RUSSIAN DISINFORMATION ATTACKS ON ELECTIONS: LESSONS FROM EUROPE

HEARING

BEFORE THE

SUBCOMMITTEE ON EUROPE, EURASIA, ENERGY, AND THE ENVIRONMENT

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

July 16, 2019

Serial No. 116–55

Printed for the use of the Committee on Foreign Affairs

Available: http://www.foreignaffairs.house.gov/, http://docs.house.gov, or http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
37–051PDF WASHINGTON : 2019

COMMITTEE ON FOREIGN AFFAIRS

ELIOT L. ENGEL, New York, *Chairman*

BRAD SHERMAN, California
GREGORY W. MEEKS, New York
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
THEODORE E. DEUTCH, Florida
KAREN BASS, California
WILLIAM KEATING, Massachusetts
DAVID CICILLINE, Rhode Island
AMI BERA, California
JOAQUIN CASTRO, Texas
DINA TITUS, Nevada
ADRIANO ESPAILLAT, New York
TED LIEU, California
SUSAN WILD, Pennsylvania
DEAN PHILLIPS, Minnesota
ILHAN OMAR, Minnesota
COLIN ALLRED, Texas
ANDY LEVIN, Michigan
ABIGAIL SPANBERGER, Virginia
CHRISSY HOULAHAN, Pennsylvania
TOM MALINOWSKI, New Jersey
DAVID TRONE, Maryland
JIM COSTA, California
JUAN VARGAS, California
VICENTE GONZALEZ, Texas

MICHAEL T. MCCAUL, Texas, *Ranking Member*
CHRISTOPHER H. SMITH, New Jersey
STEVE CHABOT, Ohio
JOE WILSON, South Carolina
SCOTT PERRY, Pennsylvania
TED S. YOHO, Florida
ADAM KINZINGER, Illinois
LEE ZELDIN, New York
JIM SENSENBRENNER, Wisconsin
ANN WAGNER, Missouri
BRIAN MAST, Florida
FRANCIS ROONEY, Florida
BRIAN FITZPATRICK, Pennsylvania
JOHN CURTIS, Utah
KEN BUCK, Colorado
RON WRIGHT, Texas
GUY RESCHENTHALER, Pennsylvania
TIM BURCHETT, Tennessee
GREG PENCE, Indiana
STEVE WATKINS, Kansas
MIKE GUEST, Mississippi

JASON STEINBAUM, *Staff Director*
BRENDAN SHIELDS, *Republican Staff Director*

SUBCOMMITTEE ON EUROPE, EURASIA, ENERGY, AND THE ENVIRONMENT

WILLIAM KEATING, Massachusetts, *Chairman*

ABIGAIL SPANBERGER, Virginia
GREGORY MEEKS, New York
ALBIO SIRES, New Jersey
THEODORE DEUTCH, Florida
DAVID CICILLINE, Rhode Island
JOAQUIN CASTRO, Texas
DINA TITUS, Nevada
SUSAN WILD, Pennsylvania
DAVID TRONE, Maryland
JIM COSTA, California
VICENTE GONZALEZ, Texas

ADAM KINZINGER, Illinois, *Ranking Member*
JOE WILSON, South Carolina
ANN WAGNER, Missouri
JIM SENSENBRENNER, Wisconsin
FRANCIS ROONEY, Florida
BRIAN FITZPATRICK, Pennsylvania
GREG PENCE, Indiana
RON WRIGHT, Texas
MIKE GUEST, Mississippi
TIM BURCHETT, Tennessee

GABRIELLE GOULD, *Staff Director*

CONTENTS

RUSSIAN DISINFORMATION ATTACKS ON ELECTIONS: LESSONS FROM EUROPE

Tuesday, July 16, 2019

House of Representatives,

Subcommittee on Europe, Eurasia,

Energy, and the Environment,

Committee on Foreign Affairs,

Washington, DC

The subcommittee met, pursuant to notice, at 2:21 p.m., in room 2172, Rayburn House Office Building, Hon. William R. Keating (chairman of the subcommittee) presiding.

Mr. KEATING. The hearing will come to order.

I want to thank the members that made it up from the last roll call. We were delayed a bit as a result of a roll call. I want to thank our witnesses for their patience in that regard.

Our national elections are just 15-plus months away. Just this week, AP reported describing how voting systems across our country still rely on old software that is vulnerable to hackers. The list of threats to our elections are numerous, and it is our job to address the weaknesses with the utmost haste and diligence.

Our intelligence community is united in its findings that the U.S. will once again face Russian threats to our elections and our democratic process, and other countries could indeed follow suit. We know countries like China are already stepping up disinformation efforts on their own.

Today's hearing is on Russia's attacks on democratic elections through targeted disinformation campaigns and the takeaways from Europe where this activity has been accelerating for years. It is on what the EU and the European countries are doing themselves, what has been effective, what has not been, lessons learned.

The United States awoke to the threat from Russian disinformation as a result of the interference in the 2016 Presidential elections. Yet this malign tactic is nothing new for our allies and partners in Europe who have experienced disinformation campaigns since the time of the Soviet Union.

Based on this experience and after Russia's invasion of Ukraine in 2014, Finland put in place a whole government strategy to combat Russian disinformation and increase the resiliency of its population against these attacks.

We are lucky today to be joined by Ms. Jessikka Aro, who is a journalist from Finland and has reported extensively on this topic. And while it was rescinded under questionable circumstances, she would have received an International Women of Courage award earlier this year for her work exposing the network of pro-Kremlin trolls linked to the Russian Internet Research Agency, a Russian

institution which, as we all know, was heavily involved in the 2016 Russian interference in our election. That was detailed in part one of the Special Counsel Mueller report.

Finland is not alone. Following numerous elections and referenda where Russia and Russian-supported actors spread disinformation and stoked conflict between and around public debates, including in the recent EU parliamentary elections, the European Union and its member States have since deployed strategies to combat Russia's malign influence.

U.S. elections are the very bedrock of our democracy. And as Members of Congress, we have shown an oath to uphold that kind of protection of our democracy.

Russian interference undermines our elections, as well as those of other countries around the world, while stoking anti-Western sentiment and threatening our alliances and our security. We have to do more.

In today's hearing we examine the lessons from our allies in Europe and we will explore areas where transatlantic cooperation serve us in advancing our response to Russian election meddling here at home.

We are faced by different types of disinformation, different actors who perpetuate it. Different options for trying to stop it have been put into place, but there are efforts to even destabilize those types of efforts.

This is where learning from our European partners comes into play. While there have been steep challenges in their effort to combat Russia's disinformation activities, we could build on their progress and start moving much more aggressively to address this here at home.

So today I hope we can learn more about what has worked, what has not worked, what opportunities exist to engage with civil society, social media companies, our legal system, multilateral institutions, how countries are increasing their resilience through media literacy programs, even some of those at the grade school level.

And this is important: How investigative journalism has helped expose Russian disinformation and what we need to do to protect those individuals who take on great risk to defend the democratic institutions that we all depend on to safeguard our freedoms.

Just as we are seeing in Europe, we will likely need to adjust course from time-to-time, monitor to make sure protections against disinformation do not veer toward unjustly restricting freedom of speech or failing to appropriately respect privacy concerns.

Our enemies use our freedoms as a type of sanctuary. However, we have to do more. So as soon as it is possible, on a number of fronts, we will move forward.

Our efforts to date, as a government, and the efforts among social media companies and other private sectors, have been woefully lacking compared to the threat we face.

I would like to thank the witnesses for joining us and some for traveling great distances to be here today. Your testimony and expertise are greatly appreciated. I hope that we can come away with some concrete next steps to guard against Russian disinformation campaigns here at home and those affecting our allies overseas.

With that, I would like to recognize the ranking member, and then I will go through some of the ground rules of this hearing.

So I recognize the ranking member, Mr. Kinzinger.

Mr. KINZINGER. Thank you, Mr. Chairman.

And thank you to the panel for joining us today. You have all great reputations, your work proceeds you, and we are excited to have you here with us.

Prior to the 2016 election, Russia engaged in one of the most sophisticated information operations to date against the United States. Regardless of your opinion of the Mueller report and reading the first part of that and seeing the depth of Russian attempts is eye opening, to be involved in this election, as well as elections in other parts of the world.

This was not the first time that Russia has used disinformation or malign influence to interfere in the democratic process of Western society and I guarantee it will not be the last. Russian trolls will amplify any message that seeks to divide Western democracy and sow discord and chaos.

From supporting Code Pink and fascist groups in the United States to spreading anti-European Union and anti-NATO messages across Europe, Vladimir Putin's goal is to divide the bond that holds democratic nations together. As long as Putin's hold on power remains unchallenged, he will continue to meddle in Western democracy.

I believe that we must go on the offensive. While Vladimir Putin won a sham reelection and will be in office until 2025, the State Duma is slated to have an election in 2021. That means that the United States has just over 2 years to highlight how Putin's corrupt tactics have stolen money from the Russian population, devaStated their economy, and ostracized their nation from the West.

From an economic standpoint, Russia's GDP of $1.65 trillion is dwarfed by that of the United States and the European Union, which sits around the $40 trillion mark. However, in far-off places like Venezuela, Syria, Ukraine, Georgia, and across the Baltic and Balkan regions, Russia can use little capital to extract unproportionate pressure.

Take Ukraine, for example, where Russian propaganda targeted a joint U.S.-Ukrainian training exercise claiming that American troops were going to provoke protests across Ukraine to interfere in their electoral process. While this operation was easily debunked, it shows how the Russians use a handful of hackers to spread lies through social media. However, other operations take decades of planning and complex support networks to execute.

It has been almost 25 years since the Dayton Peace Agreement ended the war in Bosnia and Herzegovina. However, Russia has used this time to support nationalist politicians within the republic, the main belligerents of the Bosnian war that employed genocide and killed over 100,000 people.

Last October, Bosnia held legislative elections. Since they have been unable to form a government, given disagreements between pro-Western political parties and the nationalist Serb parties over what the relationship Bosnia should have with NATO.

Staunch anti-NATO sentiment and threatened cessation from Bosnia has been a staple of the Russian-backed Alliance of the

Independent Social Democrats, who have, in effect, been blocking the government formation over NATO accession.

The Europeans have abandoned Bosnia, and the United States cannot carry all the weight. If we want to counter Russian malign operations, we must do so in conjunction with our European allies. We must show Bosnia and other nations being tempted by Putin that Western democracy is a far better option than the tyrannical Russian system.

Examples like Bosnia and Ukraine show why holding a hearing to expose Russian malign influence is so important.

And I want to put a bit of an emphasis on having recently met with representatives from the Balkan region, from all areas, every one of them mentioned, without exception, that the United States is basically the only partner standing strong with them against the Russians.

And that is not our backyard. That is Europe's backyard. Europe has a responsibility to step up and do more as well. This cannot be a U.S.-only operation, but we are happy to lead with our European friends.

And I thank last I will say this. Part of exposing Russian disinformation is understanding that if you see a news report or a media report that seems way too crazy, it probably is. Many of us here have been involved in or had written articles about us by Russian trolls that are then posted by Sputnik or RT and retweeted multiple times until it becomes mainstream.

By the way, did you know that I helped create ISIS, according to some RT story that was put out there?

So that said, understanding the idiocy of some of the stuff you read is the first step to pushing back against Russian disinformation, because without that they have no other weapon.

So with that, Mr. Chairman, I yield back.

Mr. KEATING. The chair thanks the ranking member.

And I will now introduce our witnesses.

Ambassador Daniel Fried is a distinguished fellow with the Future Europe Initiative and Eurasia Center at the Atlantic Council. He has previously served as the State Department coordinator for sanctions policy, assistant secretary of State for European and Eurasian Affairs, and the United States Ambassador to Poland.

Thank you for your service, and thank you for being here, Ambassador.

Ms. Jessikka Aro is a Finnish journalist, working for Finland's public service broadcaster Yle. She has received awards for investigative journalism on pro-Russian internet troll factories, having traveled to St. Petersburg to interview employees of the Internet Research Agency and the Russian journalists who first uncovered them.

Thank you for making the trip here.

Mr. Jakub Kalensky is a senior fellow with the Eurasia Center at the Atlantic Council. He formerly worked for the European Union's East StratCom Task Force and was the leader for countering disinformation.

Thank you for being here.

Dr. Fred Kagan is a resident scholar and director of the Critical Threats Project at the American Enterprise Institute. He is for-

merly a professor of military history at the U.S. Military Academy at West Point.

Thank you.

We all appreciate your being here and look forward to your testimony. Please limit your testimony to 5 minutes. And without objection, your prepared written statements will be made part of the record.

As a reminder, all members will have 5 calendar days to submit materials and questions for the record.

I will now go to Ambassador Fried for his statement.

STATEMENT OF DANIEL FRIED, DISTINGUISHED FELLOW, FUTURE EUROPE INITIATIVE AND EURASIA CENTER, ATLANTIC COUNSEL (FORMER STATE DEPARTMENT COORDINATOR FOR SANCTIONS POLICY, FORMER ASSISTANT SECRETARY OF STATE FOR EUROPEAN AND EURASIAN AFFAIRS, AND FORMER UNITED STATES AMBASSADOR TO POLAND)

Mr. FRIED. Chairman Keating, Ranking Member Kinzinger, members, I appreciate the opportunity to appear before you today. The topic is relevant and timely.

I have to say it is an honor to be on this panel with Jessikka Aro and Jakub Kalensky, two fighters against disinformation, and a pleasure to be here with my old colleague, Fred Kagan.

The Russians may be leaders in State-sponsored disinformation, but they are not going to be the last. The Democratic community, the free world, needs to face the challenge of Russian and other forms of contemporary disinformation while remaining true to our democratic values. As we learned during the cold war, we must not and need not become them in order to fight them.

I want to focus on what is to be done. First, the Europeans, then the U.S.

Europeans have moved since 2018 toward action to deal with disinformation. The EU approach includes strengthening the EU's capacity to identify and expose disinformation, and hopefully that includes strengthening support for East StratCom, where Jakub Kalensky used to work. They have established an EU Rapid Alert System to spread news of disinformation campaigns in real time.

Most important, the EU has negotiated and concluded a Code of Practice on disinformation with U.S. social media companies setting out terms of behavior and standards. The code notes that if progress is not satisfactory, the EU could turn to regulation.

The EU is also looking at improving social resilience against disinformation, creating a European network of independent fact checkers, launching an online platform on disinformation, and social media literacy.

European governments, particularly France, Sweden, but others, perhaps in reaction to Russian hacking of the Macron campaign in 2017, have been active. The good news is that the EU and some European national governments have been addressing the disinformation challenge. The bad news is that EU implementation, even of its own plans, has been uneven. This is just beginning.

The United States, though, and I am sorry to say this, lags the EU both in conceptual framing of the issue and actions to deal with

it. This is not due to lack of awareness of the problem inside the administration, but leadership has been uneven.

Nevertheless, there is work ongoing in the administration. The State Department's Global Engagement Center is funding research and helping civil society groups and independent media on the front lines of the threat. U.S. Cyber Command began operations ahead of our last congressional elections to deter Russian operations. USAID is supporting local media and civil society in the European countries most vulnerable to Russian disinformation. The Department of Treasury has imposed sanctions on Russian entities tied to disinformation. The Senate has introduced sanctions legislation, so-called DASKA, which actually has some useful provisions on countering disinformation.

These are good steps, but they lack the scope of what the EU has already tried to launch. There is no U.S. equivalent to the EU Code of Practice. We need to have an all-of-government approach to the problem with the backing of the highest levels of the administration. The following might serve as an action plan for the U.S.

The U.S. Government needs to get organized. Somebody and some agency needs to own the problem. Whether this is State, DHS, or a national counter-disinformation center with the backing of the President, somebody needs to answer the phone when you want to call about disinformation.

Mr. KEATING. Did you plan that?

Mr. FRIED. Yes, sir, I did.

Mr. KEATING. That was excellent.

Mr. FRIED. Yes.

The U.S. needs to work with its friends, starting with the European Union. We could stand up a transatlantic or G–7 counter-disinformation coalition to pool our knowledge, set common standards, and use our regulatory power to greatest impact.

Social media companies have happily moved beyond initial denial, but they need to keep cleaning up their platforms and reassessing online anonymity.

The administration and Congress should follow the principles of transparency and authenticity on social media, not heavy content control.

Regulation, I think, is coming. It needs to be iterative, not heavy. We need to learn as we go. But I think that it is important not to be heavy content control, but to talk about inauthentic sites and enforce the principles of transparency.

Last thought. Civil society groups in the United States and Europe are going to be the heroes of counter-disinformation techniques. They, not government bureaucracy, are going to be able to expose in real time Russian and other disinformation operations. We ought to put our trust in them. We ought to put some of our resources behind them, people like Jessikka Aro and Jakub Kalensky. But others, Stop Fake in the Ukraine, the Baltic elves, EU disinfo labs, the Atlantic Council's own DFR Lab, these are the people who can expose, and then when exposed, American society needs to wake up and pay attention to this.

There is more to be said, but I will say it during the questions if there is time.

[The prepared statement of Mr. Fried follows:]

Statement by Ambassador Daniel Fried (retired)
Distinguished Fellow, the Atlantic Council
Hearing on Russian Disinformation Campaigns
House Committee on Foreign Affairs
Subcommittee on Europe, Eurasia, Energy, and the Environment
July 16, 2019

Chairman Keating, Ranking Member Kinzinger, Members of the Committee, I appreciate the opportunity to appear before you today. The topic is relevant and timely.

The Putinism Problem

President Trump has noted that it would be nice if the United States got along with Russia. He's right. Both Presidents Bush and Obama tried to sustain constructive relations with Putin's Russia. They failed because Russia's conditions for good relations with the US are those that no US administration should accept: US deference to Russian domination of its neighbors, including through intimidation and war, and US indifference to Russia's repression at home.

Some in this country and in Europe might accept these Russian conditions. But hard experience in the 20th century – through two World Wars and the Cold War – show that a country's repression inside its borders indicates that it will be aggressive abroad, and that spheres of influence established through force and repression, Russia's usual methods, are neither stable nor self-limiting.

Putin's system of rule combines political authoritarianism and economic kleptocracy; it is a regime dedicated to enriching its members, not the nation it supposedly serves. Economically, it depends on control of raw materials which it can export. It is a value-extracted, not value-added, economy. Putinism thus keeps Russia relatively backward. Policies to develop Russia would require respect for the rule of law, property rights, independent institutions both in and out of government, and freedom of speech and assembly; in short, free market, democratic reforms. But such reforms would mean an end to Putinism.

As a corrupt system by design, lacking democratic legitimacy and, increasingly, economic results, the Putin regime is insecure. It thus relies on repression mixed with chauvinistic campaigns directed against various made up outside enemies. That is not all. The regime seeks to prevent its democratic rivals — what we used to call the Free World — from challenging Putin's regime by the power of their example. Putin, like Soviet leaders before him, seeks not just to weaken the European Union and NATO, he seeks to discredit the very idea of democracy as a potentially appealing alternative for Russia.

Russia's Disinformation Challenge

Russia's use of disinformation to interfere in the US presidential elections in 2016, documented in the Mueller Report and attested to by numerous intelligence community assessments, is only

one piece of a broad Russian effort to destabilize Western societies. While many Americans became aware of such Russian tactics only in 2016, many Europeans, particularly Ukrainians, Georgians Estonians, Latvians, and Lithuanians, have faced such Russian methods for years. Spain, Greece, Germany, France, and the UK have faced intense Russian disinformation campaigns more recently. Some Western Europeans who believed that Russian aggression and disinformation had nothing to do with them have discovered their error.

Russian use of hostile propaganda and what used to be called "active measures" against the West date back to the Soviet period; we've dealt with this before. As the US government's first Soviet specialist George Kennan wrote from Moscow in 1946[1], the Kremlin seeks through covert means "[t]o *undermine general political and strategic potential of major western powers. Efforts will be made in such countries to disrupt national self-confidence, to hamstring measures of national defense, to increase social and industrial unrest, to stimulate all forms of disunity…[p]oor will be set against rich, black against white, young against old, newcomers against established resident, etc.*"

In those years, the Soviets manipulated print media. On the ground, they infiltrated local groups, slowly taking them over. But such operations were "analogue." What then took many weeks or months now takes minutes.

Moscow's disinformation tactics — use of bots, state-sponsored trolls, inauthentic online accounts and false personas, and potential use of emerging AI technologies that enable "deep fakes" and more — is cutting edge. As explained in the Department of Justice Special Counsel report[2] and the investigation's related indictments from February 2018[3] and July 2018[4] against the Internet Research Agency (IRA, the St. Petersburg troll farm) and military intelligence (GRU), the Kremlin's disinformation system combines computer hackers, overt propaganda such as *RT* and *Sputnik*, covert social media presence, and skilled trolls, with assistance by enablers in the West (in my day, we called them "useful idiots").

The IRA has been funded through the Kremlin-connected businessman and operative Yevgeny Prigozhin. Prigozhin also serves as a channel for Kremlin funding of Ukrainian separatists (for which the Obama Administration sanctioned him in late 2016), the mercenary "Wagner Brigade" which has put Russian soldiers in Syria and Venezuela, and, according to press reports, various operation in Africa. This gives a sense of the priority the Kremlin places on its disinformation efforts, and how they stand as the cutting edge of its aggressive foreign policy.

---

[1] The "Long Telegram," reprinted in Kennan's "Memoirs"

[2] Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election" (U.S. Department of Justice, Washington, DC, 2019), https://www.justice.gov/storage/report.pdf.

[3] UNITED STATES OF AMERICA v. INTERNET RESEARCH AGENCY LLC A/K/A MEDIASINTEZ LLC A/K/A GLAVSET LLC A/K/A MIXINFO LLC A/K/A AZIMUT LLC A/K/A NOVINFO LLC et al. 18 U.S.C. §§ 2, 371, 1349, 1028A (2018). https://www.justice.gov/file/1035477/download.

[4] UNITED STATES OF AMERICA v. VIKTOR BORISOVICH NETYKSHO et al. 18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq. (2018). https://www.justice.gov/file/1080281/download.

These elements combine to produce what my colleague Alina Polyakova calls a concert of chaos: intelligence officers and hackers can steal e-mails and send them to friendly sites which will disseminate them; RT and Sputnik will pick up and push the stories; bots and trolls will amplify these messages. In the 2016 US elections, Russian disinformation techniques used automated bots, impersonation accounts, microtargeting tactics, and online ads.

More recent analysis suggests that disinformation techniques are shifting toward sophisticated interaction with (and manipulation of) domestic groups, extremist and otherwise, through various forms of impersonation and amplification of organic posts by domestic persons. Deceptive sites can steer initially authentic social media conversations, promoting extreme views and inflaming opinion, and sometimes even taking both sides of a divisive issue, ramping up the rancor. The IRA uses impersonation accounts to infiltrate public discourse online, often using initially non-political content and issues to build a social media audience on Facebook, Twitter, Instagram and elsewhere. Disinformation's next stage may involve "deep fakes," which are rapidly improving in technical quality, creating and disseminating falsified images faster than fact checkers can catch up.

The Russians may be leaders in state-sponsored disinformation, but they will not be the last. China, Iran, and other state and non-state actors are learning from the Russian tool-kit. The democratic community — aka the Free World — needs to face the challenge of Russian and other forms of contemporary disinformation, and to do so while remaining true to our democratic values and norms of freedom of expression. As we learned during the Cold War, we must not and need not become them to fight them.[5]

Europe Seeks Solutions[6]

For many years, European nations were divided about whether Russian disinformation constituted a significant problem. Starting in 2018, stung by repeated Russian disinformation campaigns, European opinion moved toward action. The emerging European Union policy is outlined in four documents: "Tackling Online Disinformation, a European Approach," prepared by the EU Commission and published on April 26, 2018; a voluntary "Code of Practice on Disinformation" prepared by the Commission, published on September 26, 2018 and agreed to on October 16, 2018 by Facebook, Google, Twitter, and Mozilla, as well as the European trade associations representing online platforms and the advertising industry; an EU Commission "Progress Report" published on December 5, 2018; and the "Action Plan against Disinformation" jointly prepared by the EU Commission and European External Action Service (the EU "foreign ministry") also published on December 5, 2018.

---

[5] See "Democratic Defense Against Disinformation," February 2018, The Atlantic Council, Ambassador Daniel Fried (Ret.) and Alina Polyakova. This testimony draws on this report and on Dr. Polyakova's own congressional testimony, as well as our joint appearances on this topic in Europe and the United States.

[6] For a detailed assessment of the EU response to Russian disinformation, see https://www.atlanticcouncil.org/images/publications/Democratic_Defense_Against_Disinformation_2.0.pdf

The major policy elements of the emerging EU approach include:

- **Strengthening EU capacity to identify and expose disinformation.** This includes a recommendation to double the budget for strategic communications. The EU's EastStratCom unit, based in Brussels, has a mandate to identify and expose Russian disinformation. EastStratCom's staff is dedicated and skilled but has lacked consistent political support and adequate funding. This hopefully will change.

- **Establishment of an EU Rapid Alert System (RAS) to expose disinformation in real time.** This was set up before the May EU Parliamentary elections and was intended to link each EU member state government and allow for passing of alerts about disinformation campaigns.

  The RAS was supposed to have an initial operational capacity by March 2019, two months before the EU parliamentary elections. But as "The New York Times" recently reported, the system is still not fully operational.[7] Hopefully, it will improve in effectiveness.

- **The Code of Practice on Disinformation** marks a significant step forward. Under its terms, social media companies have agreed to scrutiny of ad placements; transparency of political and issued-based advertisements; integrity of service (meaning social media companies have committed to identify and remove fake accounts, including bots); empowering consumers, a general commitment by social media companies to "help people make informed decisions"; and empowering the research community, meaning that social media companies will support research on disinformation. The Code provides for the social media companies to make monthly progress reports to the EU and notes that if progress is not satisfactory, regulation could follow.

  The progress reports issued under the Code of Practice suggest a mixed picture. Social media platforms have provided details of their efforts to take down fake accounts, restrict ad purchasing by purveyors of disinformation, identify and block inauthentic behavior, and take other steps to meet the (general) commitments outlined in the code. But the EU Commission has noted insufficient information provided by social media companies, and urged specific next steps, including calling on platforms to take more serious actions to address transparency, particularly with respect to political ads. The commission is issuing monthly progress reports to test social media companies' response to their commitments.[8]

---

[7] https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html

[8] European Commission, "Code of Practice against disinformation: Commission calls on signatories to intensify their efforts," (European Commission, Brussels, 2019), http://europa.eu/rapid/press-release_IP-19-746_en.htm; "Second monthly intermediate results of the EU Code of Practice against disinformation," (European Commission, Brussels, 2019), https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation. Latest report at time of writing: http://europa.eu/rapid/press-release_STATEMENT-19-2174_en.htm.

- **Improving social resilience against disinformation,** including creating a European network of independent fat checkers; launching a secure online platform addressing disinformation; exploring means of reliable identification of information suppliers; and support long-term social media literacy.

  It remains unclear, however, how and whether these efforts have been implemented.

Individual European national governments have also taken steps to address the disinformation challenge:[9]

- **France** has taken a lead, perhaps in reaction to Russian hacking at the end of the French Presidential election in 2017 into the Macron campaign computers and dissemination of purloined e-mails. In this case, the Russian disinformation operation was detected and exposed in real time by European and US civil society groups. The hostile French social reaction to this attempt to manipulate the elections drowned out whatever impact the Russian disinformation operation hoped to trigger. *It was an outstanding success story in the fight against Russian disinformation.*

  In March 2019, President Emmanuel Macron proposed a new "European Agency for the Protection of Democracies," which included providing each EU member state with expertise to protect election processes against cyberattacks and manipulation.[10] France has also led the "Paris Call for Trust and Security in Cyberspace," established in November 2018.[11] In relation to security of the information space, the Call includes commitments to:
  - increase prevention against and resilience in the face of malicious online activity;
  - protect the accessibility and integrity of the Internet;
  - cooperate to prevent interference in electoral processes; and
  - prevent the proliferation of malicious online programs and techniques.

  The Paris Call includes backing from 66 States, 139 international and civil society organizations, and 347 private sector entities. The US is not a signatory.

- **Sweden** has created a new "Psychological Defense" agency tasked with countering disinformation and increasing societal resilience to disinformation. The Swedish Civil Contingencies Agency (MSB), with mandate similar to the US Department of Homeland Security, has worked closely with local Swedish authorities to establish lines of communication, conduct training, and analyze potential systemic weaknesses. Ahead of the Swedish national elections last fall, the MSB mailed leaflets to households explaining

---

[9] https://www.brookings.edu/wp-content/uploads/2019/07/Alina-Polyakova-House-Appropriations-Testimony-July-10-2019.pdf

[10] Emmanuel Macron, "Renewing Europe," Project Syndicate, March 4, 2019, http://prosyn.org/kCUclh5.

[11] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

the threat of information influence and outlining how to respond.[12] Swedish schools have also received information and materials to help teach students how to identify disinformation.[13]

- The **Czech Republic, Denmark, Estonia, the Netherlands**, among others, have established a cross-agency teams tasked with coordinating governmental efforts to identify and respond to disinformation operations.

The good news is that the European Union and some individual European national governments are focused on addressing the disinformation challenge. The EU action plan, especially the Code of Conduct, is a solid start, consistent with the values of freedom of expression, that provides a set of norms and objectives to which social media companies can be held. The bad news is that EU implementation of its own plan has been uneven. This effort is only beginning.

The US Tries to Get a Grip

The United States lags behind the EU, both in conceptual framing of the issue and systemic actions to deal with it. This is not due to lack of sophistication or awareness of the problem inside the Administration. But leadership has been uneven; the USG approach to Russia-sourced disinformation appears hampered by what could be called partisan reactions to the problem. Perhaps as a result, it remains unclear who in the U.S. government owns this policy challenge.

Nevertheless, work in ongoing within the Administration:

- The **State Department's Global Engagement Center (GEC)** has been tasked with countering state-sponsored disinformation, and it has begun to fund research and development of counter-disinformation tools while supporting civil society groups and independent media on the front lines of the threat in Europe. Over time, this funding will help boost independent media and groups on the front-lines of the information war.[14]

- **US Cyber Command** began operations ahead of the 2018 congressional elections to deter Russian operatives from potential interference.[15] Cyber Command, together with the National Security Agency (NSA), reportedly developed information about Russian trolls and their activities, and alerted the FBI and Department of Homeland Security

[12] https://rib.msb.se/filer/pdf/28698.pdf

[13] Dr. Polyakova and I have worked closely with the Swedish MSB in our counter-disinformation work, and the Swedish government has sponsored our efforts.

[14] See the written testimony of Lea Gabrielle, Special Envoy and Coordinator for the GEC, before the House Appropriations Subcommittee on State, Foreign Ops, and Related Programs, July 10, 2019

[15] Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," New York Times, October 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.

(DHS).[16] The operation followed the Department of Justice indictments of Russian individuals, intelligence officers, and companies involved in the Internet Research Agency and cyber operations against the US elections.[17] Cyber Command has reportedly sent messages to specific individuals active in disinformation operations, de facto outing them and their activities. While I have no special knowledge of its intentions, the press reporting of these activities may have reflected a considered strategy.

- **USAID**, working with State (including the European Bureau) has launched a set of programs titled "Countering Malign Kremlin Influence," which include supporting local media and civil society in some of the European countries most vulnerable to Russian disinformation. The intent is to support social resilience and resistance to such campaigns.

- The **Department of the Treasury** has used existing authorities to impose sanctions on Russian entities tied to disinformation efforts, including those directed at the 2016 US presidential election. This included the sanctions designations on December 19, 2018, of entities and individuals tied to the IRA and nine GRU (military intelligence) officers. Material accompanying the Treasury Department's sanctions designations exposed details of Russian operation, including establishment of an online English-language website, "USA Really."

- *Current Time*, the Russian language television news program produced by **VOA and RFE/RL** is perhaps the US government's closest response to countering RT and other Kremlin funded outlets by providing truthful information to Russian speakers in the post-Soviet states. This effort is critical as Russian speakers have little access to Russian-language broadcasting that is not Kremlin controlled. At this time, *Current Time*, lacks the resources to compete with the production values and the reach of RT.

- The **2019 National Defense Authorization Act (NDAA)** added significant (albeit second-order) provisions on countering disinformation for US national security.[18] It cemented the role of the GEC by linking its counter-disinformation task to US national security, hopefully securing the center's longer-term funding. It also defined "malign influence" as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, business, corruption, educational, and other capabilities by hostile foreign powers to foster attitudes, behaviors, decisions, or outcomes within the United States."

---

[16] David Ignatius, "The U.S. military is quietly launching efforts to deter Russian meddling," Washington Post, February 7, 2019, https://www.washingtonpost.com/opinions/the-us-military-is-quietly-launching-efforts-to-deter-russian-meddling/2019/02/07/4de5c5fa-2b19-11e9-b2fc-721718903bfc_story.html?utm_term=.1cbbaf8bf3ae.

[17] US Department of Justice, "Internet Research Agency Indictment" (US Department of Justice, Washington, DC, 2018), https://www.justice.gov/file/1035477/download; "Indictment" (US Department of Justice, Washington, DC, 2018), https://www.justice.gov/file/1080281/download.

[18] US Government Publication Office, "National Defense Authorization Act For Fiscal Year 2019" (US Government Publication Office, Washington, DC, 2018), https://www.govinfo.gov/content/pkg/CRPT-115hrpt874/pdf/CRPT-115hrpt874.pdf.

- The Senate has reintroduced the **Defending American Security from Kremlin Aggression Act of 2019 (DASKAA)**. While mostly devoted to sanctions, DASKAA also "calls for the establishment of a National Fusion Center to Respond to Hybrid Threats, a Countering Russian Influence Fund to be used in countries vulnerable to Russian malign influence, and closer coordination with allies" (sections 704, 705, and 706). [19]

These are all laudable steps. But they lack the scope of what the EU has already tried to launch. So far, for example, there is no USG equivalent to the EU Code of Practice involving US social media companies. Moreover, these steps do not seem to be integrated into an all-of-government approach with the backing of the President.

Next Steps

The following might serve as a US action plan:

- The **US government** needs to ***get organized*** to contend with Russian and other disinformation. DHS, FBI, and the State Department (especially the Global Engagement Center) have expertise and mandates of different kinds. The USG needs to designate a lead agency and a senior official to own the problem, and perhaps stand up an interagency body such as a **national counter-disinformation center** (which could act as a rapid alert system, hopefully in concert with the emerging European RAS). Those responsible for counter-disinformation policy need to have the explicit, unambiguous backing of the President and the White House. Mixed messages will not do.

- The **USG needs to work with its friends**, starting with the European Union and key member states. A best-case initiative could include standing up a ***"counter-disinformation coalition"*** of like-minded governments and including social media companies and civil society groups. The Coalition's purpose would be to pool knowledge, including in real time; and set common approaches, including regulatory standards as needed. The US could join the Code of Practice, formally if possible or otherwise, or help negotiate a broader such Code, possibly in a G7 context. The point is to combine standards and pool leverage, including with social media companies to encourage their diligence in addressing disinformation.

- ***Social media companies*** have moved beyond their initial denial of the problem, but need to keep cleaning up their platforms, including by establishing common transparency standards to deal with suspicious accounts or deceptive sites, and reassessing online anonymity. We have learned that "Angry Bob from Boise" may in fact be Ivan from the St. Petersburg troll farm (the Internet Research Agency) and we may not want to permit deception of this sort. Social media companies need to address the problem of algorithmic bias toward extremism. But because this may challenge their established business model, it may require regulation applied evenly to all social media companies to get them to move. We ought not have our

[19] US Congress, Senate, *Defending American Security from Kremlin Aggression Act of 2019*, S 482, 116th Congress, 1st session, introduced in Senate February 13, 2019, https://www.congress.gov/116/bills/s482/BILLS-116s482is.pdf.

social media companies acting as unwitting research arms or enablers for Russian intelligence.

- ***The Administration and Congress*** should follow the principles of ***transparency and authenticity*** on social media, not heavy content control. That means, for example, requiring full disclosure of the funders of political and issue ads, pressing social media companies to remove inauthentic accounts, mandating standard definitions of impersonator and inauthentic accounts across social media companies, and exploring ways to deal with the algorithmic bias toward sensational content, which leads social media users to extremism.

- ***Regulation of social media*** should be an iterative process rather an effort at a one-time act. We need to learn as we go. Congress and the Administration should start with low-hanging fruit and proceed with care to greater challenges. Recommendations include:
    - ***Regulation of advertisement and sponsored content,*** among the easier challenges (though not "easy"), as precedent exists for limits on commercial speech. The Honest Ads Act is one such example. Social media companies can be required to post accurate information about ad sponsors, rather than euphemistic or misleading self-descriptions.
    - ***Mandatory identification of bots*** under certain conditions (e.g., if disguised as persons, following the principle of transparency).
    - ***Regulatory mandates to disclose or remove inauthentic foreign accounts or impersonators.*** These raise issues of definition and the principle of on-line anonymity, but should be principal elements of a regulatory regime. Using a pseudonym online may be legitimate, but deceptive identification could be part of a disinformation operation, and there may be ways to address this challenge.
    - ***Mandating standard terms of service,*** including common definitions of impersonator and inauthentic accounts, and standards for removing bots.
    - ***Algorithmic bias*** if related to content would be among the most controversial and difficult regulatory issues (what would a "fairness doctrine" look like when applied to social media?). However, targeted fixes addressing behavior or provenance (e.g., RT, Sputnik) and involving de-ranking may be worth exploring.

- ***Civil society groups*** in Europe and the United States could be the heroes of counter-disinformation. Groups such as the Atlantic Council's Digital Forensic Research Lab or the Baltic Elves, Ukraine's Stop Fake, or EU DisinfoLab and others have proven themselves adept at exposing Russian disinformation campaigns, e.g., Russian hacking into the 2017 French elections and Russian lies about its 2014 shootdown of a Malaysian airline over Ukraine. Civil society activists — bot hunters, troll spotters, and digital Sherlocks — may be far more capable than most governments, and their work can be made public fast. They are natural partners and should be supported and brought into discussions of solutions.

Fighting disinformation *can work, but long-term social resilience will work best.* There will be no complete solution, no set of policies which can eliminate disinformation. But this need not be our objective. Actions by democratic governments, social media companies, and civil society can circumscribe and constrict disinformation. Doing so starting now can give time for democratic societies to develop greater sophistication at recognizing disinformation. Teaching everyone — from civil servants to children — how to spot disinformation ought to be standard practice as much as public health classes.

Lead and help fix the Free World

I want to end with a larger thought: a strong Russia policy – with counter-disinformation efforts one of its elements -- should be linked to an American Grand Strategy, which recognizes that a rules-based world that favors freedom is in the United States' national interest. At our best, we have recognized that our interests and our values advance together or not at all. The United States was different from previous great powers, exceptional, if you will, because we understood that our nation would do well when, and only when, other nations also did well. We were not interested in merely guarding a sphere of influence, like great powers of the past. Instead, in a breathtaking display of confidence and vision, we understood that we could make the world a better place and do well for ourselves in the process.

Putin, and likeminded nationalists and despots, stand instead for nothing more than power. We saw the results of such thinking in the first half of the 20th century. The United States can do better. In fact, when the United States' time to lead came in 1945 and again after 1989, we did do better. And so did the world. Despite our mistakes, inconsistencies, and downright blunders, the United States' leadership in the world has generated the longest period of general great power peace in human history, alongside unprecedented global prosperity.

Past success gives us no basis for complacency. Our current problems are severe, some of our own making.

But at the end of our current national debate about the United States' purposes in the world, I hope and believe that we will recall the values and purposes which have propelled America's world leadership and produced so much good for so many.

Mr. KEATING. Thank you, Ambassador.
Ms. ARO.

STATEMENT OF JESSIKKA ARO, INVESTIGATIVE REPORTER, YLE KIOSKI

Ms. ARO. Chairman Keating, Ranking Member Kinzinger, distinguished members of the committee, thank you so much. Thank you for having me here. It is such an honor to discuss the Russian trolls and how to counter them and prevent them from causing any more international damage in the future. I will tell you what I have found out in my investigations as well as give you recommendations how to prevent the damage in the future.

Five years ago, I started to investigate the Kremlin tool of information psychological warfare, Russia's use of paid online propaganda workers. Thanks to the brave Russian journalists who had infiltrated the St. Petersburg-based troll factory already in 2013, we knew that a shady office paid people to build fake identities and profiles on social media.

These trolls pretend online as real people and produce pro-Putin and pro-Russian content on an industrial scale. According to leaked emails between the factory supervisors and employees, the trolls' mission was to shift the balance of online discussions by increasing comments supportive to Putin, thus manipulating real people online.

Back then, in 2014, the Russian trolls in Finland attacked mostly opinion leaders, for example, our then defense minister. I wanted to investigate how the trolls influence and impact in the general audience, the ordinary internet users. Did they have any meaningful impact or influence on them, on Finnish real people's ideas, attitudes, and even behavior.

I found several influence methods which are still actively in use by the trolls today. Facebook, Twitter, YouTube, every other social media comment sections of traditional media and Russian discussion forums were abused already back then to spread lies benefiting the Kremlin. The trolls smeared Western leaders as Nazis and fascists, blamed the U.S., NATO, and the European Union for the war in Ukraine, claimed Russian soldiers never stepped their foot on Ukrainian soil.

The Russian Embassy in Helsinki supported these social media operations. In addition, anonymous operators formed groups on Facebook and conducted other psychological operations against civilians.

The trolls, indeed, had impact on real Finnish people. Some Finnish who are interviewed told me that they had stopped discussing Russia-related issues online altogether just to avoid the death threats and name calling that would follow from the trolls after they did that. Thus, the digital operations had succeeded in both silencing and importing fear into Finnish public debate about Russia. That is a profound threat to people's freedom of speech coming from a hostile foreign power.

But there was more. Some people had lost the idea of what is true and what is not. For example, in the case of Ukraine, disinformation had again succeeded in manipulating real people's thoughts. It is difficult to make decisions who to vote for or wheth-

er to view Russia as the aggressor in Ukraine or not after you are not sure what is factually even happening.

Russia wants to brainwash useful idiots. My most disturbing finding, in my own opinion, was that some people who are subjected to propaganda believe it and spread it further in their own networks. I also learned that not everyone are influenced, but some people are and they need protection.

Later, I started to investigate attacks on private Western individuals as I was myself made the target of Russian-originating and still ongoing defamation campaign because of my work. For almost 5 years, I have been defamed in Russian fake new sites, in Finnish pro-Kremlin racist and hate speech fake news sites by the German RT, by the troll factory, and by countless social media activists and neo-Nazis.

The retaliation campaign against me is partly criminal in nature. It has impacted even some of my friends and has led to some of the agitated people threatening to kill me. These are real Finnish individuals.

I needed police escort to attend a trial against some of these perpetrators. Police said that I faced the threat of impulsive violence if I am in the wrong place at the wrong time. Why? Because Putin's administration's employee and other propagandists want to smear and silence me and scare and stop me from investigating and talking about the troll activity.

And I am also somewhat worried to testify here today because I believe it will lead to retaliation against me just like so many other of my public appearances in the last years.

Also, the same kinds of operations are ongoing against different European and even American people who voice out their criticism or information about Russia or Putin's regime. They become systematically smeared.

And finally, I recommend the Western governments and international police organizations who, in my view, are in the core of countering this international disinformation campaign, they should be treated as what they are, international politically motivated organized crime conducted by intelligence officers and paid propagandists. These criminals, they do not want to take your money. They want to capture your thinking and control you.

Targeted people are often civilians. They need help. More robust preventive measures from intelligence services are needed.

Also, maybe it is time we start to call the Kremlin troll farms and digital disinformation for what they are, crime factories and digital crime. The word troll farm does not come close to describing the destruction of these operations.

Countries should also check their legislations on libel, illegal threats, instigating violence, secrecy crimes, privacy breaches, espionage, and computer hacks as they seem to be the Kremlin's favorite online violations used in these operations. The punishments for these crimes are often not enough to prevent this organized crime.

The Kremlin also knows that as long as Facebook, Twitter, and other social media giants are not properly regulated, they can abuse them as much as they can.

And just my most important notion today is that the Kremlin's operations continue uninterrupted all the time between and during

the elections. The trolls are given new themes every day, and they will continue unless they are stopped.

Thank you.

[The prepared statement of Ms. Aro follows:]

Testimony for the United States House of Representatives

Committee on Foreign Affairs

Subcommittee on Europe, Energy, and the Environment

16th July 2019

"Russian Disinformation Attacks on Elections: Lessons from Europe"

Jessikka Aro

Investigative Journalist

Finnish Broadcasting Company Yle, Kioski

Helsinki, Finland

European Union

***

INTRODUCTION

Chairman Keating, Ranking Member Kinzinger and distinguished members of the committee, thank you for this opportunity to testify before you today on the subject of the Kremlin's Disinformation Attacks on Elections: Lessons from Europe.

My most important notion today is, that Kremlin's disinformation operations continue uninterrupted between the elections and are targeted to many other institutions. Obviously, special operations are targeted to influence the outcome of individual elections, too, other politically important developments around Europe are targeted too. Some of those long-term information operations bear fruit in elections, too.

Moreover, I want to point out, that Kremlin's used of disinformation, fake news, trolls and influence agents don't **only** threaten our democracies, or citizens' freedom of speech or the rule of law in general, but pose a **critical threat** to national security in the targeted countries. And the issue is urgent, because the Kremlin targets many countries simultaneously. Often times we even learn about different operations only after they've already hit their target.

Instead, we should be able to pre-empt the impact of the Kremlin's disinformation attacks before they take place in our information space and reach our citizens. Basically, Western governments need unified efforts and a strategy to update their legislations and the implementation of their existing laws and international legal instruments to be able to expose and counter the Kremlin's global-scale hoaxes and crimes in the information space. This needs to be done timely and effectively.

The damage by social media trolls and viral fakes take effect quickly. After launching a fake news article in the St. Petersburg troll factory, it may take only a few seconds to cross international borders in the cyber space and land at the reader's, the targeted person's consciusness.

At the moment to my knowledge there is no international organized body investigating systematically all ongoing Kremlin's disinformation operations and sending warnings about them.

There should be, and quickly. Nowadays, too often the operations are discovered when fixing the consequences of the operations is already impossible. For example, canceling the end result of a presidential election heavily influenced by Russian trolls, hacks, intel operations and propaganda combined.

***

I'm a journalist specialized in Russia, extremism and information warfare. I have lived in Russia, studied in the most precious state university in Moscow and worked as a journalist in Russia. I have reported about Russia and former Soviet Union region to Finnish media outlets since 2005.

I started to investigate the impact and techniques of the Russian social media trolls in 2014. Next Setember I will publish a non-fiction investigative book about Kremlin's international and often criminal attacks against those Western individuals, who the Kremlin has labeled as their enemies or at least counterproductive to their own political goals.

This testimony is largely based on my own journalistic research, findings included in my upcoming book, but it also refers to research by other journalists, authors and scholars.

KREMLIN'S INTERNATIONAL DISINFORMATION NETWORK

Russian president Vladimir Putin's regime conducts information-psychological warfare against Russian citizens, and against citizens of foreign countries.

Kremlin's operations on social media have succeeded in influencing part of the population and have the ability to misguide that population's decisionmaking. With digital disinformation Kremlin wants to dictate, which electoral candidates the targeted populations vote and which policies they support. The Kremlin often fuels discussions over divisive topics such as immigration, the economic sanctions against Russia as well as individual countries' memberships in the NATO and the European Union. Kremlin's propaganda often attacks individual European countries and depicts the European Union as weak failed.

Kremlin's security structures have manufactured multi-faceted digital disinformation networks in the cyber space. These networks consist of Russian multilingual troll and propaganda factories and Russian state-controlled media outlets & news agencies, such as Kremlin's international "weapon of information warfare RT, former Russia Today" and Sputnik "news agency". The global network also employs Russian intelligence officers and local proxies, such as paid foreign citizens working - sometimes overtly, sometimes covertly - as professional propaganda spreaders and community builders in both physical surroundings and online, extending Putin's regimes interestest far beyond Russia's state borders.

The network also includes an unknown amount of proxy fake news sites, which pretend as homegrown and local, but receive either workforce, ideological, political or hidden financial support, for example through crypto currencies, from Kremlin-connected and Kremlin-minded actors.

Many operators on the highest ladders of the Kremlin's disinformation network have several different tasks: they run fake citizen organizations abroad, produce articles with fake names to pro-Kremlin disinformation outlets and/or operate as "election observers" in Kremlin-influenced elections, helping to rig the real votes. Some of these operators run "inofficial pro-Kremlin troll farms" on social media, and get to do it with impunity, as they are not directly connected to any Russian state structures and claim to only "use their freedom of speech".

Yet another layer of the Kremlin's global disinformation network consists of local "useful idiots". Usually these individuals might not even know, that they're serving Kremlin's interestest. They might for example provide hosting services to pro-Kremlin fake news online sites or write filth articles to those same sites completely unaware, that the site is lead by Kremlin's disinfo architects.

Sometimes Kremlin's security services succumb people as their propagandists by promising them support in upcoming elections or "interesting speaking opportunities" in Russian universities. Some of the local, recruited propaganda spreaders might be blackmailed, some bribed.

Yet another layer of Kremlin's disinformation spreaders consists of individuals, who have previous criminal background and take personal pride in participating in anti-social and anti-government fake news operations. Some of the spreaders represent political extremes, and in one way or another benefit from Kremlin's direct or indirect support to their ideology, such as neo-nazism, ultra-nationalism or right-wing populism. Some active spreaders or pro-Kremlin conspiracy theories are eccentrics, who feel drawn to all sorts of conspiracy theories, as long as they offer quick answers to complex global issues.

Kremlin has a variety of different themes and angles which it pushes aggressively and lavishly to its global disinformation network. To name a few themes, it wants to blur for example different audiences' perception concerning Russia's war in Ukraine (according to the Kremlin such war doesn't exist), as well as the well-investigated and proven downing of the flight MH17 by Russian-backed militants in the occupied territories of Eastern Ukraine in 2014 (Kremlin denies any involvement).

In addition, Kremlin's disinformation attacks aim at heavily eroding the target populations' trust towards named traditional journalists, individual Western-minded politicians, human rights activists, think-tankers, scholars, diplomats and government officials. Sometimes the Kremlin's plots against named individuals last years, in some cases over a decade.

SOCIAL MEDIA PAID PROPAGANDISTS MANIPULATE REAL PEOPLE

In 2014 I started to investigate the techniques of the then-newly exposed tool of Kremlin's international information warfare, the troll factory St. Petersburg, exposed already in 2013 by courageous independent Russian journalists.

The "trolls" are paid online propagandists who pretend as genuine Russian, American, British, Finnish and other countries' citizens on different social media platforms. Their task is to build social media profiles and use them to inflitrate local communities, and act practically as digital influence agents. The trolls abuse the target population's trust towards strangers in cyber sphere. As personal communication is known as the most influential form of communication, targeted

populations are more prone to believe messages originating from a "Facebook friend" than the message from, for example, an anonymous article published by Russian fake news agency.

On the course of my initial investigations, I specifically wanted to find out, how the aggressive pro-Kremlin social media fake and anonymous troll profiles **influence internationally** in real peoples' ideas, attitudes or possibly behavior. I conducted my investigation through crowdsourcing, with open questions.

With the help of the Finnish internet users, many interviewed online forum moderators and experts, I found out, that already back in 2014-2015 the Russian social media trolls, ultimately fake profiles, used multiple techniques and channels targeted specifically at manipulating international audiences.

Already in 2014 the pro-Kremlin trolls were already systematically spreading propaganda in several different languages, on Twitter, Facebook, YouTube, the comment sections of traditional medias in the US, UK and Finland. The social media propagandists conveyed their messages through social media comments, posts, groups, memes and videos, as well as bot armies on Twitter which spit out the same fakes simultaneously.

They also spread the Russian regime-controlled media's fake news stories and falsifications to wider and more international audiences. Me and my colleagues found out in February 2015, that the St. Petersburg troll factory produced political fake news in English, around the clock. In addition, the troll factory security guard slipped important information to us: the factory was indeed a state security structure - an "administrative building", as the guard put it himself.

In addition I learned and reported, that the aggressive, fake and anonymous social media profiles had already impacted and manipulated real people internationally: both regular internet users' ideas, and actions to certain extent. Some of my interviewees told, that they couldn't separate the facts and fiction for example concerning the war in Ukraine, because the internet was full of fake troll stories about the causes and the situation of the Ukrainian war. The digital disinformers had distanced Kremlin's part from the war in Ukraine, accused the European union, US and Nato of waging the war in Ukraine, smeared the European leaders as nazis and fascists - all false claims

similar to the ones spread by Russia's regime throughout international news network. As some of my interviewees had lost the idea over what really happening in Ukraine, the paid online pro-Kremlin propaganda operators had succeeded in manipulating real people.

During my investigation some or my interviewees told me, that they had stopped Russia-related commenting online completely, because the trolls had threatened and name-called them. Thus, the digital disinformation spreaders has managed to silence Finnish citizens and thus removed moderate and critical views from the public sphere.

Thus, by confusing genuine citizens' minds, the trolls had succeeded spinning the public debates as well as suffocated Finnish people's freedom of speech in a manner, that ultimately benefitted the Kremlin. Naturally, part of the interviewees told, that they had not been influenced by social media propaganda. But my investigations and later research by other journalists, researchers and intelligence services have proved, that the Russian trolls have attacked many other populations and continue to do so. Thus, those populations need protection.

CONSEQUENCES OF MY INVESTIGATION

Kremlin's information warfare, the use of trolls, influence agents, bot networks or fake news don't only threaten people's right to receive information and form well-informed decisions based on facts. Kremlin uses social media propaganda is systematically used to agitate real people into hateful actions, by manipulating their feelings of fear and hatred. In Russia disinformation against Ukraine is being used to motivate and mobilize the Russian young men to enlist the armed forces to fight the propagated "Ukrainian fascists". Thus digital disinformation threatens directly the targeted countries' national security, not just individual elections.

The information warfare also poses severe security threats to individual people, such as myself. As soon as I started my troll impact investigations September 2014, I became a still ongoing criminal defamation campaign originating from Russia and later continuing aggressively at the Finnish language pro-Kremlin fake news sites. Recently, I have been smeared by one Russian news agency, a variety of Russian social media operators and by the Russian troll factory's fake news site. In addition, documents allegedly including my name have been hacked from a British think-tank and

spread around in Russian state media and later in Finnish disinformation media, further smearing me. A couple of months ago someone conducted an identity theft and used my name to send sexually harassing post cards, including hints of assassinations to a company based in UK.

According to the Finnish police's threat assessment, I face the threat of impulsive violence, if I'm in the wrong place the wrong time. The physical security threat against myself originates from the hate campaign, through which I'm even today smeared as a Nato and CIA employee, worker of a Western propaganda factory, conducting information warfare against Finland, being a drug dealer, braindamaged, criminal, liar, threat to Finnish national security etc. Unknown people believe these writings and are agitated into hatred against me. Some of them send me death threats. A year ago in my first trial against the main perpetrators, I had to be escorted by the police to the court.

The criminal proceedings are ongoing, and my attempts to seek justice have been revenged in a mafia-like manner, and during the trial I was made target of more threats. The court convictions haven't stopped the character assassination: countless of more suspected illegal social media blogs and comments have been used to smear me after the convictions last October. Some of the harassers follow me on public and post information about my whereabouts to social media. I have been forced to moved away from my home country Finland to escape the "crowsourced stalking", which the judges depicted as "out-of-control".

According to my book investigations, Kremlin's social media trolls and influence agents carry out similar aggressive attacks in an organized manner against journalists, opposition politicians, diplomats, scholars and anyone, who sheads light to Kremlin's activities - even outside Russia's borders. Often the systematic nature and severity of the campaigns resemble cross-border organized crime.

The attacks against Western journalists and human rights promoters are similar as the ones that have been targeted and conducted inside Russia against Russian individual journalists for almost two decades.

LESSONS LEARNED IN EUROPE

After my initial investigation 2014-2015, many US, independent Russian journalists as well as other international journalists and researchers have uncovered Russian troll and fake news operation around the US and Europe.

According to many different journalists and researchers, Russian trolls have promoted UK's exit from the European union, Catalonia's independence from Spain, fueled violent conflicts in Catalonia by spreading fake images on social media, fueled clashes in France during the Yellow vest protests, spread massive amounts of Russian state media's propaganda of many different European countries, tried attacking France's presidential election 2016 with the help of email hacks, attacked against a UK-based think tank investigating Russian influence and many more.

In Europe pro-Kremlin operators often promote xenophobia and all-out racism, spread conspiracy-theories and hate speech, agitate people into thinking "all asylum seekers are criminals", dehumanize muslims, jews, members of the lgbti communities, promote misogynia, and smear people, who promote liberal, pro-democratic values. In addition, they try to rewrite not just the present world events, also the history on many different comment section online.

One of the most important lessons learned is, that the Kremlin doesn't only attack specific elections, such as the US presidential elections 2016. It attacks all the time, between, before, after and during elections in many countries and language areas. If the Kremlin's information warfare architects cannot get the result they desires the most, at least it will try and destroy people's trust in the traditional journalistic media, decent politicians, the integrity of the elections and government officials. Kremlin conducts a variety of ongoing operations and projects internationally, some of them more successfully than the others.

HOW TO COUNTER THIS?

Kremlin will continue its operations as long as it is let to continue. That's why combined international effort is required to counter the inethical and partly illegal meddling.

US-based global companies Facebook, Twitter and YouTube enable Russia's state-sponsored propaganda spreading. After the Russian trolls attacked the US presidential elections, the

platforms were demanded to take action and they introduced new policies in removing hateful and fake content. But they're still not doing nearly enough.

Still today, many citizens don't know, that the "information" on their Facebook or Twitter feed can be implanted by Russia's security structures. Facebook and Twitter are still nowhere near transparent enough concerning the Russian activities,which they should be.

More importantly, the users of Facebook, Twitter and YouTube are not safe and secured, even though as the customers and users of the platforms they are entitled to protection. Many of the users of these platforms are children browsing the platforms' content without any parental advisory. Thus, the lawmakers need to quickly impose stricter guidelaines and sanctions. The European Commission has already forced the social media companies to remove the hate speech in 24 hours after their posting, but in some language areas they're still not removed - even though it's illegal.

The social media companies' argumentation defending their inactivity in removing hateful troll content is in line with the Kremlin's as well as many far-right activists': "taking down hate speech would breach citizen's freedom of speech". The pro-Kremlin hate agitators used the argumentation in Helsinki district court a year ago, but the judges took a clear standing: hateful writings simply aren't protected by freedom of speech. In addition, anonymous fake profiles don't have freedom of speech or any other human rights.

Both Europe and the US are still lacking the robust government actions such as investigations and counter-intelligence into Russian information warfare activities. The Mueller investigations here in the US are still the most comprehensible and in-depth investigation into the combined intelligence and troll factory operations. Similar investigations should be done internationally, in co-operation with international and national law enforcement bodies.

From my point of view as a journalist, more awareness raising and public information about the threats of Kremlin's disinformation and their impact in real people is needed. In practice that means supporting investigative journalists, researchers and other organizations bringing the operations to daylight.

FINALLY

Russian security services have planned and planted international fake information and fake news campaigns for decades. For the Russian security structures fake information campaigns are a cheap, but efficient method to wage war against the West. The modern social media sphere magnifies those campaigns' effect and impact.

One former Putin's regime's insider and Putin's former economical advisor once told me, that the Kremlin has political reasons to conduct its information warfare, for example seeking acceptance to its warfare in Ukraine. But there's another reason, Andrei Illarionov told: Russia want's to show might, just like a village bandit.

It cannot be stressed enough, that the first victims of Vladimir Putin's regime have been the ordinary Russians. Their minds are taken hostage by the government, who has succumbed the independent journalistic medias as the regime's megaphone. The apathy and disillusionment in Russia are further fed by politicized justice system, systematic corruption and the impunity of the killings of critical journalists, human right activists and opposition figures.

Us lucky foreigners still have many of the freedoms that have already been robbed from the Russian people. But Putin's regime's global machine of information warfare extends abroad and will suffocates those freedoms, if it's not strictly confronted by the same Western democratic governments - the same ones, which Kremlin so eagerly would like to see fail.

While finding ways to protect ourselves, we should find the ways to protect the Russian citizens, too.

Mr. KEATING. Mr. Kalensky.

STATEMENT OF JAKUB KALENSKY, SENIOR FELLOW, EURASIA CENTER, ATLANTIC COUNCIL

Mr. KALENSKY. Chairman Keating, Ranking Member Kinzinger, distinguished members of the subcommittee, thank you very much for the invitation to speak in front of you today. It is an honor. I will summarize my written testimony for the hearing.

In 2014, NATO's military commander, Philip Breedlove, called the Kremlin's disinformation campaign targeting Ukraine the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare.

Five years later, it is obvious that the initial blitzkrieg has evolved into a sustained and ongoing disinformation campaign using thousands of channels and dozens of languages, targeting hundreds of millions of people on a daily basis. It is a campaign with the goal to undermine Western democracies, human rights, and rule of law, and to denigrate those who stand for these values, including the United States.

The Kremlin's media are tasked to advance Russian military goals regardless of the current peace-war status with a given country. These pseudo-journalists are dutifully fulfilling those tasks, and they get rewarded by the Kremlin for the more visible Russian military operations like in Ukraine or in Syria. They perceive themselves as being in a permanent information war with the whole Western world.

The messages of Russian State media get further amplified by an ecosystem consisting of so-called alternative media, social media, Russian officials and representatives, NGO's, and other less researched communication channels. Often, influencers in European States are repeating the messages of the Kremlin's disinformation ecosystem, giving their messages new legitimacy and spreading it among new audiences.

Even in the Netherlands, the country that lost the most citizens in the tragedy of the MH 17 flight where nearly 300 civilians were killed by a Russian weapon, even in the Netherlands you can find politicians repeating the Kremlin's lies about who is to blame.

As some of the opinion polls show us, the synergy of Kremlin-controlled and Kremlin-influenced channels is effective. According to one poll, 80 percent of Bulgarians did not believe that it was Russian secret services who are to blame for the nerve agent attack in Salisbury, England. That is four out of five people believing a disinformation campaign instead of facts and evidence.

After 5 years of sustained information aggression, it unfortunately seems that the European audiences are getting used to a certain level of disinformation campaign, almost perceiving it as the new normal. This fatigue facilities further disinformation campaigns, including those from new actors, both State and non-State.

It is for these reasons why I worry that the Kremlin is currently winning the information war it is conducting against the Western democracies, mostly because we in the West do not understand that we are in such a war. We do not understand what it has already cost us and what will it cost us in the future. And we have

failed to fight back and defend our values against this new kind of aggressor.

It does not have to be this way. We in the West have all the knowledge and all the capabilities to win this fight. The only thing we lack is political will and the determination of our adversary.

In my written testimony, I have described multiple measures that can be undertaken to defend against this kind of aggression. Out of all the examples, let me highlight here the case of Lithuania. This small nation shows us how the combination of documenting this threat, raising the level of awareness about it, mitigating the weaknesses of the information space, and punishing of the information aggressors can result in a successful defense even against an opponent who is many times stronger and has many times more resources. Lithuania has a track record of neutralizing a disinformation campaign even before it has time to spread and influence the audiences, which is the best possible result you can achieve.

It is these four areas of defense which I perceive as necessary in order to successfully defend against the massive disinformation campaigns that the Kremlin conducts in the past years. What we see in many European countries and in the EU are the first three of these areas: documenting the threat, raising awareness, and mitigating the weaknesses.

However, it is actually the fourth area, punishing the information aggressors, that might make the biggest difference. The other three areas will help us better cope with information aggression, but they will never help stop it.

I am deeply convinced that unless we start punishing the information aggressors in a more resolute way, we will not only fail to stop their aggression, but we will also show to other potential aggressors that we in the West are not capable of dealing with this kind of threat, and we will invite further aggression.

And there are other, more powerful actors in the world than Russia. If they start adopting the Kremlin's tactics, as we already see happening in a few cases, we might face a significantly bigger problem in the future.

Thank you very much for your attention, and I will be looking forward to your questions.

[The prepared statement of Mr. Kalensky follows:]

Atlantic Council
EURASIA CENTER

Foreign Affairs Subcommittee on Europe, Eurasia, Energy, and the Environment

"Russian Disinformation Attacks on Elections: Lessons from Europe"

July 16, 2019

Testimony by Jakub Kalenský, Senior Fellow at the Atlantic Council

Dear Chairman Keating, Ranking Member Kinzinger, Distinguished Members of the Subcommittee, thank you for the invitation to speak in front of you today, it is an honour.

I will try to describe what is the threat posed by the Kremlin's disinformation campaigns in Europe with regard to influencing electoral processes, as well as the various solutions which have been undertaken to counter this threat. Let me state at the beginning that the image I will portray might sometimes look somewhat pessimistic. However, I firmly believe that the West, both Europe and the United States, has all the necessary tools and capabilities to successfully counter this threat. We in Europe just need to do much more, be much more robust, and much more determined in order to defend ourselves against the information aggression that the current regime in Moscow is conducting, and it is my sincere hope that through my testimony here today, I can contribute to ensuring that the United States does not repeat Europe's mistakes.

Currently, I find the European response insufficient, and my fear is that because of this, the organizers of the disinformation campaigns are winning. In other words, the Western world is currently losing the information war that the Kremlin is waging, mostly because we in the West do not realize we are indeed in such a war, what this war has already cost us and what will it cost us in the future, and that we need to fight back to defend our values against an aggressor that is trying to undermine us.

I will try to describe why and against which threats we need to defend, and how it might be done.

The infrastructure of the disinformation ecosystem

The massive export of Kremlin disinformation began approximately with Russia's invasion of Ukraine.[1] There had been disinformation campaigns focused on audiences inside Russia before; and there had been some isolated disinformation incidents targeted outside of Russia; but the massive export of the Kremlin's disinformation beyond Russia's borders, in dozens of languages, using hundreds and thousands of channels, this "most amazing information warfare blitzkrieg we have ever seen in the history of information warfare," to quote NATO's top military commander General Philip Breedlove;[2] that is new since 2014 and Russia's annexation of Crimea and military aggression in eastern Ukraine. It has been ongoing since that moment, every day. Thus, the initial blitzkrieg has evolved into a sustained campaign of long-term aggression.

The confrontational approach in which information aggression is used, regardless of the peace-war status, is codified in many official documents of the Russian Federation.[3] Theoretical articles by Russian military leadership,[4] which discuss "leaking false data" and "destabilizing

[1] https://disinfoportal.org/euelections2019-the-danger-of-ignoring-disinformations-long-term-goals/

[2] https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464

[3] http://www.ndc.nato.int/news/news.php?icode=995, and https://www.osw.waw.pl/en/publikacje/osw-studies/2016-06-27/russias-armed-forces-information-war-front-strategic-documents

[4] https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf

propaganda" as parts of their toolkit, also help to enshrine information aggression in Russia's geopolitical strategy.

This attitude is publicly pushed by the very top echelons of the Kremlin. Vladimir Putin's spokesperson, Dmitry Peskov, stated on Russian TV, "we are in a state of an information war. (...) First of all with the Anglo-Saxons."[5]

The pseudo-journalists dutifully serving the regime go along with this agenda. Margarita Simonyan, the head of *the Russia Today* (RT) TV channel, describes her network as an "information weapon," a parallel to the Ministry of Defense.[6] The Kremlin's chief propagandist Dmitry Kiselyov (in 2019, still the only Russian pseudo-journalist on the EU's sanctions list) has been even more explicit: "Today, it is much more costly to kill one enemy soldier than during World War II, World War I, or in the Middle Ages. (...) [But] if you can persuade a person, you don't need to kill him."[7] Russia is probably the only country in the world where the regime's "journalists" justify their job as a less costly alternative to killing people.

Their subordinates follow these instructions and, day after day, keep spreading lies.[8] No matter how many facts are presented about the Russian invasion of Ukraine; Russian war crimes in Syria; the murder of nearly three hundred civilians on flight MH17 by Russian-made and Russian-operated weapons; Russian assassinations in Europe, like the one in Salisbury, England; state-sponsored doping in sports events; the Kremlin's information operations and cyberattacks targeting elections all around the globe; or any other event that is of importance to the Kremlin, its disinformation ecosystem will continue lying, misleading audiences, and spreading disinformation stories and false counter-accusations.

And the Kremlin rewards these lies. Three hundred pseudo-journalists who were spreading false stories that there are no Russian troops in Crimea, and thus weakened and slowed down the Western reaction and, in effect, facilitated the annexation of the peninsula, received medals from President Putin for their "objective" coverage.[9] Sixty Russian journalists received military awards for participating in the war in Syria.[10] The Kremlin sees these "journalists" as part of the rank and file of its military.

The messages spread by the outlets directly controlled by the Kremlin are spread into other languages via local language versions of *RT* and *Sputnik*. These messages then merge into a much larger ecosystem consisting of various "alternative" media, which hide their affiliation to the Kremlin and pretend to be totally independent; in fact, they frequently parrot the same lies broadcast by Russian state media.[11] Most recently, the Slovakian intelligence service identified the so-called alternative media as the most important tool for delivering propaganda campaigns that undermine the EU and NATO, spreading mistrust about official sources of information, and

[5] https://www.youtube.com/watch?v=YXcajJVddwE&fbclid=IwAR1K_YW6Fv5X4chJowSw8Rj9fU9jWgeyNqsgTCfSvSyUdfSBvujGeS5ZRAc

[6] https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88

[7] https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html?_r=0

[8] See e.g. the database of disinformation stories by the EU's East StratCom Task Force https://euvsdisinfo.eu/disinfo-review/

[9] https://www.rferl.org/a/putin-awards-journalists-objective-crimea-coverage/25373844.html

[10] https://web.archive.org/web/20160418144138/https:/www.kp.ru/daily/26518.7/3534589/

[11] See e.g. the articles in the section "How non-Kremlin actors multiply Kremlin's disinformation" in the EUvsDisinfo Reading List: https://euvsdisinfo.eu/reading-list/mechanisms/

exacerbating divisions in their society.[12] This is a pattern that can be observed in many other European countries.

This synergy between the Kremlin-controlled and Kremlin-influenced ecosystem is further amplified by well-organized operations on social media,[13] by official Russian representatives, and unfortunately also by non-Russian actors that advance the Kremlin's interests, either intentionally or unwittingly. These can be politicians, academics, journalists, or other influencers who spread Kremlin-originating disinformation for various reasons, including corruption, ignorance, or the simple need to attract attention or challenge authority. Several recent reports indicate that Russian disinformation operatives are now increasingly focusing on domestic actors who would spread Kremlin-originated disinformation for them, thereby laundering the information and blurring its source.[14]

To give an example, reporting about the Ukrainian presidential election that took place in April, the New York Times wrote: "Unlike the 2016 interference in the United States, which centered on fake Facebook pages created by Russians in faraway St. Petersburg, the operation in Ukraine this year had a clever twist. It tried to circumvent Facebook's new safeguards by paying Ukrainian citizens to give a Russian agent access to their personal pages."[15] It is the same tactic that the Soviets used during the legendary Operation Infektion, when they planted the disinformation that AIDS had been created by the CIA into an Indian newspaper to obscure the KGB origin of the disinformation.[16]

The aim is to maximize the number of possible sources spreading the same disinformation messages as often as possible, in order to create an impression of seemingly independent sources confirming each other's message.[17] The repetition of the message leads to familiarity with the message, and the familiarity leads to acceptance.

The messages and the effect of the disinformation ecosystem

The strategic objective of the overall disinformation effort is very simple: to weaken and destabilize the West at every level. These levels include intergovernmental organizations, such as NATO and EU, individual states, regional administrations, governing coalitions, political parties, and all the way down to groups within society.[18] Vladimir Putin is unable to make Russia more competitive on the global stage and weakening Russia's adversaries is the only way the Kremlin can advance in a zero-sum game approach.

In this effort, the disinformers are spreading heavily polarized messages that trigger strong emotions and sow discord. They spread conspiracies that undermine trust in reliable sources of information; support radical and anti-Western elements in the targeted societies; promote anti-Western, anti-liberal, and anti-democratic politicians; and denigrate politicians who defend

[12] https://manipulatori.cz/sis-upozornuje-na-pusobeni-ruskych-a-cinskych-zpravodajskych-sluzeb-na-slovensku/

[13] See e.g. the articles in the section "Troll/bot network amplifying pro-Kremlin messaging" in the EUvsDisinfo Reading List: https://euvsdisinfo.eu/reading-list/mechanisms/

[14] https://disinfoportal.org/a-change-of-tactics-blurring-disinformations-source/

[15] https://www.nytimes.com/2019/03/29/world/europe/ukraine-russia-election-tampering-propaganda.html?fbclid=IwAR2uGPPsFmel-1hQ-kyi0-x0olEchO802QmKZHai2p-A9WnlfAdayQH4y4xQ

[16] https://euvsdisinfo.eu/bring-back-the-fifties-and-the-colorado-beetle/

[17] https://www.rand.org/pubs/perspectives/PE198.html

[18] https://euvsdisinfo.eu/commentary-means-goals-and-consequences-of-the-pro-kremlin-disinformation-campaign/

Western, liberal, and democratic values, because democracy and the rule of law threaten the survival of the current regime in the Kremlin.

The disinformation campaign must also protect itself, which often leads to the disinformers attacking those who uncover their information aggression and raise awareness about it, whether they are journalists, NGOs, civil servants, or politicians.

The precise content of the messages varies with the audience that is targeted.[19] The disinformers have different disinformation messages for people in the east of Europe, where you can read about necrophilia being an accepted norm in the EU,[20] and different messages for the people in Western Europe, where nobody would believe inventions about widespread sexual perversion in Western Europe but could believe that Ukrainians are Nazis just because they wear the Ukrainian national symbol.[21]

Often, there are differences even within one country, because different socioeconomic groups have different sensitivity to various topics. It is easier to stoke irrational fear of migrants in the mind of a lonely pensioner living in the countryside[22] than to do so with a diplomat living in the capital. Similarly, the tools and channels used to deliver the disinformation to an audience will be different, and social media is not always the most important channel.

The aim is to find those topics that stimulate the strongest emotions, as an audience driven by strong emotions will become irrational and more vulnerable to disinformation.[23] Therefore, the disinformation machine focuses on the most polarizing topics such as immigration, LGBTQ issues, and the grievances of and prejudices against national and racial minorities. As the Czechoslovak defector Ladislav Bittman wrote, disinformers are akin to an evil doctor, making a precise diagnosis of the maladies afflicting their "patients" - but then trying to make their weaknesses and illnesses worse.[24]

The disinformation campaign also spreads wild accusations targeted at individuals, organizations, and states that the Kremlin perceives as adversaries. Nordic countries are accused of genocide against Russian children.[25] The French, Americans, Belgians, Germans, British, Ukrainians, and all of Europe are accused of conducting terror attacks against its own citizens.[26] The Baltic countries, Germany, the United States, and Europe are regularly accused of Nazism.[27] The presenter who won the most prestigious Russian TV award for "best educational program" is

---

[19] https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/

[20] https://euvsdisinfo.eu/report/necrophilia-and-bestiality-are-accepted-norms-in-sweden-germany-and-denmark/

[21] https://euvsdisinfo.eu/report/ukrainian-footballer-roman-zozulya-is-a-nazi/

[22] https://disinfoportal.org/chain-emails-and-disinformation-in-the-czech-republic/

[23] https://euvsdisinfo.eu/the-strategy-and-tactics-of-the-pro-kremlin-disinformation-campaign/

[24] "Our main objective was to note and dissect all the enemy's weaknesses and sensitive or vulnerable spots and to analyze his failures and mistakes in order to exploit them. The formulation of special operations might remind one of a doctor who, in treating the patient entrusted to his care, prolongs his illness and speeds him to an early grave instead of curing him." Ladislav Bittman, *The Deception Game*, 1972 (p. 124)

[25] https://euvsdisinfo.eu/finland-puts-russian-kids-in-prison-disinformation-that-shaped-the-minds-of-millions/

[26] https://euvsdisinfo.eu/how-pro-kremlin-outlets-abuse-the-tragedy-of-terror/

[27] https://euvsdisinfo.eu/nazi-east-nazi-west-nazi-over-the-cuckoos-nest/

the same man who is behind other programs that claim Europe is a kingdom of gays who are trying to break children's psyche and force them to change sexes.[28]

The United States is frequently demonized as a fascist dictatorship, a power occupying or controlling Europe, orchestrating color revolutions all over the world, a warmonger unleashing conflict practically on a weekly basis, and an existential threat to Russia.[29]

With Ukraine, it is the United States that is the top target for the pro-Kremlin disinformation campaign.[30] Damaging the image of these countries will have wider consequences. It will be harder to negotiate Ukraine's accession to the EU or to NATO if we have big parts of our populations believing the Kremlin's lies about this country. The derogatory campaign about the United States damages the American image in Europe, weakens Transatlantic relations, and makes it harder for the United States to further its interests in an environment that is manipulated into hostility.

Despite the absurdity of some of these messages, there is evidence that they gain traction among certain target audiences. Throughout Europe and also in North America, there are documented cases where local actors, including high-level politicians, have repeated, and thus further amplified, messages from the Kremlin's disinformation ecosystem.[31] Even in the Netherlands, the country that lost the most citizens in the MH17 flight, you find influencers repeating Kremlin-originated lies whitewashing the real culprit of this horrible tragedy, such as the far-right leader Thierry Baudet.[32]

Some opinion polls show that a significant portion of the population can be vulnerable to a sustained disinformation campaign. According to one poll, 80 percent of Bulgarians did not believe that Moscow orchestrated the poisoning of the Skripals in Salisbury, England. According to another poll, half of the Czech population does not recognize that the claim that the EU is supposedly organizing illegal migration is a lie.[33]

We need more opinion polls to show us the precise scope of the damage and the vulnerabilities that exist. If conducted regularly, polls could also show us whether the problem is getting better or worse, and whether our counter-measures are effective. Without measuring the damage and the impact of our efforts, we are just shooting in the dark. Unfortunately, I am not aware of any organization in the world that focuses systematically on such mapping.

Apart from manipulating public opinion, there are even more dramatic results of disinformation campaigns. The man who fired a rifle in a Washington restaurant in 2017 believed he was saving children from the pedophile conspiracy known as Pizzagate,[34] a disinformation campaign

---

[28] https://euvsdisinfo.eu/the-disinformation-awards/ and https://euvsdisinfo.eu/homophobic-hate-speech-on-russian-tv/

[29] See the video by the Ukrainian Crisis Media Centre: https://www.youtube.com/watch?v=YXcajJVddwE&fbclid=IwAR1K_YW6Fv5X4chJowSw8Rj9fU9jWgeyNqsgTCfSvSyUdfSBvujGeS5ZRAc and the cases related to the US in the EUvsDisinfo database: https://euvsdisinfo.eu/disinformation-cases/?text=US&disinfo_issue=&date=

[30] https://euvsdisinfo.eu/year-in-review-1001-messages-of-pro-kremlin-disinformation/

[31] See the articles in the section "How non-Kremlin actors multiply Kremlin's disinformation" in the EUvsDisinfo Reading List: https://euvsdisinfo.eu/reading-list/mechanisms/

[32] https://www.thedailybeast.com/mh17-russia-deployed-its-trolls-to-cover-up-the-murder-of-298-people

[33] https://disinfoportal.org/euelections2019-the-danger-of-ignoring-disinformations-long-term-goals/

[34] https://www.nytimes.com/2017/06/22/us/pizzagate-attack-sentence.html

amplified by Russian trolls.[35] Earlier this year, a Czech pensioner was convicted of terrorism because he caused rail crashes that were intended to resemble jihadist attacks. The man was brainwashed by anti-Muslim propaganda that was amplified by groups that take pro-Kremlin stances, including extremist political parties, in the Czech Republic.

Importantly, these information operations go hand in hand with other influence operations[36] and active measures: supporting the European far-left and far-right, supporting paramilitary and martial arts groups, recruiting fighters for the war in Ukraine from European countries, and aiding other similar activities.[37] Again, all this is done in order to advance the main goal: weaken the West. Manipulating people with guns, or people who are prepared to use physical violence, and misleading them so that they believe they are under threat and have to use every means possible to defend themselves and their "in-group" - this is one of the more reliable ways to destabilize a society.

Election-related campaigns

It is necessary to keep this larger background in mind in order to fully appraise information operations targeting democratic processes, including elections and referenda. Looking at only the last few weeks before elections is like looking at the last five minutes of a basketball game in which one side is already thirty points ahead; the game is already decided, and there is not much that is relevant to be seen in the last five minutes.

If there is a long, ongoing, well-targeted disinformation campaign focusing, for example, on migration, which in some cases has spread lies like the one that migrants have made nine Italian nuns pregnant,[38] this shapes the information environment in a way that helps political actors who are using the fear of migration in their own campaigns. This was the case in Italy, where the Russian state media outlets *Sputnik* and *RT* boosted their anti-immigration content a full year before the 2018 parliamentary elections, with messages like, "in 2065, quota immigrants in Italy could exceed 40% of the total population," as shown by research done by Alto Analytics.[39] The disinformation campaign that potentially influences the outcome of a particular election is not an isolated event; it goes on for months or even years before the election itself, to sow the seeds of vulnerability.

Various researchers and journalists have identified pro-Kremlin disinformation campaigns (to a greater or lesser degree) in the following elections and referenda:

- Scottish independence referendum in 2014[40]
- Ukrainian elections in 2014[41]

---

[35] https://www.buzzfeednews.com/article/salvadorhernandez/russian-trolls-spread-baseless-conspiracy-theories-like

[36] https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/

[37] https://www.theatlantic.com/ideas/archive/2018/08/russia-is-co-opting-angry-young-men/568741/, https://www.dw.com/en/putins-secret-sleepers-waiting-for-a-signal/a-19196685 and https://reportermagazin.cz/a/pnscW/kdyz-vlastence-vzrusuje-valka

[38] https://euvsdisinfo.eu/the-pro-kremlin-narrative-about-migrants/

[39] https://elpais.com/elpais/2018/03/01/inenglish/1519922107_909331.html

[40] https://www.theguardian.com/politics/2017/dec/13/russian-cyber-activists-tried-to-discredit-scottish-independence-vote-says-analyst

[41] https://eu.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/

- Bulgarian local elections in 2015[42]
- Dutch referendum about the Association Agreement between the EU and Ukraine 2016[43]
- Brexit referendum in 2016[44]
- Austrian presidential elections in 2016[45]
- Italian constitutional referendum in 2016[46]
- French elections in 2017[47]
- German elections in 2017[48]
- Catalan referendum in 2017[49]
- Czech presidential elections in 2018[50]
- Italian parliamentary elections in 2018[51]
- Macedonian name referendum in 2018,[52] and the Russian activities connected to that in Greece[53]
- Ukrainian presidential elections in 2019[54]
- Slovakian presidential elections in 2019[55]
- European parliament elections in 2019[56]

I cannot guarantee that this list is exhaustive. But just from this brief overview, we can see that pro-Kremlin disinformation activity is definitely not becoming less aggressive.

Apart from the effect on public opinion that could be quantified if measured properly, there are two more effects that worry me.

The first one is that the disinformers are gaining new knowledge about our audiences every single day. They gain new knowledge about who buys into disinformation messaging, who advocates it, and who spreads it. From this point of view, they already know our audiences

---

[42] https://eu.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/

[43] https://www.stopfake.org/en/kremlin-disinformation-and-the-dutch-referendum/

[44] https://89up.org/russia-report

[45] https://us11.campaign-archive.com/?u=cd23226ada1699a77000eb60b&id=df2d65b2d6&e=712c1d978f

[46] https://www.buzzfeed.com/albertonardelli/italys-most-popular-political-party-is-leading-europe-in-fak

[47] https://www.atlanticcouncil.org/publications/reports/the-macron-leaks-operation-a-post-mortem

[48] https://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/

[49] https://elpais.com/elpais/2017/11/12/inenglish/1510478803_472085.html

[50] https://www.europeanvalues.net/wp-content/uploads/2018/02/The-role-of-the-Kremlin%E2%80%99s-influence-and-disinformation-in-the-Czech-presidential-elections.pdf

[51] https://elpais.com/elpais/2018/03/01/inenglish/1519922107_909331.html

[52] https://www.dw.com/en/us-says-russia-meddling-in-macedonia-ahead-of-name-referendum/a-45515175

[53] https://www.theguardian.com/world/2018/aug/11/greece-accuses-russia-bribery-meddling-macedonia-deal

[54] https://ukraineelects.org/report-foreign-interference-in-ukraines-democracy/

[55] https://disinfoportal.org/the-corrosive-effect-of-online-propaganda-channels-in-slovakia/

[56] https://disinfoportal.org/evaluation-of-the-eu-elections-many-gaps-still-remain/

better than we know them. The disinformers have also built a robust infrastructure for spreading disinformation, enhancing it and cultivating it on a daily basis. They are able to regularly identify new channels and new individuals who will spread disinformation for them. This infrastructure and this experience can be used for any purpose in the future, and I am afraid we are not prepared for such a reality.

The second is that the longer the disinformation campaign is in effect, the more people begin to perceive it as the new normal.[57] We saw this effect around the recent EU Parliament elections—some observers even claimed that Russian disinformation is now in retreat. The only relevant data from the European Union's East StratCom Task Force show that rather the opposite is the case (the number of disinformation cases the team identified this year doubled compared to the same period in 2018).[58] But some European observers have already gotten so used to the previous level of Russian disinformation that they are already not perceiving it as something strange. I find this trend very worrying and I am sure that the Kremlin is quite happy about it since it whitewashes their aggression.

What we see from the Russian side is a very clear understanding of the battlefield they have chosen, what their goals are, and a very high level of determination to achieve them. Unfortunately, this level of clarity does not exist in most Western democracies.

Defense and countermeasures

There are various approaches used to counter the Kremlin's hostile information operations in almost every European country.[59] Among them, I see four basic lines of effort:

1. documenting the threat, getting a better understanding of what is happening,
2. raising awareness - which means exposing the threat, communicating it to audiences in order to educate them, inoculating them to some degree, and attracting other actors who can join in the effort and help educate new audiences,
3. mitigating the weaknesses that the aggressor exploits,
4. challenging the aggressors and punishing them by making them pay a serious price for their efforts to undermine our societies. This is perhaps the most sensitive area, and the most frequently overlooked, but, unlike all the others, it may provide the best chance to actually stop the information aggression.

In each of these four lines of effort, multiple tactical measures can be undertaken. Some of them are better undertaken by governments, which can commit significant amounts of funding, focus on a topic even if the media loses interest, and coordinate actions nationally. Other efforts are better undertaken by civil society, which does not operate under the constraints of government and can more nimbly and aggressively communicate with a respective audience. Some efforts are best undertaken by the media, while others are best done by private businesses, including the social media platforms. And, obviously, different societies will pursue different approaches, because countries have different legal environments, differing sensitivity to the topic, different levels of media literacy, and so on.

It is necessary to pursue all of these lines of effort, ideally at the same time and in a coordinated way. Picking just some of these solutions and ignoring the others is unlikely to result in success.

1. Documenting the threat and gaining better understanding

[57] https://euvsdisinfo.eu/eu-elections-update-reaping-what-was-sown/

[58] https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf

[59] https://www.kremlinwatch.eu/userfiles/overview-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations_15273205278094.pdf

This is a task that the team in Brussels, where I used to work, focuses on. The EU's East StratCom Task Force[60] collects and documents cases of pro-Kremlin disinformation from Russian state media and other outlets in the pro-Kremlin ecosystem. In various European countries, different departments and agencies are concerned with this threat - typically the intelligence services, but also various StratCom teams, which may be located in Foreign Ministries, Defense Ministries, or Interior Ministries.

Documenting the threat is a necessary first step without which it is close to impossible to do anything else properly.

The ideal result of this activity is to learn how many channels are spreading disinformation, how many messages per day they spread, how many people they target, and how many people they persuade. For that, we would need to have an extraordinarily robust monitoring structure for both traditional and new media, and we would need to conduct regular opinion polls measuring the appeal of the disinformation messages.

Having a proper monitoring system that spots disinformation messages in real time would also enable us to build an early warning system for newly emerging disinformation attacks.

So far, the EU still does not have answers to questions such as how many disinformation channels there are and how many messages they spread. Put simply, there are not enough resources for such comprehensive monitoring.

Comprehensive monitoring tasks are probably best done by a governmental body or a government-funded agency. Private companies do not have the necessary funding or reach, and this task is closely connected to security concerns.

2. Raising the level of awareness about the threat

This is also something that the East StratCom Task Force is involved in: publishing materials on pro-Kremlin disinformation, delivering speeches at conferences, conducting training for governments, and briefing journalists and other critical audiences. The NATO's StratCom Center of Excellence in Riga[61] is involved in similar activities.

There are several bodies in Europe that are active in this area. One of the best examples is in Sweden, where the Security Service and the Civil Contingencies Agency have educated politicians, media, and other actors in the national system about the problem of hostile disinformation.[62] The Czech Center Against Terrorism and Hybrid Threats also focuses on raising awareness within its government.[63]

Another example is the Lithuanian Armed Forces StratCom Department. Some of you might have heard about the Lisa case in Germany, in which, at the beginning of 2016, thousands of people protested in the streets against Angela Merkel's refugee policy. The story, a lie amplified by Kremlin media and officials, involved a young girl who falsely claimed to have been raped by men who appeared to be immigrants.[64] A similar disinformation story surfaced in Lithuania a year later,[65] but it received close to no traction because the authorities were properly trained for such situations and because the StratCom team anticipated the situation, countering the false claim swiftly. They warned stakeholders about the disinformation claim when it first appeared

[60] https://euvsdisinfo.eu/about/

[61] https://www.stratcomcoe.org/

[62] https://euvsdisinfo.eu/in-sweden-resilience-is-key-to-combatting-disinformation/

[63] https://en.wikipedia.org/wiki/Centre_Against_Terrorism_and_Hybrid_Threats

[64] https://www.bbc.com/news/blogs-eu-35413134

[65] https://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870

and, as a result, the first story in the media was not that a little girl had allegedly been raped, but that there had been another disinformation attack on Lithuania. This case is a brilliant example of neutralizing disinformation *before* it has time to spread.

However, for this to occur, a very high level of awareness is needed, plus excellent, real-time monitoring of the information space and expert knowledge about potential disinformation claims. All of this does not occur overnight. For others to improve in this area, they must work diligently to raise and maintain a high level of awareness over a long period of time in order to get to a point where their system can respond in the exemplary way in which the Lithuanians did.

I am afraid that the EU as a whole does not have a level of awareness as high as that of some of its Member States, such as Lithuania. It would be necessary to have a much larger and better-resourced campaign than is possible under current circumstances. Current EU communications on this issue, including those from the East StratCom Task Force, often offer excellent quality content, but do not yet have sufficient reach.

It is also necessary to bear in mind that it is not enough to focus just on government efforts. It is also important to engage with other audiences that are critical in combating disinformation, including politicians, journalists, and academics.

It is crucial to look for actors outside government because not everyone trusts what governments say. We need other opinion leaders to act as trusted messengers on these issues to their own audiences, which government often cannot reach.

A good example is, again, Lithuania, where there is a news-comedy program, similar to *Last Week Tonight with John Oliver*, that makes fun of Russian propaganda.[66] Or a young and influential Czech Youtuber who educates hundreds of thousands of his followers about media literacy and fake news.[67] These actors can address audiences that governments and other men in suits hardly reach. It is necessary to raise awareness of this problem very broadly throughout society, and for that, a variety of actors is needed.

However, governments can also support these other actors who are doing similar work by supporting quality media and independent journalists covering these topics, as well as NGOs who are working in this area. It is worrying to hear the European anti-disinformation community complain about lack of funding for their activities.[68]

And it is important to focus not only on one's own country, but also to raise awareness about what is happening elsewhere. As mentioned in the recent Atlantic Council report on the disinformation attacks surrounding the 2017 elections in France, apart from structural reasons and luck, a big role in the successful defense against the disinformation was learning from others, which raised awareness about what might happen and permitted pre-planning for contingencies. Thus, when a hack-and-leak operation similar to the one in the United States in 2016 appeared on the eve of the election, the Macron campaign was very well prepared.[69]

This case also reminds us about the adaptability of the disinformers. While the hack-and-leak operation succeeded in the United States, it failed in France. Therefore, the disinformers did

---

[66] https://www.voanews.com/europe/baltics-russian-media-use-online-humor-combat-propaganda

[67] https://hlidacipes.org/hvezda-youtube-kovy-uz-nesbira-jen-klikance-se-statisici-fanousku-v-zadech-dela-osvetu-o-mediich/

[68] https://disinfoportal.org/euelections2019-the-eu-must-take-disinformation-seriously/

[69] https://www.atlanticcouncil.org/images/publications/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

not try the same strategy in Germany in the 2017 Bundestag election, despite the fact that Russia already had the hacked content that could be used for such a purpose.[70]

3. Repairing the systemic weaknesses, building up our defense

Kremlin disinformation rarely seeks to create new divisions and weaknesses in society; instead, it exploits divisions and weaknesses that already exist. Trying to mitigate these weaknesses is one of the ways to make our societies less vulnerable.

A big part of building up our defenses is done by raising awareness of the threat. In order to solve a problem, you have to know about it. Therefore, a good communication campaign about the threat posed by disinformation can be a very good first step to repair some of the weaknesses in our societies and information systems.

However, we cannot rely only on communication experts. Structural weaknesses require the involvement of more specialized professionals.

"Media literacy" is often mentioned as a way to protect against disinformation. In the Nordic countries, which are frequently cited as examples of highly media-literate societies, the local versions of Russian disinformation outlet *Sputnik* had to shut down in a fairly short amount of time because they did not attract enough readers.[71] In particular, Finland is often cited as one of the best examples of a highly media-literate society resisting fake news.[72]

However, the results that can be expected by improving media literary are often over-emphasized. First, this will require concerted campaigns across numerous educational systems that will have to last for decades to have the desired effect. This is a massive effort with very long lead times. And we need solutions more urgently.

In addition, what we have observed in Europe is that if the information aggressors cannot exploit one weakness, they simply move on to exploit different ones. In the case of Nordic states, this could be cyberattacks or online trolling. The worst case of personalized online bullying that we know about in the entire EU was against the Finnish journalist Jessikka Aro, who was exposing Kremlin influence operations in Finland. This case has already had criminal consequences.[73]

Trying to raise the level of media literacy in any society is certainly something that can only help to counter disinformation. But it is a very long-term task, which should not be undertaken by communication teams, but by education experts, academia, and education ministries.

Another weakness to be mitigated is the social media environment. While not the only channel responsible for the dissemination of disinformation, social media platforms allow disinformation to spread virally. Social media platforms, however, cannot solve the entire problem of online disinformation. They do not produce the malicious content; they just are used and abused to spread it. Social media may be a very powerful weapon, but the platforms are not the ones pulling the trigger.

Social media platforms can be pushed to de-rank and clearly label content from outlets notorious for spreading disinformation. A similar approach was used against tobacco - the smoker can still smoke, he is just clearly warned that he is using a harmful substance. Similarly, disinformation outlets could be labelled as harmful to one's mental health.

---

[70] https://www.dw.com/en/germany-admits-hackers-infiltrated-federal-ministries-russian-group-suspected/a-42775517

[71] https://euvsdisinfo.eu/in-sweden-resilience-is-key-to-combatting-disinformation/

[72] https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/

[73] https://www.bbc.com/news/world-europe-45902496

If social media executives plead that their platforms are not there to determine which information is true and false, that is an excuse. If the companies do not know how to identify disinformation, they can ask the multiple organizations that have been working on this topic in recent years. In 2019, it is an inexcusable shame that some of the platforms still recommend known disinformation content at some of the highest positions in their search results.[74]

However, I would agree with a recent statement by Facebook CEO Mark Zuckerberg, that the social media companies cannot handle this crisis on their own and that they should not have the final word.[75] They cannot force the information aggressors to stop their aggression; that is already a task for someone else.

The European Union is working with the industry through a voluntary Code of Practice on Disinformation.[76] Several platforms like Google, Facebook, and Twitter have agreed to self-regulatory standards to fight disinformation. However, the EU Commissioners are still not fully satisfied with the progress so far and have threatened a regulatory approach.[77]

And, despite the fact that Facebook has closed down over two billion fake accounts, the number of disinformation cases identified by the East StratCom doubled in 2019 compared to the same period in 2018. That could indicate that the disinformers have adapted to the new environment, for example by using real people to spread disinformation instead of fake accounts.[78]

The traditional media can also do more to fix their own weaknesses. Five years ago, Peter Pomerantsev and Michael Weiss proposed that a Disinformation Charter for media and bloggers be formulated in order to identify which behavior is acceptable and which is not. They also recommended that media outlets hire specialized disinformation editors who could prevent the media from becoming an inadvertent purveyor of disinformation.[79] As far as I know, there has been no progress on this in the past five years.

Another action that needs to be taken consists of focusing on groups that are most vulnerable to disinformation campaigns. We need to know how many people are influenced by various disinformation campaigns, and who they are. Once we know this, we know where the biggest problems are. If we conclude that pensioners are spreading disinformation in part because they feel lonely,[80] we can try to address this problem. If political parties notice that former high-level politicians crave their former recognition and acclaim—and the disinformers are often the first ones to exploit such cravings—we can try to engage retired politicians more and thereby mitigate their vulnerability to be exploited.

Another weakness that is often exploited are tensions among different socioeconomic groups: between the younger and older generation, urban and rural areas, higher and lower income brackets, between the majority group and various religious, racial, national or sexual minorities. While overcoming these tensions should be part of a sensible policy in any society regardless of the danger of disinformation, it will also help to reduce vulnerabilities that disinformers can

---

[74] https://www.washingtonpost.com/technology/2019/04/26/youtube-recommended-russian-media-site-above-all-others-analysis-mueller-report-watchdog-group-says/?utm_term=.b98692da9a61

[75] https://www.theguardian.com/technology/2019/jun/26/facebook-constitution-supreme-court-zuckerberg

[76] https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[77] http://europa.eu/rapid/press-release_STATEMENT-19-2570_en.htm

[78] https://disinfoportal.org/a-change-of-tactics-blurring-disinformations-source/

[79] https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev_The_Menace_of_Unreality.pdf

[80] https://disinfoportal.org/chain-emails-and-disinformation-in-the-czech-republic/

exploit. And the opposite holds: worsening these tensions and divisions will provide the disinformers with more fertile ground for their operations.

In the area of mitigating weaknesses that can be exploited by disinformation, almost every part of our society could do more: governments, NGOs, media, both traditional and new, politicians, influential opinion leaders and opinion makers, tech companies, academia and schools, etc.

4. Punishing the aggressor

All three areas above are necessary, but they are not enough to stop information aggression. We can document information attacks, but that will not make them stop. We can try to prepare our populations for information attacks and do our best to mitigate weaknesses that can be exploited, but there will always be weaknesses and fissures in every society. In addition, disinformation, like a virus, mutates and adapts to new environments, and will always find new weaknesses and targets.

It is in the nature of the aggressor to be aggressive. If we want to stop aggression, we must punish it and do our best to dissuade any further incidents. This is not an appeal to create new rules or new laws. In many cases, we just need to use the already existing ones.

It is necessary to name and shame those who are part of pro-Kremlin disinformation campaigns, either wittingly or unwittingly. It should not be perceived as normal or acceptable to repeat Kremlin lies about Ukraine, Syria, MH17, or about Russia being the supposed protector of traditional values against the decaying West. Individuals who are helping the Kremlin to spread these lies should be named and shamed - by the media, politicians, NGOs, academics, and others. Some European NGOs are doing this, but, unfortunately, this is not a usual part of mainstream media reporting, and it is almost never done by governments or civil servants.

The most aggressive and most visible propagandists should be sanctioned. It is a shame that, to this day, it is only Dmitry Kiselyov, who is something like Vladimir Putin's Joseph Goebbels, who has been sanctioned by the EU.[81] Another pet journalist of Putin, Vladimir Solovyov, uses his show to spread hatred against the West several times a week, yet freely enjoys the pleasures of luxurious villas at Lago di Como in Italy.[82] And there are dozens more who deserve to be on the sanctions list. Punishing the most visible propagandists and periodically adding new individuals who participate in Kremlin disinformation would send a clear signal that the West does not tolerate the spreading of lies and hatred. Those who propagate lies and hatred about our world in order to break it down simply should not enjoy all the benefits our system and our values offer.

Similarly, Western companies should pull their ads from disinformation outlets, both in Russia and in Russian media publishing abroad. It is mind-blowing to see Western companies among the top advertisers on Russian TV.[83] A quote ascribed to Vladimir Lenin said, "The capitalists will sell us the rope with which we will hang them." Those Western companies that are buying advertising time in Russian media that is used as a weapon against the West are doing exactly that. Sanctioning not only the individuals but also the companies involved in spreading disinformation could help to achieve that goal.

Western countries and politicians should limit access to disinformation-oriented outlets and cut them off, with no accreditation, no access to press conferences, no statements for them, and no answers to their questions. These restrictions would make it clear that they are not media, as they themselves admit, but weapons in an information war, as noted above. Estonia made the correct decision not to allow Russian pseudo-reporters to cover an EU foreign ministers' meeting in 2017, and I find it horrible that the OSCE and the European Federation of Journalists

[81] https://euvsdisinfo.eu/a-disillusioned-democrat/

[82] https://belsat.eu/en/news/russian-propagandist-solovyov-notorious-for-demonizing-west-buys-como-lake-villas/

[83] https://www.vedomosti.ru/technology/articles/2016/10/20/661678-reklamiruemim-tinkoff-bank

reproached the Estonians for this.[84] This is the equivalent of professional medical doctors defending the right of quacks and charlatans to harm people with bogus treatments.

Fortunately, the UK Foreign Office followed Estonia's example very recently and also refused accreditation to *RT* and *Sputnik*, thereby effectively banning them from attending a conference on media freedom.[85] European countries should also be inspired by the US example and have such media register as foreign agents.

In many countries, it is possible to use existing laws and regulations to force pro-Kremlin pseudo-media to adhere to industry standard. In 2016, Lithuanian authorities punished a Russian TV channel for inciting hatred based on nationality.[86] At the beginning of this year, a Latvian broadcast regulator temporarily restricted a Russian TV channel because of hate speech and incitement of war.[87] This May, Lithuania kicked out the head of Lithuanian *Sputnik* since he is considered a threat to national security.[88] Britain's media regulator, Ofcom, has punished *RT* several times already, primarily for not upholding media impartiality.[89] The pro-Kremlin disinformation ecosystem regularly spreads lies, defamation, false accusations, and false alarms —I believe there are many cases when they might violate the laws or regulations of different countries.

In order to be able to identify those who deserve to be punished, it is also necessary to conduct official investigations, similar to the one conducted by Special Counsel Robert Mueller. This is an area where the United States is far ahead of Europe—the Americans are investigating the attack on their democracy, and a proper investigation is the necessary prelude to a just punishment. Despite the long list of European elections and referenda that have been targeted by Kremlin disinformation in the past five years, I am not aware of a single similar investigation in Europe.[90] We Europeans are basically saying that we do not care whether someone attacks our democracy, we will not react. As a result, logically, we thereby invite further aggression.

Punishing the information aggressors will have one more desirable effect: it will deter other potential aggressors. We already see that other state and non-state actors are adopting the Kremlin's playbook, apparently because they have calculated that the weak reaction of Western societies is nothing that would deter them. According to some reports, it is especially China that is active in this regard.

A resolute punishment of the number one information criminal would send a clear signal to other potential criminals.

Conclusion

---

[84] https://www.rferl.org/a/osce-desir-calls-on-estonia-reconsider-ban-russian-reporters-russia-today-sputnik/28706515.html

[85] https://www.bbc.com/news/world-europe-48919085

[86] https://www.politico.eu/article/eu-court-backs-lithuania-in-tv-hate-speech-case/

[87] https://eng.lsm.lv/article/culture/culture/latvian-broadcast-regulator-hits-russian-channel-with-3-month-ban.a307942/

[88] https://www.rferl.org/a/lithuania-expels-chief-editor-of-sputnik-local-branch/29968909.html

[89] https://www.reuters.com/article/us-britain-russia-ofcom/uk-media-watchdog-says-russian-broadcaster-rt-broke-impartiality-rules-idUSKCN1OJ1D2

[90] The closest comparison was probably the UK Parliamentary investigation into disinformation and fake news, which does not have criminal consequences: https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/

Just recently, a white paper prepared in the Pentagon warned that the United States is still underestimating the scope of Russia's aggression and the danger posed by their influence operations.[91] I am afraid much the same could be said about Europe and most of its countries.

On the other hand, the Western countries have all the necessary tools in order to win this fight; we are just not using them. Russia is currently besting us only because of its ruthless determination and total lack of morals. They act, while we engage in seemingly endless discussions about whether we should act, how, and toward whom. It does not have to be this way. If we decide we want to win this fight, we will win it. It is only a matter of political will, not knowledge or capabilities.

[91] https://www.politico.com/story/2019/06/30/pentagon-russia-influence-putin-trump-1535243

Mr. KEATING. Dr. Kagan.

STATEMENT OF FREDERICK W. KAGAN, PH.D., RESIDENT SCHOLAR AND DIRECTOR, CRITICAL THREATS PROJECT, AMERICAN ENTERPRISE INSTITUTE

Mr. KAGAN. Mr. Chairman, Ranking Member Kinzinger, thank you for the opportunity to appear before the subcommittee today. Thank you also for calling this hearing to address the challenges of Russian information operations against both the United States and Europe generally.

It is vitally important to keep in mind, as the subcommittee clearly does, that Vladimir Putin is engaged in a general attack on the institutions of democracy and representative government throughout the West and, in fact, throughout the world.

One of his aims is to destroy the trust and confidence of Western peoples in their governments and in the very institutions of representative government themselves. He pursues this aim, unfortunately, in an increasingly conducive environment, as Western people seem increasingly to be losing faith in critical institutions on their own. Addressing the Russian challenge will thus require that we also address that internal problem.

Putin is not an opportunistic predator as he is often portrayed. He has a concrete program. He has articulated an end state. He has articulated an alternate vision of the world. He pursues those objectives through concrete and organized campaigns. They are very flexible, they are opportunistic, they take advantage when he can, but they are nevertheless clear.

Russian military doctrine increasingly is making the argument that even tactical undertakings, even kinetic actions, should all be subordinated to the aim of shaping the information environment rather than achieving specific military ends, and that is important because I think that we need to see the activities that Putin is engaged in in the context of a political military campaign that he is pursuing globally, not just as crimes, although they clearly are crimes and also need to be punished in that way.

The Soviet concept of reflexive control is central to this entire undertaking, and it is important to understand that concept. Basically, the idea of reflexive control is so to shape your adversary's perception of reality as to cause your adversary voluntarily, of his own will, to choose the course of action you prefer without even being aware that he has been manipulated into doing so.

It is a kind of jiu-jitsu in information operations, which is not surprising considering that Putin himself is a fan of the Russian or Soviet version of Judo. Also, that he is a small person, which bears repeating as part of an information operation.

One of the advantages that Putin's aims give him is that they are negative. What matters to Putin is less that we believe what he is saying and more that we do not believe what we are saying. And so Putin's objectives are achieved if people simply say to themselves and to each other: Well, who really knows? I mean, after all, did the Russians shoot down the airplane? I mean, who really knows?

And of course, we do know. But getting people to positive belief is much harder than getting them simply to throw up their hands

and say: Who knows? And we have to understand how important, how difficult that makes the challenge that we are facing here.

But the approach that Putin is taking has vulnerabilities as well. It relies to a very heavy extent on a degree of stealth and anonymity and on the ability to persuade people that what they are hearing is not simply Russian propaganda but is coming from sources that they trust and so forth.

And in addition to that, we have now seen on several occasions that Putin can pay a very significant price when covert operations are blown, and there are two major examples of that in, ironically, two of his biggest successes, Ukraine, where the sense of Ukrainian nationhood and nationalism and resistance to and separation from Russia in western Ukraine is higher than it has ever been. And I do not actually think that it will be undone regardless of what settlement is reached by this government in Kiev or any other. And that is a result of the reaction against what Putin did there.

And even in our own election, the fact that we are having this hearing, the fact that we are here, is evidence of a Putin failure. It demonstrates the degree to which he has caused us to reflect on what he is doing.

And that blowback phenomenon is something that we can take advantage of. But we are not, as my co-panelists have pointed out, equipped as a government or a people to take advantage of it yet, and we should focus on that.

And so some of my concrete recommendations to you are to consider establishing cells in various places in the government, I do not really care who owns them, whose job it is to follow the Russian campaigns, to understand what Putin is trying to do generally, which will allow us to predict the kinds of information operations that he is likely to undertake, the kinds of cyber operations that he is likely to launch in support of them.

And then those cells need to develop plans. When should we blow this operation? When should we make it public that the Russians are doing this? To what purpose? What will we try to accomplish? What are our plans for accomplishing that?

And I would submit this needs to be a specialized cell because we must also restrict ourselves only to telling the truth. We must never get into the business of lying to ourselves, to the American people. We can do that, but it makes it harder. And so I think that this is something that organizationally and structurally would require a great deal of attention.

And we also need to have cells that are prepared to take advantage when third parties blow Russian operations, because that will happen more frequently than us blowing them ourselves. We have heroic people like Ms. Aro, who will do this on their own, and others, and we need to be prepared to take advantage of that.

And there are various other specific things that I think we could talk about as well, and I would be happy to address those.

I simply want to end, though, by saying we also have to recognize the weaknesses in our own current political discourse that make us particularly vulnerable to what the Russians are doing. The incivility, the mistrust, the hate, the emotion that is spewed by both sides and within both parties at each other is undermining

Americans' faith in themselves and what we stand for, in our institutions, and it is opening opportunities for Putin.

I do not expect to get to some grand kumbaya moment where all of that stops, but to the extent that we can close that gap and restore civility to our discourse, we will make it much harder for Putin to attack us in this fashion.

Thank you.

[The prepared statement of Mr. Kagan follows:]

AMERICAN ENTERPRISE INSTITUTE

Statement before the House Committee on Foreign Affairs
Subcommittee on Europe, Eurasia, Energy, and the Environment
On "Russian Disinformation Attacks on Elections: Lessons from Europe"

Confronting the Russian Challenge

Frederick W. Kagan
Resident Scholar and Director, Critical Threats Project

July 16, 2019

Chairman Keating, Ranking Member Kinzinger, and members of the subcommittee: thank you for the opportunity to testify.

Russia poses a significant threat to the United States and its allies for which the West is not ready. The West must act urgently to meet this threat without exaggerating it. Russia today does not have the military strength of the Soviet Union. It is a poor state with an economy roughly the size of Canada's, a population less than half that of the U.S., and demographic trends indicating that it will lose strength over time. It is not a conventional military near-peer nor will it become so. Its unconventional warfare and information operations pose daunting but not insuperable challenges. The U.S. and its allies must develop a coherent global approach to meeting and transcending the Russian challenge.

The Russian Threat

President Vladimir Putin has invaded two of his neighbors, Georgia and Ukraine, partly to stop them from aligning with NATO and the West. He has also illegally annexed territory from both those states. He has established a military base in the eastern Mediterranean that he uses to interfere with, shape, and restrict the operations of the U.S. and the anti-ISIS coalition. He has given cover to Bashar al Assad's use of chemical weapons, and Russian agents have used military-grade chemical weapons in assassination attempts in Great Britain. Russia has threatened to use nuclear weapons, even in regional and local conflicts. And Moscow has interfered in elections and domestic political discourse in the U.S. and Europe.

The Russian threat's effectiveness results mainly from the West's weaknesses. NATO's European members are not meeting their full commitments to the alliance to maintain the fighting power needed to deter and defeat the emerging challenge from Moscow. Increasing political polarization and the erosion of trust by Western peoples in their governments creates vulnerabilities that the Kremlin has adroitly exploited.

Moscow's success in manipulating Western perceptions of and reactions to its activities has fueled the development of an approach to warfare that the West finds difficult to understand, let alone counter. Shaping the information space is the primary effort to which Russian military operations, even conventional military operations, are frequently subordinated in this way of war. Russia obfuscates its activities and confuses the discussion so that many people throw up their hands and say simply, "Who knows if the Russians really did that? Who knows if it was legal?"—thus paralyzing the West's responses.

Putin's Program

Putin is not simply an opportunistic predator. Putin and the major institutions of the Russian Federation have a program as coherent as that of any Western leader. Putin enunciates his objectives in major speeches, and his ministers generate detailed formal expositions of Russia's military and diplomatic aims and its efforts and the methods and resources it uses to pursue them. These statements cohere with the actions of Russian officials and military units on the ground. The common perception that he is opportunistic arises from the way that the Kremlin sets conditions to achieve these objectives in advance. Putin closely monitors the domestic and international situation and decides to execute plans when and if conditions require and favor the Kremlin. The aims of Russian policy can be distilled into the following:

Domestic Objectives. Putin is an autocrat who seeks to retain control of his state and the succession. He seeks to keep his power circle content, maintain his own popularity, suppress domestic political opposition in the name of blocking a "color revolution" he falsely accuses the West of preparing, and expand the Russian economy.

Putin has not fixed the economy, which remains corrupt, inefficient, and dependent on petrochemical and mineral exports. He has focused instead on ending the international sanctions regime to obtain the cash, expertise, and technology he needs. Information operations and hybrid warfare undertakings in Europe are heavily aimed at this objective.

External Objectives. Putin's foreign policy aims are clear: end American dominance and the "unipolar" world order, restore "multipolarity," and reestablish Russia as a global power and broker. He identifies NATO as an adversary and a threat and seeks to negate it. He aims to break Western unity, establish Russian suzerainty over the former Soviet States, and regain a global footprint.

Putin works to break Western unity by invalidating the collective defense provision of the North Atlantic Treaty (Article 5), weakening the European Union, and destroying the faith of Western societies in their governments.

He is reestablishing a global military footprint similar in extent the Soviet Union's, but with different aims. He is neither advancing an ideology, nor establishing bases from which to project conventional military power on a large scale. He aims rather to constrain and shape America's actions using small numbers of troops and agents along with advanced anti-air and anti-shipping systems.

Recommendations

A sound U.S. grand strategic approach to Russia

- Aims to achieve core American national security objectives positively rather than to react defensively to Russian actions;
- Holistically addresses all U.S. interests globally as they relate to Russia rather than considering them theater-by-theater;
- Does not trade core American national security interests in one theater for those in another, or sacrifice one vital interest for another;
- Achieves American objectives by means short of war if at all possible;
- Deters nuclear war, the use of any nuclear weapons, and other Weapons of Mass Destruction (WMD);
- Accepts the risk of conventional conflict with Russia while seeking to avoid it and to control escalation, while also ensuring that American forces will prevail at any escalation level;
- Contests Russian information operations and hybrid warfare undertakings; and
- Extends American protection and deterrence to U.S. allies in NATO and outside of NATO.

Such an approach involves four principal lines of effort.

Constrain Putin's Resources. Russia uses hybrid warfare approaches because of its relative poverty and inability to field large and modern military systems that could challenge the U.S. and NATO symmetrically. Lifting or reducing the current sanctions regime or otherwise facilitating Russia's access to wealth and technology could give Putin the resources he needs to mount a much more significant conventional threat—an aim he had been pursuing in the early 2000s when high oil prices and no sanctions made it seem possible.

Disrupt Hybrid Operations. Identifying, exposing, and disrupting hybrid operations is a feasible, if difficult, undertaking. New structures in the U.S. military, State Department, and possibly National Security Council Staff are likely needed to:

1. Coordinate efforts to identify and understand hybrid operations in preparation and underway;
2. Develop recommendations for action against hybrid operations that the U.S. government has identified but are not yet publicly known;
3. Respond to the unexpected third-party exposure of hybrid operations whether the U.S. government knew about the operations or not;
4. Identify in advance the specific campaign and strategic objectives that should be pursued when the U.S. government deliberately exposes a particular hybrid operation or when third parties expose hybrid operations of a certain type in a certain area;
5. Shape the U.S. government response, particularly in the information space, to drive the blowback effects of the exposure of a particular hybrid operation toward achieving those identified objectives; and
6. Learn lessons from past and current counter-hybrid operations undertakings, improve techniques, and prepare for future evolutions of Russian approaches in coordination with allies and partners.

The U.S. should also develop a counter-information operations approach that uses only truth against Russian narratives aimed at sowing discord within the West and at undermining the legitimacy of Western governments.

Delegitimize Putin as a Mediator and Convener. Recognition as one of the poles of a multipolar world order

is vital to Putin. It is part of the greatness he promises the Russian people in return for taking their liberty. Getting a "seat at the table" of Western-led endeavors is insufficient for him because he seeks to transform the international system fundamentally. He finds the very language of being offered a seat at the West's table patronizing.

He has gained much more legitimacy as an international partner in Syria and Ukraine than his behavior warrants. He benefits from the continuous desire of Western leaders to believe that Moscow will help them out of their own problems if only it is approached in the right way.

The U.S. and its allies must instead recognize that Putin is a self-declared adversary who seeks to weaken, divide, and harm them—never to strengthen or help them. He has made clear in word and deed that his interests are antithetical to the West's. The West should therefore stop treating him as a potential partner, but instead require him to demonstrate that he can and will act to advance rather than damage the West's interests before engaging with him at high levels.

The West must not trade interests in one region for Putin's help in another, even if there is reason to believe that he would actually be helpful. Those working on American policy in Syria and the Levant must recognize that the U.S. cannot afford to subordinate its global Russia policy to pursue limited interests, however important, within the Middle East. Recognizing Putin as a mediator or convener in Syria—to constrain Iran's activities in the south of that country, for example—is too high a price tag to pay for undermining a coherent global approach to the Russian threat. Granting him credibility in that role there enhances his credibility in his self-proclaimed role as a mediator rather than belligerent in Ukraine. The tradeoff of interests is unacceptable.

Nor should the U.S. engage with Putin about Ukraine until he has committed publicly in word and deed to what should be the minimum non-negotiable Western demand—the recognition of the full sovereignty of all the former Soviet states, specifically including Ukraine, in their borders as of the dates of their admission as independent countries to the United Nations, and the formal renunciation (including the repealing of relevant Russian legislation) of any right to interfere in the internal affairs of those states.

Defend NATO. The increased Russian threat requires increased efforts to defend NATO against both conventional and hybrid threats. All NATO members must meet their commitments to defense spending targets—and should be prepared to go beyond those commitments to field the forces necessary to defend themselves and other alliance members. The Russian base in Syria poses a threat to Western operations in the Middle East that are essential to protecting our own citizens and security against terrorist threats and Iran. Neither the U.S. nor NATO is postured to protect the Mediterranean or fight for access to the Middle East through the eastern Mediterranean. NATO must now prepare to field and deploy additional forces to ensure that it can win that fight.

The West should also remove as much ambiguity as possible from the NATO commitment to defend member states threatened by hybrid warfare. The 2018 Brussels Declaration affirming the alliance's intention to defend member states attacked by hybrid warfare was a good start. The U.S. and other NATO states with stronger militaries should go further by declaring that they will come to the aid of a member state attacked by conventional or hybrid means regardless of whether Article 5 is formally activated, creating a pre-emptive coalition of the willing to deter Russian aggression.

Bilateral Negotiations. Recognizing that Russia is a self-defined adversary and threat does not preclude direct negotiations. The U.S. negotiated several arms control treaties with the Soviet Union and has negotiated with other self-defined enemies as well. It should retain open channels of communication and a willingness to work together with Russia on bilateral areas in which real and verifiable agreement is possible, even while refusing to grant legitimacy to Russian intervention in conflicts beyond its borders. Such areas could include strategic nuclear weapons, cyber operations, interference in elections, the Intermediate Nuclear Forces treaty, and other matters related to direct Russo-American tensions and concerns. There is little likelihood of any negotiation yielding fruit at this point, but there is no need to refuse to talk with Russia on these and similar issues in hopes of laying the groundwork for more successful discussions in the future.

Mr. KEATING. Thank you, Doctor.

I now give myself 5 minutes for questions.

Ms. Aro, you mentioned in your testimony that you have been—well documented—you have been threatened in the past, harassed, defamed, and you mentioned even being here today could result in that. And I admire your courage, we all do, for continuing that effort and for the role of journalists to continue that effort.

If you would like, could you take a few minutes and be more specific about the kind of things that were done to you. I think if you are worried about the future, one of the best things to do is a little sunshine and tell the kind of tactics that were used against you personally, and hopefully, this will deter them to do that in the future, if you could.

Ms. ARO. Of course. Thank you so much for the encouraging words.

So, for example, over 300 articles in a fake news site, pro-Kremlin, Finnish-language site called—excuse me, my language—WTF paper, somewhat popular far-right neo-Nazi, pro-hate speech site. They have published around 300 articles in which they smear me as a paid NATO agent, paid America propagandist, brain damaged, drug user, that I am a threat to Finnish national security, that I work in cooperation with British and American troll armies. And they also post really nasty photos of my face, like manipulated horrible photos, and they even attack anyone who publicly supports me or even, you know, credits my work. They attack them as well. They smear them as well.

They also have attacked the policemen who have investigated my case. They have attacked just, you know, anyone. They also cyber stalk me and my activities.

In addition, for example, the police found in their investigations that someone, even my colleague within the Finnish Broadcasting Company, had been keeping an eye on me inside my workplace and then passed on that information about my job assignments as well as my job, you know, activities and my location to the main suspected stalker, who works for Putin's think tank in Moscow and who has been in charge of these operations.

And, yes, so because also these operations have been international, I have also received death threats and shooting phone calls from Russian-speaking countries, because there are Russian smear articles against me. And, for example, I have been forced to leave Finland some years back just to, you know, try and make my investigative book about Russian trolls in peace.

Mr. KEATING. Actually you had to leave your home?

Ms. ARO. Sorry?

Mr. KEATING. You had to leave your home?

Ms. ARO. Yes.

Mr. KEATING. That is amazing. Have the authorities done much to help you in that regard? What is available? What was available to you to help you?

Ms. ARO. Yes, they have definitely investigated my crime complaints very carefully and I believe they still continue to do so. But of course these court processes take time, and the trolls and propagandists and security services who run these operations, they take advantage of our longish justice system.

Mr. KEATING. Thank you for sharing that. I know it was not easy.

Just quickly, Ambassador Fried and Dr. Kagan mentioned this in particular, and in a different way Mr. Kalensky did too. Reflecting on the U.S. situation, what I heard from your testimony was we are not as organized or centralized as we should be, that we are lacking in political will to deal with this, and there is further need of punishing or some kind of a response to this. Pretty disturbing reflections.

We are out of time, almost. Can you just quickly, what could we do to improve this in our own country?

Ambassador.

Mr. FRIED. The signals from the top of the U.S. administration should not be ambiguous.

Mr. KEATING. Let me be clear. When you say top of the administration——

Mr. FRIED. The President.

Mr. KEATING. The President.

Mr. FRIED. Ambiguity is not helpful. There are a lot of people in the administration, political appointees and career people, who understand the problem and want to do the right thing. But in an atmosphere of, let us say, mixed signals, there is a natural disincentive for somebody to stand up and try to own the problem, to try to push forward difficult solutions.

And regulatory solutions are going to be difficult. We are going to be bumping up against issues of free speech. And you need a collaborative, cooperative base from which to tackle them.

It is possible. This is not an impossible problem to manage. It is impossible if your standard for solving it is 100 percent. But that need not be our standard. This is doable, but we have to go out and start doing it.

Mr. KEATING. I have gone over my time. I am sure some of the other witnesses will reflect that with the other questions of the members of the committee.

I now recognize the ranking member for 5 minutes, Mr. Kinzinger.

Mr. KINZINGER. Thank you, Mr. Chairman.

And, again, thank you all for being here.

Ms. Aro, I just want to say that you are heroic in what you are doing. And I know that it is difficult, I know that it is not fun, and I know that the easiest thing to do would be to walk away and just say you did your peace. But I appreciate you being here and continuing to stand strong in the face of a really tiny man, as Dr. Kagan pointed out.

Mr. Ambassador, you are correct, too, in talking about ambiguity. I think the reality is Russia tried to interfere in the 2016 election. We can have debates about, you know, what the result was of that, we may disagree on that, but there was no doubt there was interference.

And it is going to happen to both parties eventually. It is all about creating instability. It is all about creating doubt. And it is something that we have to be very clear about, because lack of clarity leads to Dr. Kagan's point about, well, who knows what is true? And then if you are, "Who knows what is true?" you are, like, "I

will just watch, you know, whatever is on TV and not care," and still get fed this disinformation.

So thank you all for your testimoneys.

Dr. Kagan, I want to ask you about disinformation and any advantages or disadvantages we have.

When we do Radio Free Europe, for instance, or Radio Free America, we tell the truth on that, and sometimes that truth is not pretty to our own system of governance. And telling the truth, I think, is the right thing.

But that can be a disadvantage when Vladimir Putin puts out disinformation. So, yes, it is true that Vladimir Putin is tiny in stature, for instance, right, that is something important to know, that he is stealing money from his people, getting that information out there.

But it is not true that Bashar al-Assad defends Christians and is the hero of Christian civilization, and Vladimir Putin is a defender of Christianity against radical Muslims, as we hear. He is just a violent man that wants power.

So when it comes to us countering with our own information, what are disadvantages and advantages we have, and how do we do that better? Because again, if you put a disinformation campaign against a true information campaign, the disinformation is going to be more powerful. But we do not want to get in the lying game, either. So how do we do that?

Mr. KAGAN. Well, Congressman, I think you put your finger on a big part of the advantage that we have, which is actually the truth favors us. He has to tell lies in order to make anything look good for himself.

He has an economy the size of Australia's, and it is not even a real economy. It is a kleptocracy, which is dysfunctional and which harms the Russian people. The Russian standard of living is dropping. Russian health is dropping. The demography is terrible. Russia is in a terrible, disastrous situation. That truth is an advantage for us.

We, on the other hand, are a vibrant, thriving society with the largest economy in the world and great freedoms and the ability to have a lot of civil discord. That is a tremendous advantage for us.

I think it comes down to how we tell our own story, and I think that we have been so focused on ripping each other apart that the message that we are sending to the world is that we are awful and that no one should copy us, no one should want to join us, no one should want to work with us. And I do not attribute that to any individual in government. I think it is across the board, the nature of our argumentation.

So I think our advantage is the story that we actually have to tell. The disadvantage is the nature of our discourse buries that story.

Mr. KINZINGER. Yes. Thank you for bringing that up.

I mean, I look at we have not done a good job of selling our side. We assumed we won the cold war and that was it was 100 agreed that this was the best way of life. We can put up a $40 trillion economy between the United States and Europe versus 1.6 or 1.7 trillion dollar economy of Russia. But that does not sell it because Vladimir Putin uses ethnic tensions now, and ethnic tensions actu-

ally are more compelling than saying you get a new iPhone or you get a little bit more money.

The reality is this is the best time to be alive. I mean, you have any information you want here. We are comfortable. The United States of America, at least, and most of Europe does not worry about an attack on a daily basis besides maybe a cyber attack. But yet we are more miserable than I think we have ever been in our life.

And I think getting our heads around what we have and what we are and projecting that is how we won the cold war. It was not necessarily a military buildup. It was an idea war. That is how we are going to defeat radical terrorism, by giving an idea war to show what possibility lays out there.

Ms. Aro, do you have anything to add to that? I only have 20 seconds left, but I want to give you a chance to add to the information side of that.

You are good. I like that.

All right. Well, with that, Mr. Chairman, I will yield back.

Mr. KEATING. Thank you.

The chair recognizes the gentlewoman from Pennsylvania, Ms. Wild.

Ms. WILD. Thank you very much, Mr. Chair.

Ambassador, I would like to direct my first question to you, and that is relative to the disinformation campaign that we know that took place here in the United States in 2016. And of course, we are coming up on a very important election again next year.

In your view, what kind of Russian influence operations are currently operating in the United States?

Mr. FRIED. I think the Russian disinformation tactics are beginning to shift from ads and bots over to manipulated organic content and maybe in the direction of deepfake, artificial intelligence.

And I mean by that that instead of making up stuff and posting it under an impersonation account, they are going to take genuine U.S. posts, blogs, tweets from radical groups, right, left, does not matter, and they are going to amplify them, and then use their sophisticated trolls to slip into that radicalized conversation and try to play both sides of an issue, the better to stimulate social tensions.

Now, we do not have to search far. The Soviets used to do that, but they did it analog. It took weeks. Now it is done in minutes.

But I think we are going toward manipulation of organic content rather than wholesale fabrication and then use of artificial intelligence, spreading around deepfakes. I think that is the cutting issue more than bots and ads.

Ms. WILD. And do you have any sense of how the U.S. Government should work to guard against that kind of interference?

Mr. FRIED. Several levels.

First, working to expose it. Sunlight is the great disinfectant. One of the great success stories of counter-disinformation was the French elections where European and American civil society groups exposed what the Russians were up to, and then the story became in France not what was stolen, not the stolen files and disseminated nasty information about the Macron campaign, but the fact

of the Russian campaign. That was a successful example of turning back disinformation.

So expose it, and then start working with social media companies so they stop acting as purveyors, unwitting purveyors of Russian intelligence operations. They are past denial of the problem; I will give them that. I think they want to be part of the solution, but they are going to need various forms of persuasion.

And I was skeptical about regulation when I started looking at this issue before, but I think it is coming, and I think it probably should. I think that we and the Europeans ought to be working together to develop common standards. The democratic world, the free world needs to develop a common approach to this, and I think it can be done.

Ms. WILD. And do you believe that the deterioration of our relationship with our allies adversely affects that kind of cooperation?

Mr. FRIED. It makes it a lot harder. Why on earth are we spending our political capital making theoretical fights against the European Union which was our idea in the first place? That is—pardon me—but that is nuts.

They are our closest democratic partner. We together, we and the Europeans, form the core of the free world. Sure, the EU can be difficult to deal with. Well, so can the American government. That is irrelevant.

We have a similar set of assumptions. We have a similar problem. The Finns, the Balts, the Poles, the Ukrainians, they have been telling us about this for years. Now we are in a position to listen. We ought to be working, making common cause with the Europeans.

And the solution set of issues is not going to be that hard to find. There are problems in this world that are genuinely somewhere between difficult and impossible. This is not one of them. This is fixable.

Ms. WILD. Ms. Aro, did you want to add something to that?

Ms. ARO. Yes, please, about the kinds and types of disinformation campaigns targeted to the United States.

There was last year a really interesting university research in which the researchers found that the Russian troll accounts on Twitter, which had previously been pushing pro-Russian and pro-Trump messages, they have started to push anti-vaccination messages to America, and you can just imagine the outcome of that.

Ms. WILD. Yes. Thank you so much.

I am out of time. I yield back.

Mr. KEATING. Thank you.

The chair recognizes the gentlewoman from Missouri, the home of the Stanley Cup champions, and it pains me to say that, Mrs. Wagner.

Mrs. WAGNER. I thank the chairman. And you know I did not bring up the fact that my St. Louis Blues are, in fact, the NHL Cup winners, but over a certain Bruins team of Massachusetts. But very kind of you to acknowledge it, Mr. Chairman, very kind. And I thank you for organizing this hearing.

And I thank you to our witnesses.

Russia's capabilities in the information space cannot be underestimated. Russian disinformation activities run counter to our

U.S. values and our interests, and we must prioritize efforts to counter Russian information warfare in coordination with our transatlantic partners.

Mr. Kalensky, you mentioned Russia's attempts to, you said, launder information in order to obscure its source. What can the intelligence communities in the United States and Europe do to improve attribution, so to speak?

Mr. KALENSKY. I think for that, it is actually very useful if you have the first part of the four solutions I offered, and that is actually documenting the threat, because then you can always highlight that it was the Russian information space where the disinformation appeared.

I come from a country where we have quite a pro-Kremlin President, and when the attack in Salisbury happened, the Russians tried to spread multiple versions, often contradicting, about the story. You could see after the murder of Boris Nemtsov, after shooting down MH 17, and it was the same after Salisbury, you try to spread contradicting versions of events because the aim is not to persuade about one version, but precisely so, as Dr. Kagan said, so that you end up like say: I do not know where the truth is.

And one of the versions was that it was not only Russia who was the producer of novichok, the poison that was used there, but it was also Czech Republic. The Czech President was one of the first people to repeat that piece of disinformation. Suddenly you would see the Russian disinformation machine not saying it was us inventing the lie in the first place, but it was, as even the Czech President admitted, the Czechs produced novichok. The information was laundered.

You have to monitor the information space very accurately so that you can say that actually, no, it was the Russians who came with the lie in the first place, we know it, and whoever parrots it is just multiplying Russian lie and is playing a useful idiot for the Russian disinformation machine.

I think that is why we also need to be a bit more resolute in punishing the information aggressors. We have to call them out. We have to call out when someone acts as a useful idiot of Russian disinformation campaign and parrots its lies.

Mrs. WAGNER. Absolutely.

Dr. Kagan, I agree that the United States needs to develop new structures and strategies to identify, expose, and disrupt these hybrid operations. This must include coordination with our NATO allies. How should the U.S. approach the development of a coherent, NATO-based response to hybrid threats?

Mr. KAGAN. Thank you, ma'am.

It is important for us to do as much of this work as possible at the unclassified level and probably not in the intelligence community.

Mrs. WAGNER. Again, the sunlight, the transparency, needs to be seen by all.

Mr. KAGAN. Exactly. And as soon as you do it in the IC, then it is classified, and so forth.

Mrs. WAGNER. Right. Interesting.

Mr. KAGAN. In addition to that, if you are not aware of them, if you look into the restrictions on the IC's ability even to monitor

publicly available information, a lot of people would be surprised at how hard it is for the IC to do that.

So I think that this is something where governments need to facilitate interaction of civil society organizations. The computer algorithms to catch deepfakes are not going to be written by the government. They are being written by private industry, by individuals. The ability to track stories from one place to another, that is out there. It is a matter of encouraging the mobilization of civil society.

And then what the government needs to do is to be—and the governments need to do—is to coordinate on our responses to these things. So what are we going to try to accomplish?

We know that we have got the Russians cold on this, for example. Just pick any example you like. What are we going to do with that information to maximize the damage to the entire Russian disinformation campaign and to demonstrate to our own people that there is truth out there, that we can know what it is, and to defeat the "who knows" principle?

Mrs. WAGNER. Thank you. The IC part of this I think is very, very important.

Ms. Aro, in my very limited time, what lessons should Western governments draw from Finland's programs to improve media literacy and public awareness regarding disinformation and influence operation, ma'am?

Ms. ARO. Well, first and foremost, of course, everyone needs to make university education free for everyone as we have in Finland, but when that is not possible, then what was mentioned already before, the program of the Finnish Government, of training government officials to recognize and counter disinformation operations already at the very early stage, and 2014 has been a good example.

Also, journalistic community has started to train school kids on their free time. They just visit schools and tell what is facts and what is fiction and how you separate the two.

Mrs. WAGNER. You have got to find the truth. Yes. Absolutely. Well, thank you, and thank you for your courage.

Thank you all for being here today.

I have gone past my time. I yield back to the chair. Thank you.

Mr. KEATING. Thank you.

The chair recognizes the vice chair of the committee, the gentlewoman from Virginia, Ms. Spanberger.

Ms. SPANBERGER. Thank you very much for being here today.

My colleague Mrs. Wagner's comments raised for me this idea of recognizing what the real threat is. And so before I ask my question, Mr. Kalensky, from your testimony, you outline that researchers and journalists have identified pro-Kremlin disinformation campaigns have occurred in the following elections: Scottish independence referendum, Ukrainian elections, Bulgarian local elections in 2015, Dutch referendums, Brexit referendum, Austrian Presidential elections, Italian constitutional referendum, French elections in 2017, German elections in 2017, Catalan referendum, Czech Presidential elections, Italian parliamentary elections, Macedonian name referendum, Ukrainian Presidential elections, Slovakian Presidential elections, European Parliament elections. And you note that this list is likely not exhaustive.

I list through those because I think it is so vitally important that while we are focused on what has happened in the United States or some of the larger known efforts by the Russian Government to meddle in election and democracies, looking at that exhaustive list is incredibly important.

But I would like to ask a question focused on the European response and specifically the European Union's Rapid Alert System. It was developed this year to facilitate communication among members relating to disinformation campaigns in their countries in order to coordinate their responses. The RAS is based on open source information and will also draw upon insights from academia, fact checkers, online platforms, and international partners.

However, there are reports that have surfaced, including a recent article in The New York Times, that some countries are choosing not to participate and a number of potentially high profile alerts of Russia disinformation were not shared with the public or relevant organizations because of internal disagreement over the significance of this detected disinformation.

In your opinion, what tools does the European Union's Rapid Alert System utilize to combat disinformation, and what is your assessment of the effectiveness of these mechanisms?

Mr. KALENSKY. I am a bit worried that the Rapid Alert System looks a bit better on paper than in reality.

The European Union will always obviously praise the system in its public documents. It is the job of the communication experts there. But from my private conversations with government officials from various member State governments, I am a bit afraid that the system is not as effective as it probably should be. Most of the information there is actually from publicly available East StratCom documents and that the member States themselves are actually not putting in too much information.

So if we have a Rapid Alert System that does not produce any alerts, I am not sure whether it is really a rapid alert system.

I think what would really help would be if the system was made public, because then the journalists and the researchers and everybody could see what is being reported there and what is not being reported there. And I could ask my, you know, Czech authorities: How come you have not reported this case of Russian disinformation that even I know about?

If there is not this public pressure, and the system is nontransparent, I am a bit afraid that we can read basically anything in the public documents, but we have no way to check it.

And it is a bit of a paradox that part of the EU's anti-disinformation efforts is pushing the platforms to being more transparent, and yet this system for rapid alert is actually nontransparent and nonpublic.

Ms. SPANBERGER. And in an effort to provide greater transparency, what would be some of the actual changes to the system that you all would recommend if we were looking at a system like that, how it could be effective, or how it could be made more effective?

Mr. KALENSKY. I think we could learn from the best examples we have in Europe, and again, I will come back to Lithuania, the Lithuanian armed forces. STRATCOM has trained most of the impor-

tant stakeholders in the country, be it civil servants, government officials, but even local authorities.

So, for example, when the Lisa case, I referred to in the written testimony, when it appeared it was the mayor of a small town alerting the armed forces STRATCOM that something like this has happened. So we have to get to a phase where even a mayor of a small-sized city somewhere, you know, in Alabama or Missouri will be aware of what Russian disinformation is, what topics it exploits, what it tries to achieve.

So for that, the No. 2 solution I offered, raising the awareness about the threat, I think you can achieve that. If we would be able to see what is reported in the alert system, A, we would be alerted, which would be nice, and B, we would know what the authorities actually—I mean, where is the failure in their monitoring, what they do not see, and where we, for example, the civil society, what we can help them with.

Because, as Dr. Kagan mentioned, sometimes exhaustive monitoring tasks are not extremely easy sometimes. The civil society might be even quicker than the government because, yes, the civil society is younger people, more tech savvy, and they might fulfill this task better than the government.

Ms. SPANBERGER. And it is an interesting process where you create a circumstance where you are expecting people to be aware of it if they have the ability to report or they are looped into what the reports are.

Thank you all for your time today. I yield back.

Mr. KEATING. The chair recognizes the gentleman from Tennessee, Mr. Burchett.

Mr. BURCHETT. Thank you, Mr. Chairman, Ranking Member, and thank you all for being here.

I am interested to hear your all's take on how the EU and NATO can respond to these disinformation campaigns, and specifically what the abilities they have to push back are. Just all of you all. Remember, I have got 5 minutes. I know you all like to talk. If you all can kind just make sure everybody gets to answer because I have another question to followup with.

Mr. FRIED. NATO has set up a Center of Excellence to counter disinformation in Riga, and there is a NATO-EU hybrid center set up in Helsinki. So there is some institutional capacity already existing.

These centers can do two things. They can identify Russian disinformation operations and spread the word, hopefully more effectively than the EU system, but they may get up—I am hopeful that the EU system gets up to speed.

Second, they can start targeting Russian bad actors. And when I know who the bad actors are, there are various ways we can go after them, including, by the way, through sanctions. So there is the beginning of an institutional capability.

But if I had one wish, you know, a magic wand loaded with one wish, it would be transparency and the ability to expose in real time Russian disinformation ops.

Mr. KALENSKY. What you can see in the EU and in NATO, it is definitely some of the documenting of the threat and some raising the awareness about the threat. You could see it there.

I would like to see more of punishing of the information aggressors. I think we should sanction more of the Russian so-called journalists because they are not journalists, they are just part of the Russian Army. And I find it horrific that you have a person called Vladimir Solovyov, he has a show two or three evenings per week. He uses it to spread hatred against the West in general or against its countries in particular.

Mr. BURCHETT. Is he on CNN?

Mr. KALENSKY. Unfortunately, no.

Mr. BURCHETT. OK. I was just throwing that out.

Mr. KALENSKY. And after the show, he sits on the plane and he enjoys his villas at Lago di Como.

I do not think we should allow those who are trying to——

Mr. BURCHETT. Say that last sentence again. You lost me. I am from east Tennessee. You are going to have to slow it down.

Mr. KALENSKY. Lago di Como. That is an Italian lake, a very, very nice resort, a very nice touristic area.

We should also sanction the companies. When you have a look at the list of advertisers on Russian State TV, you would see a lot of Western companies even in the highest positions. This quote ascribed to Vladimir Lenin said: Capitalists will sell us the rope with which we will hang them.

This is precisely what the Western companies are currently doing, those Western companies that are buying advertisement time on Russian TV. They are actually paying for destroying the West.

Mr. BURCHETT. OK. One other question.

Ma'am, maybe you would—tell me how you say your last name.

Ms. ARO. Aro.

Mr. BURCHETT. Aro? All right. You say it a lot better than I do.

In your view, what are the most vulnerable European States to Russian disinformation campaigns? And what do you project to be the next electoral target?

Ms. ARO. Well, I would say Balkans, which were already mentioned here, because many of these countries are—for example, Serbia is very fully engaged with different types of Russian projects. For example, they do military operations. And the Russian disinformation really much wants to tie them even more tightly together with Russian Federation.

So they also have a lot of pro-Russian propaganda media, which other so-called traditional, normal, neutral journalists also follow and called for stories.

So I would be really careful in addressing those regions, just like mentioned here before.

Mr. BURCHETT. Yes, sir?

Mr. KALENSKY. In 2016, there was an article in Frankfurter Allgemeine Zeitung in Germany, and the author said they got hold of a document that the Bundesnachrichtendienst, the domestic secret service, acquired, a document created for the Kremlin, ranking the European member States, European Union member States, according to their vulnerability to Russian propaganda. And the first three were countries on this list were Austria, Hungary, and Czech Republic.

So that is for the most vulnerable countries. At the end of this list were the Nordic countries.

Mr. BURCHETT. I am out of time. But if you all ever hear about them messing in the Second congressional District in Tennessee, I would sure like to know.

Thank you all very much you.

Mr. Chairman, I yield back to you, Brother. Thank you again.

Mr. KEATING. Well, thank you.

The chair recognizes the gentlewoman from Nevada, Ms. Titus.

Ms. TITUS. Well, thank you, Mr. Chairman.

Thank all of you for being here.

In addition to this committee, I serve on the House Democracy Partnership where we partner with legislatures in other countries with budding democracies, and a lot of those are in pretty hostile neighborhoods.

Just this morning, we had a panel talking about some of the threats that authoritarianism is kind of posing for new democracies. Three of the countries there were Georgia, Ukraine, and North Macedonia. So you know they have been dealing with this for a long time.

You have talked about some of the successes that we have seen Russia have. I would like to talk about some of the failures and see what we can learn from there.

They tried messing in the election in Greece and in Macedonia over the name change to try to prevent Macedonia from moving forward with the NATO accession. They failed there. They failed perhaps in the French election last time around.

What can we learn from where they failed? And is it legislative? Is it policy? Is it a difference in the media structure? And if it is the latter, what can we do maybe to try to change things here?

Anybody? Everybody?

Mr. FRIED. The common element of the successes you cited was exposure of Russian disinformation campaigns in real time, and then the national media understanding the importance of talking about that, rather than the message the Russians were trying to push.

This was successfully used in France, Greece. I think that the Germans turned back some disinformation operations that the Russians tried, trying to stir up anti-immigrant sentiment. That is the first piece, expose it and disseminate the exposure.

The second piece is longer term. It is to get societies to be more sophisticated about what they read. And that takes time, though, that is a generation. And we need to act in the here and now.

Ms. TITUS. And how can we possibly do that when people do not read anymore? Students do not read. They do not write. Everything comes out in 40 characters. Is this just a challenge to our whole educational system?

Mr. KAGAN. I think the issue is it does not matter whether we are teaching them how to read or not. It is a question of teaching people how to process information that they are receiving. It does not—the medium does not matter. And, in fact, in many respects, I am less worried—like many others—I am less worried about what they are doing in the text space than I am about deepfakes and

various other things, because it is well documented that images are much more powerful.

And talking someone around from a text story that they have read is a lot easier than getting an image—something that is taken in by an image, even if it is known to be fake.

And so there is a larger issue here that really has nothing to do with the deplorable fact, and I agree with you, that people do not read anymore, but that really comes to how do we process and receive information that is presented to us in any form.

Mr. FRIED. I agree with that. And I would add that, therefore, the social media companies need to act—they need to up their game and not be used as the conveyer belts for what I think will be the future in disinformation ops, which is lurid, provocative, completely phony visual posts, videos of speeches that look like Donald Trump or Elizabeth Warren but are not, that are completely fabricated.

Ms. TITUS. Or slowing down Speaker Pelosi's words?

Mr. FRIED. That was not an even good example. A good example is going to be something that looks exactly like a candidate, sounds like them, sounds like the kind of thing they could say, but is 100 percent fabricated. That could be disseminated within minutes, and social media companies that—the regulatory framework that I am thinking about would require social media companies to have a check, especially when they discover that there is a foreign connection, which often is going to be technically feasible.

Now, I do not want to drive it into the weeds. But you are asking exactly the right question.

Ms. TITUS. Thank you.

Ms. ARO.

Ms. ARO. I would like to contribute to listing the failures of the Kremlin. The Russian agents who operated here really widely in 2016, without any foreign agent registration in place, and tried to repel the Global Magnitsky Act, as well as smear Bill Browder, the human rights promoter and businessman, but they failed and basically ended up in the Mueller and other types of investigations. So that was one epic fail.

Ms. TITUS. Thank you.

Thank you, Mr. Chairman.

Mr. KEATING. Thank you.

I know that Ambassador Fried might be leaving in a few minutes. So when you do, we will take no offense. Hold in there until you can.

And the chair recognizes the gentleman from South Carolina, Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman. And thank you for this hearing on Russian disinformation.

I and my sons, daughter-in-laws, and grandchildren, have visited Russia a number of times. It is so impressive, the people, the beautiful countryside, the architecture, the literature, the art. That is why it is so sad, that Putin's abuse of such talented people, with a corrupt elite, is so sad.

My first visit was actually to Moscow in 1990. It was the last year of the Soviet empire. And it was really inspiring to see the

empire disappear, to be replaced by hopefully a more modern society, but that did not necessarily occur.

And then I had the opportunity, with the National Endowment for Democracy, to lecture to different youth groups across Siberia. And it was incredible to appear as we, on an expressway, came to Novosibirsk, and there was a sign in English welcoming everyone to the Chicago of Siberia.

And then I had the opportunity to lead a delegation to St. Petersburg to place a wreath at the cemetery, on behalf of the American people, to show our love and affection for the hundreds of thousands of people in the mass grave who had been murdered by the Nazi siege.

And so, again, see what an extraordinary city, St. Petersburg. And then I was grateful to participate with Mayor Bob Coble of Columbia, South Carolina, to visit Chelyabinsk, Russia, which is the sister city of Columbia, South Carolina.

And so you would not anticipate all of this, but the reason I review these associations is because my view is that the American people are not anti-Russian, but they certainly hope the best for the citizens of Russia for a positive change.

With all of this in mind, Dr. Kagan, Ambassador Fried, in your view, what are the most vulnerable European States to Russian disinformation?

Mr. FRIED. Ukraine used to be, but in a possible other epic Russian failure, Ukrainian patriotism has crystallized in a pro-Western, pro-American direction, which otherwise might not have been possible. Nevertheless, they are vulnerable because they are under attack.

I think Hungary, Czech Republic are vulnerable for the reasons that Mr. Kalensky mentioned. I think Poland less so. I think Serbia is still vulnerable to Russian disinformation operations. The legacy of the NATO operations and break-up of Yugoslavia weighs heavily.

But we have also found that countries you would not expect to be vulnerable to Russian disinformation ops have had them in their countries. Spain, around the Catalonia referendum; the U.K. as it turns out, with Brexit. And we do not know where the Russians are going to pop up. But the countries I mentioned come to mind.

Mr. WILSON. Dr. Kagan.

Mr. KAGAN. I agree with the list of vulnerabilities. I would like to put a couple of other countries on the list. The issue is a little less how vulnerable they might be than how desirable a target they are to the Russians.

We have not spoken about Moldova, but Moldova is in the midst of a major political crisis at the moment, and where it ultimately lands on the pro-Russia or pro-West trajectory is very much up in the air. The Russians are playing massively in that space. Virtually no one in the West is paying any attention at all. And it matters a lot for all sorts of reasons, including there is still a Russian military presence in Moldova held over from the Soviet days.

Latvia is very concerning to me, not because I think that the Latvians themselves are vulnerable, but the Russian minority in Latvia is vulnerable to manipulation. And as part of a hybrid war approach, that could be an immediate problem, huge problem for

NATO. I am very concerned about Latvia in particular among the Baltic States, although they are all at risk.

Even Belarus. We do not really imagine Belarus as ever being in play, because it is so much in the Russian orbit. But there is a gambit that Putin seems to be engaged in to try to warp Belarus so fully back into the Russian orbit that it basically recreates a single State of the two entities.

And the Russia team at the Institute for the Study of War has actually hypothesized that that is potentially one way in which he could imagine dealing with a constitutional problem he has as his term ends, ostensibly without ability to run again, he could theoretically make himself President of this new organization. And there is a weird degree of small, little pushback in Belarus against this, which might be worth paying attention to.

And in two countries, which in principle are not hugely vulnerable, but I think will be massive targets, are Germany, because the question of who succeeds Angela Merkel will determine the fate of Europe, if you want to really be hyperbolic about it. But it is not all that hyperbolic; it really matters a lot. And so I see that Putin will for sure be all over that.

And the U.K. The opportunities to continue to sow discord and advance nationalist agendas, look at the Irish question, various other things, there are a lot of opportunities there that I think Putin will be aggressive about taking advantage of.

Mr. WILSON. Thank you very much. And we appreciate you and your wife.

Thank you very much.

Mr. KEATING. The chair recognizes the ranking member for any closing statement you might have.

Mr. KINZINGER. I have no closing statement except to thank again the witnesses for being here and all your great work. And hopefully we can all together, you know, do something of action instead of just talking.

So thank you very much for being here.

Mr. KEATING. I also want to thank you. It was tremendous testimony, important testimony, not only for our allies in Europe, but for lessons learned that we should take home here.

We certainly learned that from the top down, from the President, as Ambassador Fried said, we need clarity, focus, no ambiguity whatsoever. We are under attack. Our intelligence community has been clear. Experience in Europe has taught us that.

We have to organize better in this country. There has been testimony about how to centralize this effort into one agency. We are fragmented, frankly. Whether it is Homeland Security, whether it is our intelligence groups and agencies, there should be, I believe—and I think it was great testimony—a greater central focus on this.

And we need a strong political will as well. And that means, to the extent that we can, less infighting among our parties and among different views within our own parties.

I think it is important and it has been emphasized how difficult but important social media is from the private side to engage in this, as well as a free and vibrant press, free from intimidation and threats. And making sure they are backed up in that regard.

In the absence of all of this, I agree with Ambassador Fried, and some of you, there could be results in more sanctions, to put teeth into our actions, and reluctantly in the difficult task of regulation.

So these are all things that we have to consider.

In this closing statement, I have recognized one more member who has come. And, if we could, we will recognize Mr. Costa from California for 5 minutes to conclude this hearing.

Thank you.

Mr. COSTA. Thank you very much, Mr. Chairman.

And this was an important hearing with some very good witnesses. And I appreciated very much getting their insight on what is continuing to be a very vexing issue with the Russians' interference not only in our elections, but in Europe, what is obviously part of a comprehensive effort that Putin and his team have been planning on for Western democracies.

To what extent on the Russian disinformation that we have discussed here this afternoon draw upon and amplify on anti-Semitism and other forms of prejudices, in your view?

Mr. KALENSKY. As I was trying to describe in the written testimony, it is always about finding the most pulsating weakness that the particular, that the given audience might have. And in some audiences, it might be anti-Semitism. So, yes, in some audiences you would find that the anti-Semitic remarks are being played.

If I am not mistaken, it was nice research by Kate Starbird from University of Washington in Seattle, where she was looking at which accounts and which sites were pushing the lies about White Helmets. And she found out that very often they were obviously pro-Russian, or almost in all cases.

But she even found out that you would find there aggressively pro-Zionistic websites, but also aggressively anti-Semitic websites. So it is always about playing both parts of the extreme, because if you manage to play both parts of the extreme, you will have a more polarized discussion, more hysterical, less rational. And less rational people are more vulnerable to disinformation.

Mr. COSTA. Well, and you are playing upon the populism and the nationalism that is taking place not only in this country, but in Europe as well. And a lot of that deals with not only the misinformation that is rampant, but also the fact that a lot of people are relying on social media to get their information, which I think is part of the problem when we look at the totality of what we are dealing with here.

Mr. KALENSKY. Sometimes. But, you know, sometimes I have a feeling, especially here in the United States, that the importance of social media is a bit overemphasized.

And, for example, in the country where I come from, you have a huge group that is not present on social media, and yet they consume heavily polarized and disinformation messages, for example, via chain emails. And you would really have half of Europe and half of Europe's pensioners consuming information via this channel. They are not on Twitter, they are not on Facebook, and they do not turn on the TV news because everybody is lying.

Mr. COSTA. Yes. Well, has there been any, either among either of you or with other efforts that we are trying to get a handle on this, a collection of information that tries to measure to what suc-

cess these disinformation campaigns have had success in elections or the impacts of these campaigns? And how much evidence do we have regarding the Russian efforts on the spread of disinformation like in the Brexit vote?

Mr. KALENSKY. That is, again, part of the trouble. We do not actually research this enough. There are not enough people focusing on the topic.

I am aware of——

Mr. COSTA. Would that be something that you think that this committee should look at in a separate piece of legislation of trying to collect and gather that data, that information?

Mr. KALENSKY. I believe——

Mr. COSTA. Yes, if you would like to respond, please.

Ms. ARO. I am sorry.

Yes, definitely. I also proposed in my written statement that because part of the problem is really that we do not even—at the moment, we do not even know what kind of operations we are targeted to. We might know in 2 years, when someone starts to really investigate them. But we should address and counter these operations while they are ongoing, because they take effect like that.

Mr. COSTA. So, Mr. Chairman, this is something that I think we should try to look into, I mean, to measure this. We have all of this work, and we should probably sit down with you folks to get that.

Finally, my time is expiring, but I guess the—as chairman of the Transatlantic Legislators' Dialogue, I know our European colleagues are as concerned about this as we are. And to what effect do you think that they had on the most recent parliamentary elections that just finished in May in the EU? Do we have any idea?

Mr. KALENSKY. How impactful were the operations?

Mr. COSTA. Yes.

Mr. KALENSKY. Unfortunately, again, we do not have the measure. So what we saw, for example, from the data of the East StratCom Task Force, the team where I used to work, their numbers show that the amount of disinformation cases in 2019, before the elections, has actually doubled compared to the same period in 2018. There were two times more disinformation cases that the StratCom unit has identified.

So you would see that there was probably more—more of disinformation, more disinformation messages. But measuring the impact, this is unfortunately a thing that not too many government agencies are doing, as far as I know.

For example, I know about a very nice book by Professor Kathleen Hall Jamieson from University of Pennsylvania about cyber war and about the effect that the Russian disinformation operations had on the U.S. elections. Unfortunately, you would not see that many investigations in Europe.

Mr. COSTA. Well, Mr. Chairman, my time has run out. I want to thank you for calling this hearing. And maybe this is something that, with your subcommittee, we could work together with our European counterparts to really take a deep dive in trying to measure what really is taking place, both here and Europe, in a way in which we could use it to protect ourselves from further elections—in future elections.

Mr. KEATING. Great. Thank you. This will be a continuation of those efforts.

I am just reminded as we close that Russia and the things that they have done, these attacks, are like bullies. And many times bullies cannot build themselves up. If they cannot stand on their own success and merits, they have to tear others down.

And that is what is happening with the Russian leadership. It is certainly not the case with the Russian people.

I believe that today's hearing, I hope, will help the U.S. and the West work together and make sure that we realize this threat and that we address it as successfully as we can. And that means working together to address that threat.

So I want to thank you for a very important hearing, and we will continue on this together.

With that, I adjourn the hearing.

[Whereupon, at 3:54 p.m., the subcommittee was adjourned.]

APPENDIX

SUBCOMMITTEE HEARING NOTICE
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515-6128

Subcommittee on Europe, Eurasia, Energy, and the Environment

William R. Keating (D-MA), Chairman

July 16, 2019

TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS

You are respectfully requested to attend an OPEN hearing of the Committee on Foreign Affairs, to be held by the Subcommittee on Europe, Eurasia, Energy, and the Environment in Room 2172 of the Rayburn House Office Building (and available live on the Committee website at https://foreignaffairs.house.gov/):

DATE: Tuesday, July 16, 2019

TIME: 2:00 pm

SUBJECT: Russian Disinformation Attacks on Elections: Lessons from Europe

WITNESS: The Honorable Daniel Fried
Distinguished Fellow
Future Europe Initiative and Eurasia Center
Atlantic Council
(Former State Department Coordinator for Sanctions Policy, Former Assistant Secretary of State for European and Eurasian Affairs, and Former United States Ambassador to Poland)

Ms. Jessikka Aro
Investigative Reporter
Yle Kioski

Mr. Jakub Kalenský
Senior Fellow, Eurasia Center
Atlantic Council

Frederick W. Kagan, Ph.D.
Resident Scholar and Director
Critical Threats Project
American Enterprise Institute

By Direction of the Chairman

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF SUBCOMMITTEE ON *Europe, Eurasia, Energy, and the Environment* HEARING

Day *Tuesday* **Date** *July 16th* **Room** *2172*

Starting Time *2:22* **Ending Time** *3:55*

Recesses ____ (____to____) (____to____) (____to____) (____to____) (____to____) (____to____)

Presiding Member(s)

Keating

Check all of the following that apply:

Open Session ☑
Executive (closed) Session ☐
Televised ☑

Electronically Recorded (taped) ☑
Stenographic Record ☑

TITLE OF HEARING:

Russian Disinformation Attacks on Elections: Lessons from Europe

SUBCOMMITTEE MEMBERS PRESENT:

See Attached

NON-SUBCOMMITTEE MEMBERS PRESENT: *(Mark with an * if they are not members of full committee.)*

HEARING WITNESSES: Same as meeting notice attached? Yes ☑ **No** ☐
(If "no", please list below and include title, agency, department, or organization.)

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*

Ambassador Daniel Fried's Testimony
Ms. Jessikka Aro's Testimony
Mr. Jakub Kalenský's Testimony
Dr. Frederick W. Kagan's Testimony

TIME SCHEDULED TO RECONVENE _____
or
TIME ADJOURNED *3:55*

Subcommittee Staff Associate

HOUSE COMMITTEE ON FOREIGN AFFAIRS

EUROPE, EURASIA, ENERGY, AND THE ENVIRONMENT SUBCOMMITTEE HEARING

PRESENT	*MEMBER*
X	William Keating, MA
X	Abigail Spanberger, VA
	Gregory W. Meeks, NY
	Albio Sires, NJ
	Theodore E. Deutch, FL
	David Cicilline, RI
X	Joaquin Castro, TX
X	Dina Titus, NV
X	Susan Wild, PA
	David Trone, MD
X	Jim Costa, CA
X	Vicente Gonzalez, TX

PRESENT	*MEMBER*
X	Adam Kinzinger,IL
X	Joe Wilson, SC
X	Ann Wagner, MO
	James F. Sensenbrenner, Jr., WI
X	Francis Rooney, FL
	Brian K. Fitzpatrick, PA
X	Greg Pence, IN
	Ron Wright, TX
X	Michael Guest, MS
X	Tim Burchett, TN

○