, explains disinformation narratives, and [conducts] myth-busting." It also raises awareness of disinformation and provides data for "analysts, journalists and officials dealing with this issue."[40]

The EEAS East StratCom Task Force also has a strategic communications branch concerned with communicating EU priorities and narratives to the Eastern neighborhood.

Audience: EU policymakers; Ukraine/Russia watchers

Reach: Twitter: 23.1k, FB: 15k

Evaluation: In the 18 months of the Disinfo Review's existence, they have successfully raised awareness of the threat of disinformation in European Parliament, which passed a resolution recognizing the threat and calling for increased funding and staff for the task force (which High Commissioner Mogherini did not heed).[41]

Polygraph.info

Founded: 2016

Affiliation: Joint project of Voice of America and Radio Free Europe/Radio Liberty

Location: Prague, Czech Republic

Funding: Voice of America and Radio Free Europe/Radio Liberty

Type of organization: Media

Line(s) of effort: Fact-checking

Objectives: Act as "a resource for verifying the increasing volume of disinformation and misinformation being distributed and shared globally. Teams of journalists from RFE/RL and VOA research and analyze quotes, stories, and reports distributed by government officials, government-sponsored media and other high-profile individuals. The reporters separate fact from fiction, add context, and debunk lies."[42]

Audience: Speakers of English (as a second language) in the Former Soviet Union

Reach: Twitter: 900, FB: 1,740

Evaluation: It is too early to rate Polygraph's successes, though its target audience is peculiar, given the combined translation resources of VOA and RFE/RL. One might assume their reach and resonance would be much higher if stories were translated into local languages.

NATO StratCom Center Of Excellence

Founded: 2014

Affiliation: NATO (Member states: Estonia, Germany, Italy, Latvia, Lithuania, Poland, and the United Kingdom)

Location: Riga, Latvia

Funding: Staffed and financed by sponsoring nations and contributing participants.

Type of organization: Multilateral

Line(s) of effort: Analysis, Awareness Raising

Objectives: Enhance NATO strategic communications capabilities through research and analysis.

Audience: NATO; Policymakers in NATO member states

Reach: Twitter: 5.3k, FB: 10k

Evaluation: Among its achievements the COE lists trainings and courses on disinformation it conducts for NATO officials, senior government officials among member states, as well as governments in the Eastern neighborhood.

Outside of these activities, the COE mostly conducts studies based on requests from NATO member states, some of which are made public. It's study on Germany's "Lisa" case was the most highly accessed of all its work.

Hybrid Threats Center, Czech Ministry of Interior

Founded: 2017

Affiliation: Czech Government

Location: Prague, Czech Republic

Funding: Czech Ministry of Interior

Type of organization: Unilateral / governmental

Line(s) of effort: Analysis / fact-checking

Objectives: "Monitor threats directly related to internal security... including disinformation campaigns related to internal security."[43] Advise the government on threats in Czech information space; publicly debunk fakes pertaining to domestic issues.

Audience: Czech government policymakers, Czech citizens

Reach: Twitter: 6k

Evaluation: The Center has only been operational for four months, so it is too soon to measure success.

However, it has run into a few problems that could serve as lessons learned for governments pursuing a similar strategy. It faced political backlash from President Zeman and his supporters, who compared its mission to that of a Communist-era "Ministry of Truth."[44] The Hybrid Threat Center's specialists are now forced to communicate about the necessity of their existence in addition to the rest of their portfolio. Governments considering a similar intervention should take note of these difficulties, making sure to widely and clearly communicate goals before launching any new effort, and perhaps consider whether the public arm of such an effort would be worth its potential perception by citizens or hostile parties as an affront to freedom of speech.

"Learn to Discern" Program, IREX

Program Active: July 2015-March 2016

Type of organization: Non-profit

Location: Ukraine

Funding: Canadian government

Line(s) of effort: Direct support / training to citizens

Objectives: 'To strengthen Ukrainians' resilience in the face of destabilizing misinformation by: (1) Enhancing citizen capacity to establish reliability of news sources and content; (2) Increasing public demand for truthful reporting in the 14 eastern, southern, and central target oblasts."[45]

Audience: Adult Ukrainians

Reach: 400 trainers trained 15,000 citizens who had contact with 90,000 others about the training

Ad campaign reached at least 2.3 million Ukrainians

Evaluation: "89% of training participants surveyed reported using their new skills (e.g. the number of trainees who "almost always" crosscheck the news they consume increased from 21% to 50% over three months);

54% of the 2.3 million Ukrainians who viewed the information campaign during its first two weeks reported a need for skills in discerning untruthful reporting."[46]

Focus on equipping citizens with skills necessary to navigate today's cacophony of digital media not only shows citizens how to fact check on their own, but teaches them to recognize when they are being emotionally manipulated.

Russian Language News Exchange, Free Press Unlimited

Program Active: September 2016 - present (currently funded through 2019)

Location: Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine and Russia.

Funding: Government of the Netherlands and a range of European governments and institutions.

Type of organization: Non-Profit

Line(s) of effort: Direct support /training to media

Objectives: To contribute to the increased quality of information available in Russian-speaking region by providing reliable, balanced, timely and accurate news and information in Russian.

To increase the capacity of independent media outlets in countries with significant Russian-speaking populations to provide audiences with independent local, regional and international news and analysis, offering an alternative to Moscow-based content, through producing and distributing high quality reporting.

Audience: Reporters/media outlets in Eastern Partnership countries;
Russian speakers in Eastern Partnership countries

Reach: Each story produced by the exchange in 2016 had at least 1 million views across platforms.

Evaluation: In 2016, RLNE produced and exchanged more than 500 stories and trained 35 journalists and editors trained in new media, web strategies and international reporting.

Focus on local reporting with an eye to the Eastern Partnership region, rather than the international stories that dominate Russian disinformation and legitimate international press allows Exchange members to begin to bridge the trust gap.

Endnotes

[1] Edward Lucas and Ben Nimmo. "Information Warfare: What Is It and How to Win It?," Center For European Policy Analysis, November 2015: 7.

[2] Edward Lucas and Peter Pomeranzev. "Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe," Center for European Policy Analysis, August 2016: 5.

[3] Richard Edelman. "An Implosion of Trust." Edelman, 15 January 2017.

[4] Jerzy Pomianowski. "Key findings of the EED's Feasibility Study on independent Russian-language media initiatives in the Eastern Partnership and beyond," Foundation for European Progressive Studies, *Resisting Foreign state Propaganda in the new Information Environment: the Case of the EU, Russia, and the Eastern Partnership Countries*, September 2016: 93.

[5] European Commission, "Trust in National Government," EC Public Opinion, November 2016.

[6] Gallup, Inc., "Ukrainians Disillusioned With Leadership," December 23, 2015.

[7] Kiev International Institute of Sociology, "Trust to Social Institutions," December 2016.

[8] Lucas and Pomeranzev, 8.

[9] Jakub Janda, "The Lisa Case: STRATCOM Lessons for European states," Federal Academy of Security Policy, Security Policy Working Paper, No. 11/2016: 2.

[10] Stefan Meister, "The Lisa Case: Germany as a target of Russian disinformation," NATO Review, 2016.

[11] Lucas and Pomeranzev, 15-20.

[12] Prague Security Studies Institute, "Summary of an Expert Roundtable: Russian Influence in Central Europe," 27 February 2017.

[13] Dan McLaughlin. "Weaponizing History: World War II Memorial Attackers Aim to Divide Poland and Ukraine," *Coda Story,* 27 February 2017.

[14] Daniel Boffey and Jennifer Rankin. "EU escalates its campaign against Russian propaganda," *The Guardian,* 23 January 2017.

[15] Duke Reporters' Lab, "International fact-checking gains ground, Duke census finds." 25 March 2017.

[16] Jasper Jackson, "BBC sets up team to debunk fake news," *The Guardian,* 12 January 2017.

[17] Jen Weedon, William Nuland and Alex Stamos, "Information Operations and Facebook," 27 April 2017.

[18] "President Signs Portman-Murphy Counter-Propaganda Bill into Law," 23 December 2016.

[19] Rosendahl, Jussi, and Tuomas Forsell. "EU, NATO Countries Kick off Center to Counter 'Hybrid' Threats." *Reuters*, 11 April 2017.

[20] European Values Think Tank, "Open Letter to Frederica Mogherini: Please start taking the Russian disinformation threat seriously!", 20 March 2017.

[21] Lucas and Pomeranzev, 13.

[22] *Ibid,* 10.

[23] Claiire Bigg. "Putin Awards 300 Journalists For 'Objective' Crimea Coverage," *RFE/RL*, 06 May 2014.

[24] Lucas and Nimmo, 8.

[25] "Interview with Andis Kudors." Personal interview. 20 February 2017.

[26] United States Congress, Senate. "Countering Information Warfare Act of 2016," Sen. Rob Portman and Sen. Chris Murphy. 114th Cong., 2nd sess. S 2692.

[27] Danah Boyd. "Did Media Literacy Backfire?" Data & Society: Points. 5 January 2017.

[28] "Interview with Jaroslav Plesl." Personal Interview. 19 January 2017.

[29] Paul Copeland, "Factual Entertainment: How to Make Media Literacy Popular," The Legatum Institute, August 2016: 21.

[30] Christopher Paul and Miriam Matthews, "The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation, 2016.

[31] "Interview with Ondrej Soukoup." Personal Interview. 18 January 2017.

[32] "Learn to Discern," International Research and Exchanges Board, 2017.

[33] Mark Galeotti, "One-and-a-Half Cheers for new Czech centre to resist Political Warfare," *In Moscow's Shadows*, 28 December 2016.

[34] Steve Tatham, "Target Audience Analysis," *Three Swords*, May 2015, 50-53, cited in Lucas and Nimmo, 15.

[35] Pomianowski 94.

[36] "Russian Language News Exchange Supports Independent Media," Free Press Unlimited.

[37] *Ibid.*

[38] "About us," StopFake.org.

[39] "Questions and Answers about the East StratCom Task Force," EEAS, 5 January 2017.

[40] *Ibid.*

[41] "MEPs Sound Alarm on Anti-EU Propaganda from Russia and Islamist Terrorist Groups," European Parliament, 23 November 2016.

[42] "About," Polygraph.info.

[43] "Centre Against Terrorism and Hybrid Threats," Ministry of Interior of the Czech Republic.

[44] Jan Lopatka, "Czech 'Hybrid Threats' Center under Fire from Country's Own President." Reuters, 4 January 2017.

[45] "Learn to Discern," IREX.

[46] *Ibid.*

Nina Jankowicz is a communications, democracy, and governance specialist with a focus on Eastern Europe and the former Soviet Union. She currently serves as a Fulbright-Clinton Public Policy Fellow in Ukraine's Ministry of Foreign Affairs. Prior to her work in Ukraine, Ms. Jankowicz was a Program Officer at the National Democratic Institute for International Affairs (NDI), where she managed NDI's democracy assistance programs to Russia and Belarus and later joined NDI's Government Relations and Communications team.

Ms. Jankowicz received her MA in Russian, Eurasian, and East European Studies from Georgetown University's Edmund A. Walsh School of Foreign Service, where she was a Title VIII and FLAS scholarship recipient, and her BA from Bryn Mawr College, where she graduated *magna cum laude*. She has lived and worked in Ukraine and Russia, and speaks fluent Russian and proficient Ukrainian and Polish.

nina.jankowicz@gmail.com | www.tinyletter.com/wiczipedia | @wiczipedia