UNDERMINING DEMOCRACY: KREMLIN TOOLS OF MALIGN POLITICAL INFLUENCE

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

May 21, 2019

Serial No. 116–41

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
36–426PDF 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

UNDERMINING DEMOCRACY: KREMLIN TOOLS OF MALIGN POLITICAL INFLUENCE

Tuesday, May 21, 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 10:04 a.m., in room 2172 Rayburn House Office Building, Hon. William Keating (chairman of the subcommittee) presiding.

Mr. KEATING. This hearing will come to order. The subcommittee is meeting today to hear testimony on "Undermining Democracy: Kremlin Tools of Malign Political Influence."

Without objection, all members have 5 days to submit statements and questions, extraneous materials, and the like for the record subject to the length limitation in the rules.

I will now make an opening statement and turn it over to the ranking member for his opening statement. But I would like to ask, without objection, unanimous consent that my remarks might be extended a bit because we are going to show a film—a short film, 2 and a half minute film—that I think will shed some light on what we are discussing today.

I would like to welcome you all to the hearing on Russia and, specifically, the Kremlin's tools of political influence around the world.

Much of our work so far in the subcommittee is focused on our need as the United States to remain a leader in standing up for democracy, human rights, and the rule of law, and the importance of working together with our allies who share our commitment to these ideals.

Today, we continue along that vein and have before us expert witnesses who will explain how Putin's Russia undermines democratic processes and institutions around the world through various means such as illicit finance, so-called dark money, and corruption.

It is interesting that, as was focused on military aggression in places like Georgia and Ukraine and we are focused on cyber threats, the idea of the corrupt influence operation, as Dr. Carpenter so called it, hasn't received the same attention.

But it is so important in realizing what's going on in the threats to our democracy, particularly by Russia. So these issues are among other inventions that are attempts to weaken public discourse around elections and affect their results.

We ourselves have experience with this. Russia intervened in our elections in 2016. With greater awareness now after this experience, officials from European and EU elections have been vigilant

working to protect their electoral systems and monitor for attempts at undermining their democracies.

More systemic ways, however, are used and using illicit financing and corruption to influence political actors and parties is one of them.

Just this weekend Austria's vice chancellor resigned after a shocking video was released seemingly showing him voluntarily engaging with an individual posing as a member—a family member—of a Russian oligarch to advance his far-right political party.

We are still learning about this video and the circumstances behind how this exchange came to occur. The Russian government has asserted that they have nothing to do with that.

We will hear from our witnesses in their testimony how Russia does use in instance agents that have that degree of separation. Whether that is the case here or not is to be determined. But it will be important to analyze this as one graphic way that this can be done.

The vice chancellor in question has apologized for aspects of his behavior and has resigned over the weekend, and the chancellor has called for snap elections to take place.

I do believe, though, that regardless of the unfolding details that this is an important glimpse for everyone who has been working on these issues into what kind of corruption occurs and what it could look like.

We have an excerpt of the video, and with unanimous consent we will play it for the subcommittee now. Just note that if you are watching it, Kronen refers to a prominent newspaper and Strabag is a major Austrian construction company.

So if we could queue this and take a few minutes—a couple of minutes to look at this film.

[Video is played.]

Mr. KEATING. This whole situation underscores two things in particular. First, that corruption around elections and political power is real. Whether this was a real transaction or whether anything would have come of it has not taken away yet, as the investigation continues.

But it does not take away from the fact that this video affirms what many experts have studied including those joining us today, that this kind of corruption happens.

It is more commonplace than I think we often would like to admit.

Second, that once we recognize Russian malign political influence around the world for the threat that it is, we have an opportunity here.

There were protests in Austria following the release of these tapes and there has been widespread condemnation of the elected officials' blatant willingness to sacrifice important democratic principles like fair competition, government accountability, and freedom of the press.

Sunlight is the greatest disinfectant. We need to support investigative journalism and transparency around campaign financing and always will be sure to protect civic space for free speech and association.

Whether it is a setup or actual Russian corruption transactions designed to affect internal governing or elections in a country, democracies, including the United States and our European allies, need to come together to expose corruption and illicit financing and work together to ensure that our democracies remain independent and free from malign foreign influence.

So I look forward to addressing these points in detail today and to hear from our witnesses on their work analyzing how the Kremlin uses various means, financial or otherwise, to undermine the stability of democracies around the world.

We will not only discuss the tools the Kremlin uses but also what can be done about it together with our allies. Sanctions are an important piece of this discussion.

I hope we discuss how we can strengthen our own financial systems and democratic institutions while also strengthening our public discourse and media literacy so that we are less vulnerable to these kind of attacks and interference.

With that, I now turn to the ranking member for his opening statement.

Mr. KINZINGER. Well, thank you, Mr. Chairman, and I thank this panel for joining us today. Obviously, the video was very disturbing and, hopefully, it serves as a warning into the future for anybody that would think to do likewise.

I do not believe any member in this room would deny the fact that Russia, led by Mr. Putin, is a destabilizing factor in this world. The Russians have developed an advanced set of tools to apply pressure on democracies around the world and they have shown their willingness to use it.

Whenever Putin attempts a new maneuver, he waits to see the international community's response, and when nothing happens he escalates.

One of the first tools developed and deployed by the Kremlin was to hide behind the guise of protecting ethnic Russians to invade Georgia and Ukraine.

While open hostilities between Russia and Georgia began in 2008, it was Putin's distribution of passports to Georgians earlier that laid the groundwork for Russian intervention.

In Ukraine, Putin claimed that ethnic Russians were being persecuted as a precursor for intervention. By using little green men instead of the Russian military, the Kremlin was able to deny any involvement in the invasion and occupation of Ukrainian territory.

Both Ukraine and Georgia have been stalwart allies of the United States since gaining their independence. Ensuring their territorial sovereignty of these two countries is essential to European security and to American interests.

When personal interests are at stake for Vladimir Putin and his allies, the Russians do not hesitate to utilize their forces to engage in international affairs.

In 2015, Bashar al-Assad was losing control of Syria. He requested assistance from the Kremlin, who were more than willing and dutifully bound to protect—help protect their naval base in Syria.

In exchange for Russian air power, Assad granted Putin a 50-year lease to the airbase, the same location where they have

launched waves of attacks on civilian centers and hospitals, killing thousands of men, women, and children, which continues to this day.

It is not just in Europe or the Middle East where Russia is attempting to exert their influence. Earlier this year we saw the Kremlin provide Nicolas Maduro with soldiers to protect Russian investment in Venezuelan energy sector and provoke the United States by getting involved in our hemisphere.

The Russian Federation has long used energy as a weapon to coerce, manipulate, and create conflict around the world. One of my growing concerns is how European and Eurasian countries have become reliant on Russian gas and oil without a domestic backup.

Though almost completed—through the almost completed Nord Stream II pipeline project, Russia will soon control our European allies' energy markets.

That is why I introduced H.R. 1616, the European Energy Security and Diversification Act with Chairman Keating. This legislation would help our partners defend themselves from the malign activities of Russia by developing and diversifying their own energy sources.

I hope our Senate colleagues can pick this up and pass it quickly. While hindsight is 20/20, we must be able to learn from our mistakes and adapt.

Prior to the 2016 elections Russia engaged in one of the most sophisticated information operations to date against the United States.

This past February the Russians tried to halt the democratic progress being made in Moldova by manipulating their elections.

As a result, the pro-Russian socialist party won 35 seats in the election while the pro-Western democratic party won 30.

We must remain vigilant and I have no doubt that Russia will continue to do similar attacks on democracies, going forward. Just this week the EU will be holding their parliamentary elections.

The Russians will look at every possible avenue to sow discord and division across the continent to further strain democracy in Europe. It further shows us why the topic of this hearing is so important.

I look forward to hearing from our witnesses about Russia's malign activities today and how the United States can best defend itself and go on the offense against them, and one of the things I think is extremely important is simply exposing Russian tactics to be able to disinfect against them.

If you are looking at Twitter or Facebook or social media and you see a story that looks crazy, it probably is. It is probably not true and, unfortunately, we live in a moment where people automatically accept the narrative that they are predisposed to instead of thinking critically about if this a disinformation campaign.

So, again, I thank the chairman for calling this important hearing. I thank the witnesses for being here and I yield back the balance of my time.

Mr. KEATING. I would like to thank the ranking member for his comments and I would like to thank our witnesses, an extraordinary group of witnesses here on the panel on the subject matter, and I will introduce them in order.

Dr. Michael Carpenter is a senior director at the Penn Biden Center for Diplomacy and Global Engagement, and a nonresident senior fellow at the Atlantic Council.

He previously served in the Pentagon as deputy assistant secretary of defense with responsibility for Russia, Ukraine, Eurasia, the Balkans, and conventional arms control.

He also served in the White House as a foreign policy advisor for Vice President Joe Biden as well as on the National Security Council as the director for Russia.

Laura Rosenberger is a director of the Alliance for Securing Democracy and senior fellow at the German Marshall Fund of the United States.

Prior to that, she served at the State Department and the National Security Council.

Heather Conley is a senior vice president for Europe, Eurasia, and the Arctic, and director of the Europe Program for the Center for Strategic and International Studies. Ms. Conley previously served as the deputy assistant secretary at the Department of State's Bureau of European and Eurasian Affairs.

Peter Doran is the president and CEO of the Center for European Policy Analysis and served as a Foreign Affairs fellow in Congress and as a George C. Marshall fellow at the Heritage Foundation.

I appreciate all of you being here. I look forward to this testimony. Please limit your testimony as best you can within the 5-minute arena and without objection your prepared written statements will be made part of the record.

I will now go to Dr. Carpenter for his statement.

STATEMENT OF MR. CARPENTER, PH.D., SENIOR DIRECTOR, PENN BIDEN CENTER FOR DIPLOMACY AND GLOBAL ENGAGEMENT, FORMER DEPUTY ASSISTANT SECRETARY OF DEFENSE WITH RESPONSIBILITY FOR RUSSIA, UKRAINE, EURASIA, THE BALKANS, AND CONVENTIONAL ARMS CONTROL

Mr. CARPENTER. Chairman Keating, Ranking Member Kinzinger, and distinguished members of the committee, thank you very much for this opportunity to testify today on the subject of the Kremlin's tools of malign political influence.

I also could not imagine three better co-witnesses to be here on the stage with me.

Today Russia is doubling down on malign influence operations across Europe and North America. But we remain unprepared, underfunded, and often ignorant of the threat.

Furthermore, it is not just Russia but also China and other State and nonState actors whose influence and destabilization operations pose a threat to our democracy.

To deal with this threat we urgently need to focus more resources on rooting out Russia's malign networks, addressing our own massive vulnerabilities, especially to foreign dark money, and imposing greater costs on Russia when the Kremlin is caught interfering in our democratic process.

Russia's subversive attacks on our democracy can be grouped into three main categories: cyber operations, information warfare, and corrupt influence operations.

Today, I will focus on influence operations or what in Russian intelligence jargon are called active measures. Active measures are occurring with increasing frequency. I will not review all the cases cited in my written testimony but a few examples should suffice to give a flavor for what we are dealing with.

In Lithuania in 2004, a Russian oligarch contributed $400,000 to the campaign of a Presidential candidate who won the election but was later impeached and removed from office by the Lithuanian parliament after it was shown that the oligarch had improperly been given Lithuanian citizenship.

In France in 2014, far-right Presidential candidate Marine Le Pen received a 9 million euro loan from a bank owned by a Russian oligarch.

In the Netherlands in 2015, Russian proxies posing as Ukrainians tried to sway a referendum against Ukraine's free trade agreement with the EU.

In the U.K., Brexit's biggest financial backer had numerous meetings with Russian embassy officials and businessmen who offered attractive investment opportunities.

In the Central African Republic, Libya, Sudan, Madagascar, Syria, and Venezuela, Russian private contractors provide services ranging from personal security to election support in return for access and money.

Russia's State-owned enterprises—Rosneft, Gazprom, Rosatom, et cetera—regularly offer foreign government officials preferential deals in return for influence.

In Montenegro, Russia's military intelligence service, the GRU, crossed the line from influence to destabilization operations when it tried to foment a violent coup d'etat against the country's prime minister in October 2016.

Similarly, in Greece a former Duma member and billionaire oligarch personally funded violent protests against a historic agreement between Greece and North Macedonia that paved the way for the latter country to join NATO.

All of these operations are funded through a financial ecosystem that makes use of laundered money. The Panama Papers and other sources have showed how offshore networks of shell companies and shady financial institutions have enabled Russian oligarchs, officials, and organized crime syndicates to launder billions of dollars into Western financial institutions.

So the question is how do we stop Russian malign influence. I would group our responses into three buckets of measures: law enforcement, legislative, and cost imposition.

First, we need to root out illicit Russian networks. To do this, we need better coordination between our domestic law enforcement agencies and our national security apparatus.

Too often one hand does not know what the other is doing. A standing interagency task force on malign Russian influence chaired by an NSC senior director would help address this problem.

Second, we urgently need to address our own vulnerabilities by closing crucial gaps in governance. The most important is our cam-

paign finance system, which is so opaque that we do not even have an inkling how much foreign dark money is sloshing around the system.

Legislation to identify the beneficial owners of limited liability companies is also necessary and urgent since shell companies are often used to mask illicit financial transactions.

Stricter anti-money laundering regulations are needed to tighten illicit financial flows and more transparency is needed for high-end real estate transactions.

This also means more resources are needed for the Treasury Department's Financial Crimes Enforcement Network.

Finally, law firms need to be subjected to greater transparency so that attorney-client privilege cannot be used as a loophole through which foreign entities channel illicit funds to U.S. legal representatives.

A number of bills have been drafted to address these vulnerabilities, but none so far has been passed into law.

Finally, the third bucket of measures involves imposing greater costs on Russia for its interference in our democratic process. In my view, we need to consider much more forceful actions such as full blocking sanctions on select Russian banks.

It is time to recognize that trying to change Russia's behavior through "targeted sanctions" on this or that oligarch or official is not going to work.

It is time to impose real costs on Russia and we have the tools to do so.

Thank you for your time and I look forward to your questions.

[The prepared statement of Mr. Carpenter follows:]

Testimony for the
United States House of Representatives
Committee on Foreign Affairs
Subcommittee on Europe, Eurasia, Energy, and the Environment

May 21, 2019

"Undermining Democracy: Kremlin Tools of Malign Political Influence"

Dr. Michael Carpenter
Senior Director
Biden Center for Diplomacy and Global Engagement
University of Pennsylvania

Note: The statements, views, and policy recommendations expressed in this testimony reflects the opinions of the author alone, and do not necessarily reflect the positions of the Penn Biden Center for Diplomacy and Global Engagement or the University of Pennsylvania.

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 tools of malign political influence.

In my previous role as Deputy Assistant Secretary of Defense, I was the senior Pentagon official responsible for coordinating our defense policies and posture against Russia. It is my belief today that it is not Russian ICBMs or hypersonic vehicles that pose the greatest threat to our national security but rather Moscow's covert influence and destabilization operations.

In terms of hard power, the United States and its NATO allies retain a significant conventional military advantage over Russia and a credible nuclear deterrent that provides for strategic stability. In the area of covert political influence, however, not only have we failed to establish a credible deterrent for Russia's malign activities, but we are failing to address the vulnerabilities that are continuously being exploited by Russia, China and other state and non-state actors to undermine our democratic institutions. Russia's growing use of malign influence operations combined with our lack of pushback and failure to address crucial governance gaps is leading us into an era of dangerous strategic instability and possible escalation.

What is Russia trying to achieve through its malign influence? The Kremlin's chief geopolitical goals vis-à-vis the West are to weaken Western democracies, fragment the transatlantic community (to include NATO and the EU), and undermine international norms pertaining to the promotion of democracy and human rights. The Kremlin has concluded that only by going on the offense can it shore up its corrupt authoritarian regime against the influence of Western norms of democracy, transparency, and accountability. Ever since President Vladimir Putin's return to the Kremlin in May 2012 on the heels of an unprecedented wave of anti-regime protests, the Putin regime has taken a far more aggressive stance towards suppressing internal dissent at home and subverting Western democracies abroad. Indeed, these are two sides of the same coin since both are efforts to shield Russia's kleptocratic regime from democratic principles.

While the Kremlin has not hesitated to use military force to achieve its geopolitical goals, as was the case in Georgia in 2008 and Ukraine in 2014, it may now be recognizing (or at least some Kremlin strategists are) that even successful military action can result in strategic failure. Following Russia's military operations in

Georgia and Ukraine, both nations came to see the Kremlin as an implacable enemy. This is one of the reasons why President Putin has increasingly turned to covert influence operations or "active measures" (*aktivnyye meropriyatiya*) to achieve his geopolitical aims. The goal of such measures is to cripple or weaken an adversary without it even fully realizing it is under attack, or as the Chinese strategist Sun Tzu put it, "to subdue the enemy without fighting." Putin's various successes with covert action in the last five years show that such operations are not only more effective and cheaper, but they have also resulted in far fewer international repercussions than conventional military operations.

Active measures to undermine Western democracies can be grouped into three main categories: cyber operations, information warfare, and corrupt influence operations. Today I will focus my testimony on corrupt influence operations since these have received far less attention than cyber attacks or information warfare.

Unlike traditional espionage activity, whose aim is to gain access to state secrets or sensitive technologies, Russia's influence operations aim to shape and influence the target society, and especially its political class. The ultimate goal of these active measures campaigns is not just to change the target's behavior but to alter its perceptions of what constitutes a threat and who is an ally and an enemy. This is an intelligence officer's holy grail. As KGB defector Yuri Bezmenov put it, influence operations ultimately seek "to change the perception of reality of every American."[1] Or as Kremlin strategist Vladislav Surkov recently boasted to a Western audience, "Russia [seeks to interfere] in your brains, [to] change your conscience."[2]

Influence Campaigns

To fully appreciate how the Kremlin runs influence operations one has to first understand the nature of the informal networks that underpin Russia's political and economic system. In today's Russia, power is only sometimes wielded through formal institutions, positions, and offices. More often, though, it is wielded through

[1] Tomas Schuman (aka Yuri Bezmenov), *Love Letter to America* (Los Angeles: Almanac Panorama, 1984).
[2] Quoted in Cristina Maza, "Vladimir Putin's Advisor Tells Americans: 'Russia Interferes in Your Brains, We Change Your Conscience,'" *Newsweek*, February 12, 2019. https://www.newsweek.com/russia-president-vladimir-putin-election-americans-1327793.

personal connections to the key players who sit atop the neo-feudal network of patronage that defines the contemporary Russian polity. President Putin and a small circle of former KGB colleagues and friends sit at the apex of this network, and through a mix of bureaucratic power and personal ties they maintain influence or control over not just state institutions but also private companies, charities, and cultural and religious organizations. In this highly personalized and networked system of power, a modern-day "baron" like Igor Sechin, the chairman of Rosneft, can even order the arrest of a cabinet official like Economic Development Minister Alexei Ulyukayev.[3] Personal connections are what count, not official positions.

Russia's influence operations abroad are essentially efforts to extend this personalized system of influence beyond Russia's borders to Western political, media, business, and cultural elites. Although some of these operations are managed by Russia's intelligence services, they are just as often carried out by oligarchs, politicians, or even organized crime figures who have connections to the ruling elite. To maintain plausible deniability, Moscow in fact prefers to leverage non-official relationships wherever possible so as to avoid any direct connection to the Russian state. In the case of Maria Butina, for example, who was arrested by the FBI for conducting an influence operation here in the United States, Ms. Butina's lack of any formal bureaucratic role is far less significant than her personal ties to influential Russian officials such as former Senator and Deputy Central Bank Governor Alexander Torshin.[4] The same is true of Russian oligarch Pyotr Aven, who told Special Counsel Robert Mueller that he was given an "implicit directive" by President Putin to make inroads with the Trump transition team.

Russia uses similar methods to conduct influence operations in Europe. In 2004, Russian oligarch Yuri Borisov contributed $400,000 to the campaign of Lithuanian presidential candidate Rolandas Paksas. Shortly after Paksas was elected president, it was revealed that Borisov had received Lithuanian citizenship. Following a parliamentary inquiry, however, Paksas was impeached and removed from office. More recently, it was revealed that French far-right presidential candidate Marine

[3] Amy Knight, "A Show Trial in Moscow," *The New York Review of Books*, September 8, 2017. https://www.nybooks.com/daily/2017/09/08/a-show-trial-in-moscow/.

[4] United States District Court for the District of Columbia, "AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT." https://www.justice.gov/opa/press-release/file/1080766/download.

Le Pen received a €9 million loan from the First Czech-Russian Bank, which is owned by a Kremlin-connected oligarch, during the course of her presidential campaign. Subsequent investigation showed the loan was secured following extensive discussions between members of Le Pen's party and affiliates of a prominent Russian politician, Alexander Babkov, who in turn had ties to the bank's owner.[5]

Influence operations are also used to directly influence geopolitical outcomes. In the Netherlands, Russian proxies posing as Ukrainians were engaged in efforts to sway a 2015 referendum against Ukraine's Free Trade Agreement with the EU.[6] In the UK's Brexit campaign, Russia also played a role in supporting the Leave campaign to advance its aims of fragmenting the EU and creating divisions within the transatlantic community. Media reporting has uncovered, for example, that the biggest financial backer of the Leave campaign, Arron Banks, had numerous meetings with Russian Embassy officials and businessmen who offered Banks and his associates attractive investment opportunities in the Russian minerals sector.[7]

A slightly different model of influence operation can be seen in the deployment of private Russian military contractors and "political technologists" with expertise in rigging elections. Such contractors have been deployed to the Central African Republic, Libya, Sudan, Madagascar, Syria and Venezuela. In most of these countries, Russian contractors provide a suite of services ranging from personal security to technical support for manipulating elections (in the case of several African countries). In return, the parent company – in most cases the Wagner private military contractor – receives a cut of mineral extraction revenues and of course has direct influence over the host regime.[8] The brainchild of this vast network of private contractors is Putin crony Yevgeny Prigozhin, who manages

---

[5] German Marshall Fund and C4ADS, "Illicit Influence: A Case study of the First Czech Russian Bank," 2019. https://securingdemocracy.gmfus.org/first-czech-russian-bank-case-study/.

[6] Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," *New York Times*, February 16, 2017. https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html.

[7] Ed Caesar, "The Chaotic Triumph of Arron Banks, the 'Bad Boy of Brexit,'" *The New Yorker*, March 18, 2019. https://www.newyorker.com/magazine/2019/03/25/the-chaotic-triumph-of-arron-banks-the-bad-boy-of-brexit.

[8] Neil Hauer, "Russia's Favorite Mercenaries: Wagner, the elusive private military company, has made its way to Africa—with plenty of willing young Russian volunteers," *The Atlantic*, August 27, 2018. https://www.theatlantic.com/international/archive/2018/08/russian-mercenaries-wagner-africa/568435/. Ilya Rozhdestvensky, Michael Rubin, and Roman Badanin, "Master and Chef: How Russia interfered in elections in twenty countries," *Proekt*, April 11, 2019. https://www.proekt.media/investigation/russia-african-elections/.

Wagner and bankrolls the St. Petersburg-based Internet Research Agency, whose disinformation operations were at the center of Russia's interference in the 2016 U.S. presidential election.

Finally, a third model of conducting influence operations is to use Russia's state-owned enterprises – Rosneft, Gazprom, Rosatom, Rostech, etc. – to offer foreign government officials preferential deals in return for influence. The hiring of former German Chancellor Gerhard Schröder as Chairman of Nordstream AG and Rosneft testifies to the close ties that Russian parastatal companies form with leading European politicians.

Destabilization Operations

While bearing many similarities to influence operations and often using many of the same techniques, Russia's destabilization operations aim not just to influence, but also to stoke or amplify divisions, recriminations, and disorder among Russia's adversaries.

In Montenegro, Russia's military intelligence service, or GRU, developed connections to the leaders of a small pro-Russian political party that later merged into a larger coalition bloc called the Democratic Front as part of a systematic effort to derail the country's plans to join NATO. At first, Russia's support was alleged to consist primarily of financial resources laundered through various corrupt schemes into party coffers. Subsequently, the operation expanded into an attempt to foment a violent coup d'état against the country's Prime Minister in October 2016 using right-wing thugs recruited from Montenegro and the neighboring region. Two GRU agents, Eduard Shirokov and Vladimir Popov, have been charged and sentenced in absentia for masterminding the plot.

Based in nearby Thessaloniki, former Duma member Ivan Savvidis provides another example of how Russian oligarchs who either live in foreign countries or have investments there can be leveraged to financially support local destabilization operations. Intercepted communications have reportedly shown how Mr. Savvidis used personal funds to support violent protests against the Prespa Agreement between Greece and North Macedonia. The goal of these efforts, which dovetailed closely and may have been coordinated with influence operations conducted by Russian intelligence agents based in the Russian Embassy in Athens (several of

whom were later expelled by the Greek government), was to block North Macedonia's membership in NATO.[9] According to media reports, Savvidis helped advance the Kremlin's cause by paying Macedonian soccer hooligans to demonstrate against the Prespa agreement in the hopes of undermining a crucial referendum on the agreement that was held in North Macedonia in September 2018 and by seeking to generate a political backlash against the agreement in Greece.

Although the Kremlin is usually opportunistic about its use of proxies to sow discord in Western societies, it has shown a particular proclivity for supporting far-right fringe groups, as I have written about.[10] GRU veterans, in particular, have directly funded or actively supported right-wing paramilitary groups in Hungary, Slovakia, and several other NATO countries. Russian Spetznaz veterans and possibly even active-duty GRU agents have also been closely associated with a network of *systema* martial arts clubs across Europe and North America, where they have attempted to recruit local sympathizers. In a number of European cities, the Russian security services have developed ties to local soccer hooligans ("ultras") and some believe that these services have also indirectly funded travel for Russian hooligans to go to Europe to engage in violence. Similarly, the GRU is an active backer of the Night Wolves motorcycle club, which played an important role in the seizure of the Crimean peninsula from Ukraine and currently maintains local affiliates in countries ranging from Serbia to the Baltic states to Germany. Finally, "patriotic" organizations inside Russia have been used to cultivate Neo-Nazi fringe groups across Europe. Sometimes these groups have sought to recruit neo-Nazi from Europe to serve as irregular fighters in Ukraine while in other cases they have provided them with weapons training in Russia. The bombers of a Swedish refugee center in January 2017, for example, had received weapons training from a Russian far-right organization that regularly hosts foreigners.

Russia's Illicit Financial Ecosystem

[9] Helene Cooper and Eric Schmitt, "U.S. Spycraft and Stealthy Diplomacy Expose Russian Subversion in a Key Balkans Vote," *New York Times*, October 9, 2018. https://www.nytimes.com/2018/10/09/us/politics/russia-macedonia-greece.html.

[10] Michael Carpenter, "Russia Is Co-opting Angry Young Men: Fight clubs, neo-Nazi soccer hooligans, and motorcycle gangs serve as conduits for the Kremlin's influence operations in Western countries," *The Atlantic*, August 29, 2018. https://www.theatlantic.com/ideas/archive/2018/08/russia-is-co-opting-angry-young-men/568741/.

Russian influence and destabilization operations are financed through a financial ecosystem that exists in Western countries thanks to the investments of Russian oligarchs and businessmen. Typically this money passes through offshore financial centers such as Cyprus, the British Virgin Islands, and the Cayman Islands, where its origins are obscured through layers of shell companies, and then it ends up being invested in Western countries such as the United States, Germany or the UK. While we do not know how much illicit Russian money is in the United States, in 2015 the Treasury Department estimated that $300 billion is laundered annually into this country from different sources around the world. Meanwhile, total private Russian holdings abroad are estimated to be in the range from $800 billion to $1.3 trillion.[11]

The Panama Papers and a number of other sources have helped reveal the precise mechanisms through which Russian money is laundered into Western financial and real estate markets. The Russian Laundromat is one such scheme that used an offshore network of shell companies and financial institutions to enable Russian oligarchs, officials, and organized crime syndicates to launder over $20 billion into Western financial institutions, mostly through banks in Moldova and Latvia.[12] Another well-known enabler of Russia's illicit financing schemes is Denmark's Danske Bank, which facilitated Russian money laundering through an Estonian correspondent bank that resulted in the transfer of a staggering $225 billion in illicit funds into Western financial markets.

So how does laundered money end up being used to fund influence operations? The Special Counsel's indictment of 12 GRU agents involved in hacking operations in the United States in 2016 provides one snapshot by showing how the GRU laundered over $95,000 using bitcoin and other cryptocurrencies to lease servers, register domains, and buy virtual private network accounts. More typically the Kremlin takes advantage of its diverse network of businessmen and oligarchs abroad to channel money – both licit and illicit – to those fronts that carry out it influence operations, such as pro-Kremlin think tanks, lobbying organizations, and nonprofits. In a number of countries, for example, Russia has financially supported

---

[11] Anders Aslund, "It's time to go after Vladimir Putin's money in the West," *Washington Post*, March 29, 2018. https://www.washingtonpost.com/news/democracy-post/wp/2018/03/29/its-time-to-go-after-vladimir-putins-money-in-the-west.

[12] OCCRP, "The Russian Laundromat," August 22, 2014. https://www.occrp.org/en/laundromat/russian-laundromat/.

NGOs opposed to fracking, which is a technology for producing unconventional oil and natural gas resources that are in direct competition with Russian hydrocarbon exports.[13] As the Savvidis, Borisov, and Aven cases demonstrate, an extensive network of regime-linked oligarchs stands ready and willing to finance all sorts of influence operations, whenever necessary.

Policy Recommendations

To combat Russian malign influence, the United States needs to work with its allies to accomplish three basic tasks. First, we need to coordinate law enforcement and intelligence activities to weed out malign networks of influence in Western societies. Second, we must proactively address our vulnerabilities to foreign malign influence by plugging governance gaps and creating greater transparency within our financial, real state, and media ecosystems. Third, we must impose greater costs on Russia whenever we discover Russian interference in our democratic process. Let me briefly elaborate on each of these.

First, with regards to weeding out Russian networks of malign influence, we need better coordination in the United States between our national security agencies and domestic law enforcement, as well as better intelligence sharing with our NATO allies. The firewall that currently exists between U.S. domestic law enforcement agencies and our national security apparatus needs to be broken down to allow for more information sharing about covert influence networks. My own experience serving at the NSC has shown that NSC staff are often oblivious to ongoing investigations by, say, a U.S. attorney's office, while U.S. attorneys and their staff often lack information on the latest Russian operations in Europe or elsewhere in the world. A standing interagency task force on malign Russian influence chaired at the level of NSC Senior Director is probably the best structure to coordinate such action.

Second, there are a number of good legislative proposals to address our vulnerabilities to Russian malign influence that need to be passed into law as soon as possible. The most important of these is also the most difficult politically:

---

[13] James Edgar, "Russia in secret plot against fracking, Nato chief says," *The Telegraph*, June 19, 2014. https://www.telegraph.co.uk/news/earth/energy/fracking/10911942/Russia-in-secret-plot-against-fracking-Nato-chief-says.html

reform of our campaign finance system, which is so opaque as to practically invite foreign adversaries to channel dark money into our political process. Legislation to identify the beneficial owners of limited liability companies (LLCs) is also necessary and urgent, since many LLCs function simply as shell companies whose sole purpose is to mask covert financial transactions to evade scrutiny by U.S. law enforcement. Similarly, stricter anti-money laundering regulations are needed to tighten illicit financial flows, particularly between the United States and offshore tax havens. In the real estate market, there needs to be more transparency for high-end real estate transactions as well as greater resources devoted to the Treasury Department's Financial Crimes Enforcement Network (FinCen), so that investigations can be pursued whenever there is evidence of suspicious behavior. Despite a growing recognition of the problem of money laundering through real estate, the U.S. market is simply too big for FinCen to patrol with its current resources and staffing. Lastly, law firms also need to be subjected to greater transparency so that attorney-client privilege does not become a loophole through which foreign entities channel funds to their U.S. legal representatives for nefarious purposes.

The third and final major task for the United States and our allies is to impose more significant costs on Russia for its brazen interference in our democratic process. In January of this year, the Director of National Intelligence and the FBI Director both testified to this Congress that Russian interference in our democratic process is still ongoing. Clearly, our current patchwork of sanctions on oligarchs, government officials, and a few select companies is not enough. To impose real costs on Russia, it is time to look at much more forceful measures, such as full blocking sanctions on select Russian banks, as I have suggested elsewhere.[14] Let's be honest: our current sanctions on Russia are designed to be weak, and this is true despite the fact that we have the capacity to impose devastating costs on Russia for its malign activity. It's past time that we do so.

[14] Michael Carpenter, "How to Make Sanctions on Russia Work," *The American Interest*, December 18, 2018. https://www.the-american-interest.com/2018/12/18/how-to-make-sanctions-on-russia-work/.

Mr. KEATING. Thank you, Doctor.
Ms. Rosenberger.

STATEMENT OF MS. ROSENBERGER, DIRECTOR OF THE ALLIANCE FOR SECURING DEMOCRACY AND SENIOR FELLOW WITH THE GERMAN MARSHALL FUND

Ms. ROSENBERGER. Thank you so much, Chairman Keating, Ranking Member Kinzinger, and distinguished members of the committee. Thank you for inviting me to address you today.

I submitted my full statement for the record but let me highlight key points on Russia's operations to undermine our democracy and what we need to do to address it.

These operations employ five primary asymmetric tools: information operations, cyber attacks, malign financial influence, political and social subversion, and strategic economic coercion.

They exploit democracy's openness while weaponizing societal and institutional vulnerabilities and election interference is but one component.

I am glad to address two underappreciated tools today: malign financial and coercive economic tactics that Russia uses in Europe.

These activities threaten U.S. national security by undermining cohesion of NATO and the EU, encouraging policies favorable to Moscow, and weakening democratic governance.

Putin's primary goal is maintaining power and these activities also protect and grow the ill-gotten assets of his inner circle, defending their favored position and the wider patronage system.

Russian corporations, oligarchs, and organized crime networks are all agents of malign influence abroad, often acting on their own to curry favor with those in power, protect their standing, and guarantee future opportunities.

Here is how. First, Russia enriches elites in target countries including government officials, former political leaders, and other well-connected individuals in order to influence government's policies.

Second, Russian entities provide direct support for euroskeptic and illiberal populist parties.

Third, energy investments are used similarly to enrich elites, to fund political parties, and to create dependence in order to build leverage and impede leaders' ability to challenge Russia.

Fourth, Russian proxies establish and finance a network of NGO's in Europe that support and connect euroskeptic and pro-Kremlin movements.

Fifth, Russia empowers fringe elements including paramilitary groups to increase polarization and hinder States' ability to govern.

Finally, Russia uses dark money to support media outlets across Europe that spread favorable narratives. Russian online information operations including by the infamous Internet Research Agency often accompany these tactics, injecting disinformation and divisive content supporting the Kremlin's agenda.

These tactics exploit weak regulatory enforcement, legal loopholes, enabling jurisdiction, erosion of the rule of law, and societal polarization.

Vulnerabilities include weak penalties for money laundering, lax foreign investment screening in Europe, and weak or absent laws

on foreign funding of political candidates or parties, as well as the ability to form anonymous companies in the United States.

The recent scandal in Austria, which the chairman discussed, highlights these vulnerabilities and how illiberal forces in Europe embrace Russian support and facilitate its activities.

As Dr. Carpenter noted, Chinese investments in Europe bring similar concerns over elite cultivation by entities with opaque ties to the party State and Chinese and Russian activities can reinforce one another.

And as you know, Russia has also used these tools to undermine democracy in the United States. The U.S. Government needs to develop a unified and integrated approach to this issue including by creating a national hybrid threat center and appointing a counter foreign interference coordinator at the National Security Council to coordinate U.S. Government efforts.

They also need to work closely with our allies across the Atlantic including to facilitate a unified EU and NATO response. This is particularly essential as Putin seeks to divide us.

We need to enhance coordination to share threat information and learn from one another's responses. NATO should continue to increase focus on nontraditional threats and enhance cooperation with the EU.

The United States should also work with allies to articulate clear warnings about the consequences for unacceptable foreign interference.

The United States should increase assistance programs to ensure partners and allies can withstand and respond to these tactics. We should continue working with European partners to reduce dependence on Russian energy and increase assistance to civil society including investigative and independent media.

The United States needs to do more to raise costs on Moscow by fully implementing existing sanctions as part of a comprehensive strategy with consistent messaging and coordination with European allies.

Congress should consider additional sanctions particularly in the financial sector as well as automatic sanctions triggers if Russia engages in further interference operations.

The United States should make clear that it will not tolerate enabling, indulging in, or importing Russia's corrupt and anti-democratic practices including by allies like Hungary.

The United States should prioritize diplomatic efforts to convince countries of key concern to undertake reforms. We also need to enhance financial transparency.

Congress should pass measures that require disclosure of beneficial ownership. Treasury's geographic targeting order program should be made permanent and nationwide.

The United States should encourage the EU to develop a central anti-money laundering agency, fortify its new investment screening framework, and encourage stronger anti-money laundering enforcement and penalties.

Finally, Putin and his cronies rely on the Western financial system to protect and grow their assets even while they seek to weaken us. This gives us leverage and we should use it.

We can do more to cutoff access to our financial systems including through targeted sanctions on Putin's cronies and implementation of the Global Magnitsky Act, and we need to do more to expose these activities.

Russia's undermining of democracy demands a bipartisan response. The United States must recognize the threat and, together with our European allies, act with the urgency and strength required.

Thank you.

[The prepared statement of Ms. Rosenberger follows:]

Statement by Laura Rosenberger, Director of the Alliance for Securing Democracy and Senior Fellow at the German Marshall Fund of the United States

BEFORE THE UNITED STATES HOUSE COMMITTEE ON FOREIGN AFFAIRS

Concerning: "Undermining Democracy: Kremlin Tools of Malign Political Influence"

May 21, 2019

Chairman Keating, Ranking Member Kinzinger, and Distinguished Members of the Committee, thank you for inviting me to address you today on the Kremlin's undermining of democracy through tools of malign political influence.

Vladimir Putin's Russia uses a suite of low-cost, asymmetric tools to undermine democratic institutions as a means of weakening Europe, the United States, and transatlantic ties. This threat poses a unique national security challenge, as the attacks exploit democracies' openness while weaponizing societal and institutional vulnerabilities. Putin and his proxies wage these operations using five primary, non-military tools – information operations, cyberattacks, malign financial influence, political and social subversion, and state economic coercion. These activities support Putin's goals of discrediting democracy as a form of government, destabilizing and weakening Russia's competitors, and gaining relative power on the world stage.

While these attacks opportunistically exploit specific vulnerabilities in individual societies, there are patterns to how they manifest across countries. Elections, which are a key institution in any democracy, often serve as an opportune target. But attacks on elections are typically just one part of ongoing, multi-pronged operations. Effectively countering this threat requires understanding the full toolkit that Russia uses to attack our institutions and its broader transnational strategy.

Malign Financial and Coercive Economic Tools: An Underexplored Dimension of Interference

According to a review of open source reporting, Russia has conducted at least 362 operations targeting 41 European countries using at least one of these tools since 2000.[1] While Russia's employment of information operations and cyberattacks has received significant attention – if insufficient response – in the United States, I have been asked to address underappreciated dimensions of its toolkit: the use of malign financial and coercive economic tactics to undermine democracies and support illiberal forces across Europe.

Our open source review, which captures a significant subset of all known cases of Russian interference, has identified Russia's use of malign financial tactics, defined as "the facilitation of financial activity involving illicit proceeds or in furtherance of other illicit ends,"

[1] Authoritarian Interference Tracker, Alliance for Securing Democracy. Accessed 17 May 2019. https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/

in 28 European countries since 2000.[2] We also document its use of strategic economic coercion, defined as "the exploitation of national resources and commercial activity as leverage over another country's government to weaken it and force a change in policy," in 19 European countries since 2000.[3] These activities constitute threats not only to good governance and the rule of law in Europe, but to national security, with direct implications for the United States. First, these activities undermine the cohesion of both NATO and the EU, discourage policies that Moscow sees as unfavorable and encourage policies it prefers, and facilitate dependencies that make it difficult for political leaders to challenge Moscow. Second, these activities – which include cultivating political sway with favored individuals and groups, providing non-transparent support for political parties and fringe or illiberal movements, and funding of pro-Kremlin media and information operations – weaken democracies by making it more difficult for them to govern cohesively, and by promoting corruption that makes them less responsive to their citizens.

These activities are not just tools of leverage for Putin – they are part of how he obtained and maintains power. These dark money tactics serve to both protect and grow the assets of Putin's inner circle – assets largely stolen from the Russian people through insider contracts and non-transparent financial tactics.[4] Putin's primary goal is maintaining power, and for him, that is highly dependent on protecting the favored position of his inner circle and the functioning of the wider patronage system. Up to $800 billion in Russian assets, accounting for over half the country's financial wealth, are believed to be held offshore and extremely concentrated in the hands of a small elite.[5] Putin and his cronies depend on the Western financial system to grow, hide, and attempt to clean their spoils. Anders Aslund estimates that since 2006, Putin and his cronies have extracted $15-25 billion a year from these assets, or a total of $195-325 billion, including $10-15 billion extracted from Gazprom for their personal gain.[6]

The Russian government itself does not direct all of these activities. Russian corporations, oligarchs, and even organized crime networks are agents of malign financial influence and economic coercion, often acting of their own volition to curry favor with those in power, to protect their wealth and standing, and to help guarantee favorable opportunities in the future.[7] As Russia expert Mark Galeotti puts it, "As part of the price of doing business without potential hindrance, or in the hope of future benefit, companies may be expected to provide funding for foreign political parties or campaigns, contribute to favoured causes, or otherwise dance to the Kremlin's tune."[8]

---

[2] Ibid.
[3] Ibid.
[4] Dawisha, Karen. *Putin's Kleptocracy: Who Owns Russia?* New York: Simon & Schuster, 2015. Print. p. 3-4.
[5] Zucman, Gabriel *et al.* "From Soviets to Oligarchs: Inequality and Prosperity in Russia, 1905-2016." NBER Working Paper No. 23712. August 2017, p. 23.
[6] Aslund, Anders. "Money Laundering Involving Russian Individuals and their Effect on the EU." Testimony to the European Parliament Tax-3 Committee. 29 Jan 2019. http://www.europarl.europa.eu/cmsdata/161070/2019%2001%2029%20-%20%20Andreas%20Aslund%20Replies%20and%20EP%20Testimony%20Russian.pdf
[7] Galeotti, Mark. "Controlling Chaos: How Russia Manages Its Political War in Europe." European Council on Foreign Relations, 01 Sept. 2017. Web. 13 May 2019. p. 6.
[8] *Ibid.*, p. 4.

Russia's Modes and Methods of Malign Financial and Coercive Economic Influence

Former President of Freedom House David Kramer rightly observed that "corruption is Putin's biggest export," but that is because the West imports it, enabling Putin's efforts to blur the distinction between democracies and his kleptocracy.[9] Let me highlight a few of the modes and methods Putin's Russia uses to undermine democracy and gain malign influence in Europe.

First, Russia targets and enriches elites in target countries to cultivate direct political influence. This can include government officials and politicians, former political leaders who remain influential, and other well-connected individuals, in order to influence governments' policies. Former German Chancellor Gerhard Schröder is the most well-known example of this, having joined the board of Russian state-owned oil company Rosneft, but lower level elites are also targets. For instance, the Organized Crime and Corruption Reporting Project (OCCRP) revealed in March that Aivars Bergers, one of the largest donors to the Latvian pro-Russian Harmony Party, received €270,000 from two offshore companies used in the Azerbaijani Laundromat and the Magnitsky affair, two well-known international money laundering schemes.[10]

In some cases, Russian entities provide direct support for Eurosceptic and illiberal populist political parties. The most well-known of these was in France, with the 2016 loan to Marine Le Pen's National Front brokered by the Russian government.[11] The money was disbursed by First Czech Russian Bank, which was connected to organized crime and later had its license revoked for money laundering violations.[12] In Italy, Matteo Salvini's La Lega party was, as of October 2018, reportedly brokering a deal with Russian state oil interests to receive part of the proceeds from the sale of three million metric tons of diesel. If confirmed, this would be a brazen instance of direct Russian funding of an illiberal populist political party in Europe.[13] In Estonia, Russian Oligarch Vladimir Yakunin's Alliance for Peace and Freedom gave 1.5 million Euros to the campaign of Edgar Savisaar, the mayor of Tallinn and leader of the opposition party. Savisaar did not disclose the donation and later tried to claim the funds as donations for construction of a church.[14] In the UK, Arron Banks, co-founder of the Leave.EU campaign and one of the largest donors to the U.K. Independence Party (UKIP),[15] was allegedly offered the opportunity to invest in gold and diamond mines by Russian businessmen connected

[9] Kramer, David. Remarks at conference: "The New Tools of Authoritarian Influence." The German Marshall Fund of the United States. Berlin, Germany.14 May 2019.
[10] Springe, Inga, and Karina Shedrofsky. "Mega-donor to Pro-Russian Party Benefits from Magnitsky and Azerbaijani Laundromats." *Re:Baltica*. The Baltic Center for Investigative Journalism, 20 Mar. 2019. Web. 14 May 2019.
[11] "Comment les partis sont-ils financés ?" *Vie publique*. Direction de l'information légale et administrative de la RF, 14 Jan. 2018. Web. 14 May 2019.
[12] Rosenberger, Laura, and Thomas Morley. "Russia's Promotion of Illiberal Populism: Tools, Tactics, Networks." *Alliance for Securing Democracy*. German Marshall Fund of the United States, 11 Mar. 2019. Web. 17 May 2019. p. 4.
[13] Nadeau, Barbie Latza. "An Italian Expose Documents Moscow Money Allegedly Funding Italy's Far-Right Salvini." *The Daily Beast*, 22 Feb. 2019. Web. 22 Feb. 2019.
[14] Rosenberger and Morley, p. 5.
[15] Caesar, Ed. "The Chaotic Triumph of Arron Banks, the "Bad Boy of Brexit"." *The New Yorker*, 18 Mar. 2019. Web. 17 May 2019.

to Aleksandr Yakovlenko, then the Russian Ambassador to the United Kingdom.[16] Although Banks denies accepting the offer, *The Guardian* reports that Leave.EU staff met with representatives of the Russian government as many as eleven times in the lead-up to the 2016 Brexit referendum.[17]

The Russian government also uses foreign investments to create dependence on Russian energy or natural resource exports, in order to build foreign policy leverage. This also includes foreign investments designed to enrich local elites in other countries, eroding those nations' political independence. The Russian government's significant control over its energy sector provides it "the ability to manipulate European energy trade to accomplish political aims, enrich chosen elites, and interfere with domestic political processes."[18] In the gas sector, pipeline links and business ties date back to the Soviet era, but new deals are creating new vulnerabilities. In Hungary, for instance, businessmen linked to Viktor Orban made hundreds of millions of dollars buying underpriced Gazprom gas through a Swiss trading firm and reselling it in Hungary at market prices.[19] And Hungary granted Rosatom a contract to expand a nuclear power plant without an open tender and without any public oversight. The Hungarian Parliament voted to keep most details of the agreement a state secret for thirty years.[20] At the strategic level, Heather Conley found in CSIS' *Kremlin Playbook*[21] that countries where Russia's economic footprint was greater than twelve percent of GDP were vulnerable to Russian influence and state capture. In Bulgaria, for instance, Russia dominates the energy sector, with Russia's economic footprint peaking at 27% in 2012.[22][23] Russia uses a network of compromised officials and Bulgarian businessmen to maintain and further this dominance.[24]

In addition to targeting elites and capturing interests at the state level, a network of friendly oligarchs, businesspersons, and other cut-outs establish and finance NGOs in European countries that spread and support the Kremlin's agenda. Yakunin, the former head of Russian Railways, is one of the most prolific founders and funders of NGOs used by the Russian government to advance its foreign policy goals abroad. In France, his Foundation of Saint Andrew the First-Called partnered with far-right anti-LGBT and anti-Semitic groups.[25] Yakunin also funds the Dialogue of Civilizations (DoC) Research Institute, a network of think tanks in

---

[16] Kirkpatrick, David D., and Matthew Rosenberg. "Russians Offered Business Deals to Brexit's Biggest Backer." *The New York Times*, 29 June 2018. Web. 17 May 2019.
[17] Cadwalladr, Carole, and Peter Jukes. "Revealed: Leave.EU Campaign Met Russian Officials as Many as 11 times." *The Guardian*, 08 July 2018. Web. 17 May 2019.
[18] Rosenberger and Morley, p. 3.
[19] Hegedűs, Dániel. "The Kremlin's Influence in Hungary: Are Russian Vested Interests Wearing Hungarian National Colors?" German Council on Foreign Relations, Feb. 2016. Web. 27 Feb. 2019. p. 5-6.
[20] "Austria sues over EU approval of Hungary nuclear plant," *Euractiv.eu,* 23 February 2018. Web. 19 May 2019. https://www.euractiv.com/section/politics/news/austria-sues-over-eu-approval-of-hungary-nuclear-plant/
[21] Conley, Heather A., James Mina, Ruslan Stefanov, and Martin Vladimirov. *The Kremlin Playbook.* Center for Strategic and International Studies, Oct. 2016. Web. 17 May 2019. p. xi-xii.
[22] "Greece's DEPA to Become First Gas Supplier to Bulgaria outside Gazprom." *Reuters.* Thomson Reuters, 02 Apr. 2019. Web. 15 May 2019.
[23] Conley *et al.*, p. 44.
[24] *Ibid.*, p. 45.
[25] Piérot, Jean-Paul. "Saint-Just, l'extrémiste de droite n'aime pas siéger." *L'Humanité.* 16 Jan. 2014. Web. 12 Feb. 2019

Moscow and European capitals that advocate for Russian interests. DoC hosts the yearly Rhodes Forum in Greece, a sort of anti-American Davos.[26] Underscoring the connections among these tactics and their transnational nature, Yakunin was implicated in widespread corruption at Russian Railways when he oversaw the company. Through banks in Moldova and Latvia, funds linked to that corruption scandal passed through the Russian Laundromat money laundering scheme.[27]

Russia's tactics also include empowering fringe elements in order to drive up polarization and hinder the ability to govern. In the Republika Srpska entity of Bosnia and Herzegovina, Russian officials and investors have supported nationalist president Milorad Dodik, whose regime has gone to great lengths to undermine the Bosnian state-level government and disrupt the country's Euro-Atlantic integration. In Serbia, the hardline Serbian war veterans' association opened a paramilitary (or "military patriotic") training camp for Serbian youth, allegedly with support from Russian embassy officials[28] and the Russian far-right group ENOT.[29] Russia has also long supported Ataka, a far-right political party in Bulgaria,[30] characterized by its anti-Semitic and xenophobic platform, as well as its Euroscepticism and anti-Atlanticism.[31]

Russia uses dark money to support other tools of malign influence, including its efforts to manipulate the information space. The Russian government's support for media outlets across Europe – including in Hungary,[32] the Baltics,[33] and the Anglosphere,[34] as well as the opening of RT outlets in France,[35] Italy,[36] and Germany,[37] has facilitated the spread of antiestablishment and pro-Kremlin narratives, including by hyping issues like migration that fuel support for Euroscepticism and antidemocratic forces. In 2017, investigations by the Baltic Center for Investigative Journalism revealed that Baltnews, a collection of three Russian-language news

---

[26] Buckley, Neil. "Rhodes Gathering Blames the World's Woes on the West." *Financial Times*, 04 Oct. 2016. Web. 17 May 2019.
[27] Harding, Luke, and Nick Hopkins. "How 'Dirty Money' from Russia Flooded into the UK – and Where It Went." *The Guardian*, 20 Mar. 2017. Web. 17 May 2019.
[28] "Serbian Police Close Paramilitary Youth Camp Run by Ultranationalists, Russian Group." Radio Free Europe / Radio Liberty, 17 Aug. 2018. Web. 13 May 2019.
[29] Pavelic, Boris. "Refugee Killings Controversy Haunts Croatian Serbs' Memorial." *Balkan Transitional Justice*. Balkan Insight, 12 Aug. 2013. Web. 15 May 2019.
[30] Hanlon, Bradley, and Alexander Roberds. "Securing Bulgaria's Future: Combating Russian Energy Influence in the Balkans." *Alliance for Securing Democracy*. German Marshall Fund of the United States, 21 June 2018. Web. 15 May 2019.
[31] Simmons, Jo. "The Curious Tale of Bulgaria's Extremist Flip-Flopping Party." *Huffington Post*, 03 June 2014. Web. 15 May 2019.
[32] Dezső, András. "Kiderült, amit eddig is sejtettünk: orosz propaganda fut a kormánysajtóban." *Index*, 15 Apr. 2018. Web. 25 Feb. 2019.
[33] Springe, Inga, and Sanita Jemberga. "Sputnik's Unknown Brother." *Re:Baltica*. The Baltic Center for Investigative Journalism, 6 Apr. 2017. Web. 14 May 2019.
[34] Hanlon, Bradley, and Thomas Morley. "Russia's Network of Millennial Media." *Alliance for Securing Democracy*. German Marshall Fund of the United States, 15 Feb. 2019. Web. 14 May 2019.
[35] Viscusi, Gregory, and Helene Fouquet. "France's Macron Lifts Ban on Access for Russia Today TV." *Bloomberg*, 13 Nov. 2018. Web. 25 Feb. 2019.
[36] Lusi, Domenico. "Lo zar Putin alla campagna d'Italia." *Pagina99*, 12 Oct. 2017. Web. 25 Feb. 2019.
[37] Macho, Andreas. "Russia Today: der Propaganda-Sender des Kremls in Deutschland." *Handelsblatt*, 21 Nov. 2014. Web. 25 Feb. 2019.

sites, was secretly owned by RIA Novosti via a series of Russian and Dutch shell companies.[38] The three news sites were also connected to a Russian funded NGO, part of a larger NGO network in the Baltic states whose work is targeted at reinforcing the Kremlin's interests among the region's Russian ethnic minority.[39]

Russian online information operations across Europe often accompany these other tactics, and have repeatedly injected disinformation to promote far-right groups supportive of the Kremlin's agenda,[40] drive up anti-immigrant sentiment,[41] spread anti-NATO messages, undermine support for Ukraine, and oppose fracking (which threatens Russia's energy dominance).[42] A recent report from Andrew Dawson and Martin Innes at the University of Cardiff analyzed data from accounts publicly that Twitter identified to have been operated by the Internet Research Agency – controlled and financed largely by Putin's associate Yevgeniy Prigozhin – between 2014-2016. Dawson and Innes found a more significant amount of activity targeted at Europe than previously known. They found that these accounts engaged extensively in Bulgarian, Estonian, French, German, Italian, Romanian and Spanish, and that in addition to activity on the U.S. 2016 election, there were "significant levels of interest in a series of elections and democratic events across Europe in 2016."[43]

Vulnerabilities Enable Russia's Malign Activities

Some of Russia's tactics violate existing law, but many of its malign financial activities – much like the other asymmetric tools Putin's Russia deploys – operate in a grey zone. Russia takes advantage of weak legal and regulatory enforcement, legal loopholes, enabling jurisdictions, and erosion of the rule of law. Just as Russia has exploited U.S. tech platforms to attack our democracy, Russia has used the Western financial system to facilitate illicit practices to undermine and corrupt our systems from within. A series of large-scale money-laundering scandals in the EU in recent years has revealed the scale of this problem. These scandals are not confined to countries typically seen as having corruption problems.[44]

---

[38] Spriņģe and Jemberga, 2017.
[39] Jemberga, Sanita, Mikk Salu, Šarūnas Černiauskas, Guntars Veidemanis, and Anton Lysenkov. "Kremlin's Millions." *Re:Baltica*. Trans. Aleks Tapins. The Baltic Center for Investigative Journalism, 27 Aug. 2015. Web. 14 May 2019.
[40] Farand, Chloe. "French Social Media Is Being Flooded with Fake News, Ahead of the Election." The Independent, 23 Apr. 2017. Web. 17 May 2019.; Stelzenmüller, Constanze. "The Impact of Russian Interference on Germany's 2017 Elections." Brookings, 28 Nov. 2017. Web. 17 May 2019.; Applebaum, Anne, Peter Pomerantsev, Melanie Smith, and Chloe Colliver. "MAKE GERMANY GREAT AGAIN" Kremlin, Alt-Right and International Influences in the 2017 German Elections." Institute for Strategic Dialogue, Dec. 2017. Web. 17 May 2019.
[41] Weiss, Michael. "The Kremlin Cries Rape for Propaganda in Germany." *The Daily Beast*, 02 Feb. 2016. Web. 17 May 2019.
[42] Harvey, Fiona. "Russia 'Secretly Working with Environmentalists to Oppose Fracking'." *The Guardian*. Guardian News and Media, 19 June 2014. Web. 14 May 2019.
[43] Dawson, Andrew, and Martin Innes. "The Internet Research Agency in Europe 2014-2016." Cardiff University Crime & Security Research Institute, May 2019. Web. 17 May 2019. p. 3.
[44] Prominent examples include "the Russian Laundromat" in Moldova; Deutsche Bank mirror trading; Danske Bank and Swedbank in Estonia; the Troika Laundromat/Ukio Bank in Lithuania; ABLV in Latvia; and ING in the Netherlands.

The EU also does not closely monitor foreign investments, opening itself to strategic, non-commercially motivated investments from Russia. Opaque foreign investments may also provide the Russian government access to controlled technology, personal user data, or government contracting opportunities. The ability to form anonymous companies in the United States also constitutes a weak link in the international financial system, particularly in the real estate sector, facilitating the movement of dark money. A number of European countries also have weak or no laws banning foreign funding of political candidates or parties, leaving the door wide open for Russian political influence.[45] Finally, a number of European countries play a particular role in facilitating these activities through weak enforcement, corruption, or economies that serve as offshore financial service ecosystems, including Cyprus, Switzerland, Austria,[46] and until recently, Latvia.

A recent scandal that forced snap elections in Austria highlights the ways in which illiberal forces in Europe welcome and facilitate these activities. Austrian Vice Chancellor Heinz-Christian Strache, leader of the far-right Freedom Part of Austria, was forced to resign after footage emerged of him discussing illegal quid pro quo arrangements with a woman he thought was a Russian oligarch's niece. In the video, he and a colleague explained how she could circumvent foreign donation limits, take over a media outlet to support his candidacy, and receive illegal public contracts for a company she might found.[47]

While Russia is particularly adept at exploiting these vulnerabilities, these same pathways can be and are exploited by other authoritarian actors. As this committee heard at a recent hearing, China is seeking to expand its influence in Europe using a range of tactics. Chinese investments in Europe come with some of the same concerns over elite cultivation by entities with opaque ties to the state – and in many ways Chinese and Russian activities reinforce one another in eroding European cohesion and leveraging political influence. In the Czech Republic, a nominally private Chinese conglomerate, CEFC China Energy, cultivated a close relationship with Czech president Miloš Zeman and his political associates through a series of high-profile investments in the country.[48] Zeman has since emerged as a vocal champion of a deepening partnership between China and the Czech Republic (even as CEFC's profile itself has declined).[49,50,51] However, CEFC's investment in Zeman continues to pay dividends for the Chinese party-

---

[45] Berzina, Kristine. "Foreign Funding Threats to the EU's 2019 Elections." German Marshall Fund of the United States, 15 Oct. 2018. Web. 17 May 2019.

[46] Conley, Heather A., Ruslan Stefanov, Martin Vladimirov, and Donatienne Ruy. *The Kremlin Playbook 2*. Center for Strategic and International Studies, Mar. 2019. Web. 17 May 2019.. p. 56.

[47] Leila Al-Serori, Oliver Das Gupta, Peter Peter Münch, Frederik Obermaier and Bastian Obermayer. "Caught in the Trap" *Stiddeutsche Zeitung*

[48] Barboza, David, et al. "China Seeks Influence in Europe, One Business Deal at a Time." The New York Times. 12 Aug. 2018. Web. Accessed 20 May 2019.

[49] "Zeman Hopes B&R Initiative Will Help Boost Czech Development." Xinhua. 26 January 2019. Web. 20 May 2019.

[50] Allen-Ebrahimian, Bethany, and Emily Tamkin. "Prague Opened the Door to Chinese Influence. Now It May Need to Change Course." Foreign Policy. 16 Mar. 2018. Web. 20 May 2019.

[51] Ke, Dawei, et al."Update: Prague Approves Citic Takeover of CEFC China's Czech Assets". Caixin. 30 Aug 2018. Web. 20 May 2019.

state. In a recent television appearance, he defended Huawei's desire to build the Czech Republic's 5G network and attacked his own country's security agencies for opposing it.[52]

Time to Act

To date, Putin's Russia has faced little real consequence for its nefarious activities, and the damage is compounding. The need for action could not be more urgent. And as the United States has learned all too clearly, Russia's use of these tools to undermine democracy are not confined to Europe's borders, and have been used to attack the United States as well. There are a series of steps that the United States and our allies can take that would both make our systems more resistant to these tactics and strengthen our democracies, and make it more difficult for Putin and his cronies to enrich themselves at our expense. The bipartisan initiative I co-direct developed a comprehensive strategy to counter authoritarian interference in democracies, endorsed by a bipartisan and transatlantic group of former senior national security officials (See Appendix A).[53]

The United States needs to recognize the threat to our national security posed by Russia's use of this toolkit and respond with the kind of serious effort required. Many of Russia's tactics fall in the cracks and seams of the U.S. bureaucracy. We need to ensure our analysts and policymakers are seeing and responding to the full range of tools that Russia is employing to undermine democracies and exert malign influence. Establishing a National Hybrid Threat Center at ODNI and creating a senior-level coordinator at the NSC to counter foreign interference would be critical steps to ensure the U.S. government has a full appreciation of the challenges we face and can coordinate a response across the U.S. government and with our partners and allies.

Transatlantic cooperation, including unified responses across the EU and within NATO, is essential – especially as Putin seeks to divide us. We need to enhance information sharing and coordination mechanisms, including on technical fronts like establishing a system among the United States, UK, and EU to track cross-border payments in centralized databases to support law enforcement, counterintelligence, and anti-money laundering (AML) supervision. More broadly, the United States and European allies need to share threat information and learn from one another's responses. The nascent G7 Rapid Response Mechanism presents one avenue for such coordination, though it should be broadened beyond disinformation to cover the full range of tools Russia and others are using to undermine democracies. And while NATO has expanded its strategy on dealing with hybrid threats, many of Russia's tools fall outside the bounds of the traditional political-military alliance. Given the harm these tools pose to the unity of the alliance, NATO should increase its focus on non-traditional security threats, including – as former U.S. Ambassador to NATO Doug Lute has suggested – through a renewed focus on building resilience under Article 3 of the Washington Treaty. NATO-EU cooperation on these issues is also critical, and the two bodies should form a joint task force on countering asymmetric threats,

---

[52] Willoughby, Ian. "President Slams Security Agencies over 'Campaign' against Huawei | Radio Prague." *Radio Praha*, 11 Jan 2019. Web. 20 May 2019.

[53] Rosenberger, Laura, Jamie Fly, and David Salvo. "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies." *Alliance for Securing Democracy*. German Marshall Fund of the United States, 26 June 2018. Web. 17 May 2019.

including to facilitate intelligence sharing. The mandate of the European Centre of Excellence for Countering Hybrid Threats includes economic threats, and it should emphasize this area in its work, along with ongoing work on other challenges like information operations.

The United States should also increase assistance to our European partners and allies to ensure they have the ability to withstand and respond to these tactics. This should include expanding capacity building and technical assistance programs, both bilaterally and through multilateral institutions, to strengthen our allies' ability to combat illicit finance. The Departments of State and Treasury should also increase diplomatic efforts to convince countries of key concern to undertake reforms. And the United States should continue to work with European partners to reduce dependence on Russian energy, including by encouraging them to work in solidarity with each other to oppose projects like Nord Stream 2, while continuing to swiftly permit LNG exports to provide Europe with new sources of gas. Finally, the U.S. should increase assistance to civil society in Europe, which is critical for building resilience, with a particular focus on independent and investigative media, NGOs, and transparency organizations – especially in countries where Russia is investing its own resources and where space is shrinking for civil society organizations and media.

The United States should continue to increase costs on Moscow for it continued nefarious activities. In particular, the Administration needs to fully implement existing sanctions on Russia, and ensure that these measures are part of a comprehensive strategy, including with consistent messaging and coordination with European allies. Congress should consider additional sanctions – particularly in the financial sector such as new sovereign debt restrictions – as well as consider measures such as the DETER Act that would set automatic triggers for sanctions if Russia engages in interference operations. The United States should also work with our European partners to develop a set of shared principles on unacceptable foreign interference and articulate clear deterrent warnings about the costs that will be imposed on foreign actors for engaging in such activity.

The United States also needs to make clear to our allies and partners that it will not tolerate the enabling, indulging in, or importing of Russia's corrupt practices. U.S. security interests are inherently intertwined with issues of rule of law and good governance, as corruption and anti-democratic governance makes countries more vulnerable to Russian malign influence. This poses uncomfortable choices when U.S. allies engage in these tactics, but doing business-as-usual with governments like Victor Orban's only invites further Russian malfeasance – and sends a signal to others that they can get away with similar behavior.

We also need to enhance transparency of the international financial system to track and prevent the flow of dark money, monitor foreign investments, and close legal loopholes. This includes recognizing the role that a lack of transparency in parts of the U.S. financial system plays while pushing our allies to improve their own systems. For the United States, the highest priority should be ending the formation of anonymous companies by passing measures like the bipartisan Corporate Transparency Act, which would require disclosure of beneficial ownership. Treasury Department efforts to track foreign ownership of residential real estate in select cities under a temporary Geographic Targeting Order program are welcome, but should be made permanent and expanded nationwide. The United States should encourage the EU to develop a

central AML agency across the full single market to address the current mismatch with national level regulators.[54] The United States should also encourage European partners to fortify the EU's new investment screening framework by strengthening screening at the Member State level and adding an enforcement mechanism at the EU level. And the United States should press Switzerland, the global leader in the commodities trade and a key venue for the exportation of corrupt practices by the Russian energy sector, to take the lead and regulate the industry to prevent corruption, money laundering, and other illicit activity.[55]

The United States should enhance AML enforcement and the imposition of penalties for these activities, and encourage Europe to do the same. Weak penalties for money-laundering scandals only perpetuate the problem. Additionally, targeting key offshore nodes for illicit Russian activity under Section 311 of the PATRIOT Act is a powerful tool that complement sanctions. Treasury's determination that Latvia's ABLV Bank was a foreign financial institution of primary money laundering concern demonstrated this, spurring reform in Latvia and highlighting systemic European vulnerabilities.

Finally, we need to identify our own asymmetric advantages and go on offense. Putin and his cronies rely on the Western financial system to protect and grow their ill-gotten gains, even while they seek to weaken us. This gives us leverage, and we should use it. Anders Aslund has argued that the best way of undermining "Putin's authoritarian and kleptocratic regime is transparency, shining light on this anonymous wealth" held in our countries.[56] Targeted sanctions on Putin's cronies may have limited utility as an effect on Russia's economy, but if applied correctly could affect Putin's calculus – and potentially his own wealth.[57] We can do more to cut off access to our financial systems unless Putin and his cronies change their behavior. The Global Magnitsky Act also provides a powerful avenue to impose costs on government officials or senior associates of government officials if they are complicit in "acts of significant corruption." Such designations send a strong message that there are consequences for corrupt behavior, and the Administration should make better use of this tool. Several EU countries[58] have enacted their own Magnitsky Acts, and the U.S. should encourage others to follow suit, while the EU looking to develop a European-wide framework. We should not allow Putin and his cronies to simultaneously attack our system of government while exploiting it for their own benefit.

Conclusion

The United States faces a multidimensional challenge from Putin's Russia and its use of asymmetric tools to undermine democracies and weaken transatlantic institutions. Successfully defending against and deterring these activities requires an approach integrated across the U.S.

---

[54] Kirschenbaum, Joshua, and Nicolas Veron. "A Better European Union Architecture to Fight Money Laundering." *Bruegel*, 25 Oct. 2018. Web. 17 May 2019.

[55] "Fatal Inaction: Swiss Government Has Shied Away from Regulating the Commodities Sector since 2013." *Public Eye*. Berne Declaration, 29 Nov. 2018. Web. 17 May 2019.

[56] Aslund, Anders. "The Illusions of Putin's Russia." The Atlantic Council. 6 May 2019. https://www.atlanticcouncil.org/blogs/ukrainealert/the-illusions-of-putin-s-russia

[57] The classified list of Russian oligarchs created by the Treasury Department pursuant to CAATSA could provide a roadmap for such targeted sanctions.

[58] These include Estonia, Latvia, Lithuania, and the United Kingdom.

government and coordinated with our allies. It will also require mustering the political will to address the loopholes in our own systems that allow many of these activities to proceed unimpeded. Russia's undermining of democracy is a matter of bipartisan concern. It is past time for the U.S. government to recognize the serious national security threat posed by the actions of Putin's Russia, including malign financial influence and economic coercion, and to take the necessary steps to defend the United States and our allies.

Appendix A

Jamie Fly, Laura Rosenberger, and David Salvo. *Policy Blueprint for Countering Authoritarian Interference in Democracies.* June 26, 2018. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Policy-Blueprint.pdf

Mr. KEATING. Ms. Conley.

STATEMENT OF MS. CONLEY, SENIOR VICE PRESIDENT, EUROPE, EURASIA, AND THE ARCTIC, DIRECTOR, EUROPE PROGRAM, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, FORMER DEPUTY ASSISTANT SECRETARY OF STATE IN THE BUREAU OF EUROPEAN AND EURASIAN AFFAIRS, U.S. DEPARTMENT OF STATE

Ms. CONLEY. Thank you, Chairman Keating, Ranking Member Kinzinger, distinguished members of the committee.

Using a variety of tools, from corruption to influence operations, the Kremlin undermines and weakens democracies, rendering them simply unable to respond promptly to Russia's military actions and making them so beholden to the Kremlin that the country will actually support Russia's interests over its own.

The reason we at CSIS study Russian tactics in Europe is to prevent them from working effectively here in the United States or, hopefully, to prevent them from happening in Europe.

I would like to offer a note of caution, however. We are prone to give a little too much weight and acknowledgement of the so-called brilliance of Russian malign influence operations. Sometimes they are just quite clumsy and amateurish.

But they use all of their tools persistently and purposefully, and they use all available means of influence. This can be very overwhelming to us and to the American people. In other words, we simply do not connect our dots very well.

I want to give three framing points and then dive into two issues that I am particularly concerned about as I look toward the 2020 U.S. Presidential election.

No. 1, the average American does not know that we are in a daily battle to preserve and protect the integrity of our democracy. We are at war.

But this is a very different kind of war because the main battle space is a fight for the integrity of the American mind, and this is why it is so challenging.

Russian malign influence is designed to alter how we think about ourselves and our democracy and to deepen our distrust as well as our disgust.

It seeks to touch and shape every aspect of our lives—what we read, our personal preferences, and to make us doubt what we believe in. It is designed to make us very, very angry at one another.

And the third point is it uses our weaknesses. That is Russia's strength—our weaknesses. So polarization and partisanship are our greatest weaknesses and I am so glad this committee continues to exhibit the leadership of bipartisanship.

Polarization is evident in Europe today. We are also not structured to fight this battle. We are structured to fight terrorism and terrorism financing. We are not structured to fight malign influence and its many manifestations.

So as we prepare for 2020, let me offer two thoughts. I think we are increasingly going to see U.S. voices and U.S. organizations that will be the key disseminators of Russian malign disinformation with messages targeting vulnerable and divided U.S. communities.

This is going to look a lot like domestic election campaign messaging and it will likely be accompanied by hard-to-refute deep fake videos, audio, and image files.

I am particularly concerned about U.S. citizens and organizations wittingly or unwittingly becoming under the increasing threat of malign influence, faith-based and ultra conservative organizations, and, of course, opaque financial support of key U.S. influences, which my colleagues have done a great job in explaining how that is such a powerful part of Russia's toolkit.

Just very briefly, over the last decade the Kremlin has adopted a very compelling ideological narrative to mask its kleptocratic authoritarianism. Mixing pre-Soviet, Soviet, and orthodox ideologies, they have weaved together nationalism, patriotism, and faith, and Vladimir Putin and the Russian Orthodox Church are truly the embodiment of an anti-Western anti-individualistic, xenophobic, perversion of capitalism.

They have taken this one step further and they link Vladimir Putin's leadership to the biblical incarnation of the Third Rome or the restoration of the Third Temple in Jerusalem.

If you thought the Soviet Union was the godless communism, this is a very powerful messianic and mystical vision of its domestic and foreign policy. It is furthered by the Orthodox Church.

I have seen this work in Montenegro, in Serbia, in Bulgaria. I have seen it work across the board. It touches every aspects of people's lives. Their faith is an important part of their lives. But this is a source of concern to me as we have our own challenges in separating ourselves in our faith-based views.

Finally, in my few moments—I am sorry, my voice is leaving me here—just to followup on the very impressive video of Mr. Heinz-Christian Strache, we did an entire case study on Austria in our most recently publication, "The Kremlin Playbook II: The Enablers."

This does not surprise me, and we cannot continue to articulate the problem. We have to start solving it. Congress has to pass ultimate beneficial ownership. We have to treat financial transparency and money laundering as the challenges to America's national security that they are.

We can fight this. We can win this battle. We can go on the offensive. But we have to restore confidence in our own democracy first.

Thank you so much.

[The prepared statement of Ms. Conley follows:]

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the

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

"Undermining Democracy: Kremlin Tools of Malign Political Influence"

A Testimony by:

Heather A. Conley

Senior Vice President for Europe, Eurasia, and the Arctic

Center for Strategic and International Studies (CSIS)

May 21, 2019

2172 Rayburn House Office Building

Chairman Keating, Ranking Member Kinzinger, distinguished members of this subcommittee, thank you for inviting me to speak on an issue of significant importance to the American people. We must better understand Russia's sweeping and systematic malign influence operations, which support anti-democratic and anti-Western forces in Europe and the United States. Using a variety of tools, from corruption to influence operations, the Kremlin undermines and weakens democracies, rendering them unable to respond promptly to Russian military actions or making them beholden to the Kremlin to such a point that a democratic country will support Russia's interests over its own. And this is why we study Russia's malign tactics in Europe: to prevent them from working effectively in the United States, and vice versa.

Russia is undoubtedly the adversarial power which is the most advanced and adept at using malign influence as a tool of statecraft. The Kremlin uses a comprehensive array of influence tools that have been honed for well over a century, including from its experience with Soviet-era active measures. These tactics are now enshrined in Russian military doctrine known as New Generation Warfare (NGW). But today there is greater urgency to the Kremlin's use of malign influence as it must alter the policy stances and democratic orientation of the United States and Europe before the West—or Russian internal dynamics—directly challenge Mr. Putin's political survival.

A note of caution is in order: we are prone to giving too much weight to the "brilliance" of Russian malign influence operations. Oftentimes they can be quite clumsy and amateurish, but because these tools are used persistently and they penetrate all available means of influence that are not well understood by the target, they appear overwhelming in nature both to the U.S. government and the American people. This is because we face two key challenges in this fight. First, the U.S. government is structurally designed to fight terrorism and not domestic malign influence campaigns. Second, as the American people lose faith and confidence in their democratic leaders and institutions and become more politically divided, the Kremlin's clumsy efforts can achieve a level of success even they could not have imagined.

Therefore, the true challenge lies in understanding the persistent and penetrating nature of the Kremlin's efforts to render a democracy so helpless that it cannot defend its own sovereignty or national interests. Like the U.S. government, we in the think-tank community struggle to grasp the totality of the challenge. International research in this space tends to home in on one or two elements of NGW, typically its most pressing and visible manifestations: disinformation, illicit finance, corruption, and election interference. Our research at the Center for Strategic and International Studies for the past four years, in collaboration with our European partners at the Center for the Study of Democracy—the two *Kremlin Playbook* volumes—has focused on the tactics of Russia's malign economic influence in Europe, with special attention to the use of corruption and illicit finance to alter a country's political orientation. My fellow witnesses have done great work in the disinformation space. We can put the pieces together after the fact, but struggle to preemptively understand the challenge. And this is in part why the Kremlin has been so effective.

The American People Must Understand We are at War

The average American does not know that we are in a daily battle to preserve and protect the integrity of our democracy. We take many things for granted, particularly the health of our democratic system and the national security requirement for bipartisanship on significant international issues. If the American people understood that we are facing a new kind of war, a greater sense of patriotism and duty about what is at stake would be awakened. Similarly, when the United States entered the Second World War, millions of citizen soldiers had to be made aware of what was at stake and who the enemy was. To help these citizen soldiers, the U.S. government produced information pamphlets and slogans with detailed instructions to all those who served. Perhaps the slogan with the most popular resonance was "loose lips sink ships," which summarized the following written instructions:

"THINK! Where does the enemy get his information—information that can put you, and has put your comrades, adrift on an open sea; information that has lost battles and can lose more, unless you personally, vigilantly, perform your duty in SAFEGUARDING MILITARY INFORMATION?"

I recommend we modernize the old "loose lips sink ships" to fit 21st century threats: "If the facts are not complete, delete!" Or: "Truth and trust make America strong; lies and fear are just plain wrong!"

Can you imagine if every social media platform today were required to have the following disclaimer on every one of its posts as an update to the World War II instruction: "THINK!: What is the origin of the information you have just received? Is it true? Don't share it if you can't prove it!"

Although this sounds ridiculous, a regain in patriotism and awareness is urgently needed to combat Russian malign influence alongside an increase in trust, transparency, and accountability from the government.

The Battle for the Integrity of the American Mind

In February of this year, an advisor to Russian President Vladimir Putin, Vladimir Surkov, succinctly summarized the nature of the challenge before us. It bears repeating:

> *"Foreign politicians talk about Russia's interference in elections and referendums around the world. In fact, the matter is even more serious: Russia interferes in your brains, we change your conscience, and there is nothing you can do about it."*[1]

[1] Cristina Maza, "Vladimir Putin's Adviser Tells Americans: 'Russia Interferes in Your Brains, We Change Your Conscience'," *Newsweek*, February 12, 2019, https://www.newsweek.com/russia-president-vladimir-putin-election-americans-1327793.

Russian malign influence is designed to alter how we think about ourselves and our democracy and to deepen our distrust. It seeks to touch and shape every aspect of our lives—what we read, our personal preferences—and to make us doubt what we believe in. It is also designed to make us very angry at one another. Ultimately, this interference in our brains will result in the American people losing faith in the country's founding ideals and in our unique 243-year experiment in democracy. If this attack is successful, we will simply resign ourselves to the idea that we are no different from Russia; in other words, that we are morally equivalent, which makes it much easier to find accommodation with the Kremlin (which in reality means the United States will harm its own national security interests to accommodate the Kremlin's interests).

It bears repeating that Russia is not the original cause of American doubts, fears, and uncertainties about ourselves and our democracy. But it expertly identifies these feelings, amplifies fear and division, and fully exploits distrust. If Americans are unified and confident, the Kremlin's strategy lands on fallow ground. However, if we are divided and fearful, if we distrust our institutions and leaders, Russian malign influence can grow like an invasive species. And in our current frame of mind, we have been aiding and abetting the spread of this species.

In other words, we can talk about Russian tools and tactics all day long, but we simply lose valuable time that could be spent strengthening our institutions and restoring confidence in our democracy.

The United States' Weaknesses are Russia's Strengths

There is such great irony to the "success" of Russian malign influence in the United States and Europe today. U.S. military and economic strengths are unmatched globally and Europe has great economic power, while Russia's economic and demographic picture is grim and will significantly worsen without substantial political and economic reform. Yet, America's and Europe's societal weaknesses and divisions are profound today.

The Kremlin's ultimate success in the 2016 U.S. presidential election can be attributed to these weaknesses, which Russia was able to exploit:

1) We did not sufficiently protect our election infrastructure because we did not anticipate Russia would take these steps; our national security apparatus is configured to fight terrorism, not malign influence; partisan divisions prevented a unified message to the American people; and the level of distrust between the state and federal level did not allow us to anticipate and proactively address the problem;
2) Presidential campaigns did not take proactive measures to enhance the cyber-protection of their networks;
3) Tragically, one presidential campaign's staff did not believe it was wrong to accept illegally-obtained material from a foreign adversary (here is where a warning "THINK!

> Where did the enemy get their information?" would have been useful had there been sufficient patriotism on hand).

Important and hard lessons have been learned from 2016 and incorporated in the defense of the 2018 midterm elections; unfortunately, Russian malign tactics have evolved as they persistently probe weaknesses and exploit tactical opportunities. We are fighting the last battle and not fully anticipating or preparing for the coming one, offering excuses rather than addressing national vulnerabilities.

Preparing for the Coming Battle

As the Kremlin amplifies our doubts and fears about our democracy and our world, it will increasingly seek out U.S. voices and organizations to disseminate Russian malign disinformation with messages targeting U.S. communities that are vulnerable to division (which may look very similar to domestic election campaign messages). These will likely be accompanied by hard-to-refute 'deep fake' audio, video, and image files. The Director of National Intelligence and the director of the Federal Bureau of Investigation have already warned this Congress about the use of deep fake material that will be used to sow seeds of doubt through American outlets and social media.[2]

To better prepare for the challenge, I would like to highlight two specific areas in which I am particularly concerned U.S. citizens and organizations, wittingly or unwittingly, will come under increasing threat of Russian malign influence: (1) faith-based and ultra conservative organizations; and (2) opaque financial support for key U.S. influencers.

Vladimir Putin, True Defender of Tradition and Conservative Ideas. Since the collapse of its Communist identity, the Kremlin has adroitly crafted a compelling ideological narrative to mask its kleptocratic authoritarianism and to ensure that no one mistakes the country for "just another regional power" with nuclear weapons. Mixing pre-Soviet, Soviet, and Orthodox ideologies that weave together nationalism, patriotism, and faith, Vladimir Putin has restored the concept of Russia as a unique neo-Eurasian civilization—one which is neither part of the West or the East, but its own unique civilization. This narrative is intensely anti-Western, anti-individualistic, and a perversion of capitalism. It has been shaped by Russian ultra-nationalist Aleksandr Dugin, who took this faith-based ideology one step further by suggesting that today's Russia, under the leadership of Vladimir Putin, is the Biblical incarnation of the Third Rome or the restoration of the Third Temple in Jerusalem.[3] The Kremlin has replaced a "godless" Communist ideology—as it was typically referred to during the Cold War—with a powerful messianic and mystical vision of its domestic and foreign policy.

---

[2] Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Office of the Director of National Intelligence, January 29, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf.

[3] Ulrich Schmid, "The New Third Rome: Readings of a Russian Nationalist Myth," *Scando-Slavica* 63, no. 2 (2017), 235-238.

In 2014, Patriarch Kirill of Moscow and Primate of the Russian Orthodox Church drew a direct line from Saint Prince Vladimir, the leader who brought the Orthodox faith to Russia and Ukraine, to Vladimir Putin. Patriarch Kirill has modernized the tsarist-era slogan "For the Faith, the Tsar and the Fatherland" by fusing into one the Russian Orthodox Church, Vladimir Putin, and the survival of the Russian state. Together, President Putin and the Russian Orthodox Church constitute the true defenders of the Slavic world, of traditionalists who oppose globalization and modernity, and of the faithful of Christendom who are the true conservatives against the liberal, democratic, and individualistic decadence of the United States and Europe. As Patriach Kirill argued in 2014:

"If they wrap a person with soft power, lure him with the sweet life, contrasting his poorness to wealth, which they possess only because they are different—then someone, especially among the young, may tremble. [...] If such thoughts obsess our people, we will lose Russia. [...] May God save the historical Rus, our brother Slavic nations."[4]

These dynamics may seem like concerns that are internal to Russia. But it is crucial for us to understand that this idea of defending traditional and conservative values has enormous resonance with many in the United States who may agree that these values, as well as their faith and identity, are "under attack" by modernity and the speed of societal and demographic change. Many Americans may not realize when they are the targets and recipients of Kremlin-produced messages via affinity chat rooms and social media because they share similar views regarding the perceived "decadence" of modern society. Freedom of religion and the separation of church and state dictated by our Constitution are sacrosanct, but we must understand and warn the American people that Russian malign influence will seek to exploit and amplify all societal divisions, including those that relate to faith.

The most egregious example of this interplay is the U.S.-based World Congress of Families and its overt interactions with Aleksandr Dugin and with ultra-nationalist Konstantin Malofeev. Malofeev, a Russian oligarch with close ties to the Kremlin, reportedly sponsors much of the World Congress of Families' European activities and its interactions with European far-right parties.[5] The organization's ties spread across Europe; it supported a petition to organize a referendum in Romania for a constitutional amendment that would define marriage as between a man and a woman, which is a controversial issue in Romania.[6] One of the organizations that played a central role in the Romanian referendum in 2018, Coalition for Family, is part of a

---

[4] Dmitry Adamsky, *Russian Nuclear Orthodoxy. Religion, Politics, and Strategy* (Stanford: Stanford University Press, 2019), 228.
[5] Madalin Necsutu, "Moldova to Host Global Christian Right-Wing Congress," *Balkan Insight*, January 23, 2018, https://balkaninsight.com/2018/01/23/moldova-to-host-world-congress-of-families-before-elections-01-23-2018/.
[6] "Petition in Support of Romania's Defense of Marriage," World Congress of Families, May 17, 2008, http://web.archive.org/web/20080517125923/http:/www.worldcongress.org/WCF/wcf.leadership.romania.0804.htm.

broad network of ultra-conservative activists in the United States and in Russia (including Kremlin-affiliated oligarchs) who have pushed similar referendums across Europe.[7]

The comingling of financial and religious interests is particularly visible between Messrs. Dugin and Malofeev. Dugin is the editorial director of Malofeev's far-right Tsargrad (the Orthodox reference to Constantinople, which evokes Third Rome imagery) TV channel. Malofeev founded Marshall Capital Partners, one of the leading Russian investment groups, and St. Basil the Great Charitable Foundation, the largest Russian Orthodox charity that provides humanitarian assistance to religious organizations and affinity causes. Malofeev exemplifies the ties between economic influence and religious or societal influence, as Marshall Capital supports the Foundation financially.[8] Dugin and Malofeev are both under U.S. sanctions for their involvement in the Russian invasion of Crimea and aggression in Eastern Ukraine (Malofeev is also under EU sanctions).[9]

Konstantin Malofeev and the Russian Orthodox Church are frequently cited in our research to explain the role of Russian economic and political influence in Europe. We have observed the use of the Russian and Serbian Orthodox Churches as effective tools of influence in Serbia, Bulgaria, and Montenegro.[10] Prior to Montenegro's accession to NATO, Patriarch Kirill voiced his concerns publicly about NATO membership.[11] The Serbian Orthodox Church in Montenegro, referred to by some Montenegrin politicians as Montenegro's largest opposition force, also opposed membership and released a statement noting that "[i]t is [its] duty *in the name of the Church* [italics added] that gave birth to Montenegro . . . to say that it is necessary that such a historic decision, like the decision on independence, is made by all citizens in a free referendum, and not simply by pressure from the ruling clique."[12] Such statements seek to worsen internal divisions, erode confidence in leaders and democratic institutions, and demonstrate that "decadent" Western democracy and EU and NATO membership are incompatible with Slavic identity and the Orthodox faith. The comingling of identity and religion resonates powerfully in all societies.

Does Democracy Have a Price? The spread of Russian malign influence is also made possible by corruption, illicit financing, and the weakness of Western financial institutions and the industries that service Russian illicit funds. Greed, corruption, tax evasion, and non-transparent

---

[7] Claudia Ciobanu, "'New World Order': The 'Natural Family' Franchise Goes Global," *Balkan Insight*, November 21, 2018, http://www.balkaninsight.com/en/article/new-world-order-the-natural-family-franchise-goes-global-11-05-2018.

[8] Maksym Bugriy, "Hot Issue – Konstantin Malofeev: Fringe Christian Orthodox Financier of the Donbas Separatists," *The Jamestown Foundation*, August 8, 2014, https://jamestown.org/program/hot-issue-konstantin-malofeev-fringe-christian-orthodox-financier-of-the-donbas-separatists/.

[9] "Russia Sanctions Tracker," Center for Strategic and International Studies, https://russiasanctionstracker.csis.org/.

[10] Heather A. Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Lanham: Rowman & Littlefield, 2016); Heather A. Conley et al., *The Kremlin Playbook 2: The Enablers* (Lanham: Rowman & Littlefield, 2019); Heather A. Conley and Matthew Melino, "Russian Malign Influence in Montenegro: The Weaponization and Exploitation of History, Religion, and Economics," Center for Strategic and International Studies, May 14, 2019, https://www.csis.org/analysis/russian-malign-influence-montenegro.

[11] Dusica Tomovic, "Serbian Church Urges Montenegro NATO Referendum," *Balkan Insight*, January 5, 2016, https://balkaninsight.com/2016/01/05/ser-bian-church-urges-montenegro-to-hold-referendum-on-nato-01-04-2016/.

[12] Ibid.

behavior—from foreign agent registration to "golden visas"—are *de rigueur* for the West, which is why Russian state-owned companies as well as security, intelligence, and organized crime networks find it so attractive and easy to exploit: they recognize a familiar environment. In some cases, it is difficult to see where Western financial practices end and Russian kleptocracy begins, which provides another powerful argument for the Kremlin that Western democracies are really no different from Russia. From his experience as a KGB officer, Vladimir Putin firmly believes that every person has a price, particularly influential people, and he is likely surprised by how cheap that price can be.

Western banks such as Danske Bank, Swedbank, and Deutsche Bank have welcomed Russian and post-Soviet funds into their coffers, later to be "laundered" through the international financial system. These banks facilitate capital flight out of Russia, which ultimately further impoverishes the Russian people. Yet these institutions retain their profitability and reputation—for a time, at least. As we have documented in our report *The Kremlin Playbook 2: The Enablers*,[13] corporate service providers, attorneys, accountants, and wealth managers are eager to create shell corporations or subsidiaries to avoid or evade taxes and to encourage more funds to come to their financial centers. Real estate is purchased without transparency into beneficial ownership. These funds and assets are being used to harm our country, yet we act as if this is of no concern. European enforcement in particular seems lax and political patrons (some of whom receive illicit funds themselves) can shield these deals from investigations. These illicit flows jeopardize the integrity of open market economies, creating threats to national security.[14] Furthermore, by abusing our opaque system, corrupt officials and individuals can hide or launder the profits of illegally-obtained funds (sometimes stealing from their own people) and put them beyond the reach of law enforcement and tax authorities; this depletes state revenue and insulates the perpetrators from justice, questioning the effectiveness of the whole system.[15] It is therefore no wonder that confidence in democracy is low; this must stop.

We must place the love of our country ahead of our avarice. We must pass new laws that require greater transparency of ultimate beneficial ownership, such as the one that is being considered before the House Financial Services Committee. We need new financial tools, more enforcement resources, and greater focus by the Justice and Treasury Departments to prosecute complex, multi-jurisdictional money-laundering schemes before they are discovered ten years and 200 billion euros too late. Of course, not all Russian transactions or business dealings are illicit, but as Russian foreign direct investment into our economies grows, so does the Kremlin's political influence. Greater transparency of financial transactions with law firms, think tanks, public relations firms, and lobbyists must be prioritized. Special attention must be given to the financial support of all organizations that can feed division in our public sphere (even unwittingly; the

---

[13] Conley et al., *The Kremlin Playbook 2*.
[14] Bureau for International Narcotics and Law Enforcement Affairs, *Money Laundering and Terrorist Financing – A Global Threat*, (Washington, D.C.: U.S. Department of State, 2005).
[15] See charting of this nexus between illicit finance and national security in Conley et al., *The Kremlin Playbook 2*, 17.

most innocuous ones can sometimes be the most harmful) and political campaigns, particularly figures close to presidential candidates.

A War We Must Win

We have a better understanding today than we did in 2016 of the Kremlin's tools and how it uses them to exploit our weaknesses. We need to anticipate and mend those weaknesses in 2020. I have argued that the faith-based community and the lack of transparency in funding influential organizations and voices may be new targets of or loopholes for Russian malign behavior in the United States, as they have been in Europe. We need strong, bipartisan messages on how Russian tactics may target U.S. citizens in the run-up to the 2020 election. We need strong laws that enhance our financial transparency and severely punish those who prioritize their love of money over their love of country. We need to promote unity rather than fuel the divisions that only help the Kremlin fulfill its malign aims. We must stop facilitating their malign activities.

My message to this subcommittee today is: "THINK! Have you personally, vigilantly, performed your duty in SAFEGUARDING THE UNITED STATES FROM RUSSIAN MALIGN INFLUENCE?"

Mr. KEATING. Mr. Doran.

STATEMENT OF MR. DORAN, PRESIDENT & CEO, CENTER FOR EUROPEAN POLICY ANALYSIS

Mr. DORAN. Good morning, Chairman Keating and Ranking Member Kinzinger, and members of the committee.

I am Peter B. Doran, the CEO and president of the Center for European Policy Analysis, or CEPA. It is an honor to speak with you here today.

I have already submitted my written testimony for the record so I would like to encapsulate it with one overall message for this committee.

Right now, the Russian government believes that it is in a battle against the U.S.-led economic and international order. The Russian government believes it is winning this battle and they are doubling down on their strategy to undermine Western democratic systems with tools of malign political influence.

Based on the research and reporting at my organization, CEPA, I can confirm for this committee the Russian government aims to attack Western political cohesion by using the very strengths of our liberal democratic order against us.

Russia has tried to subvert and allegedly topple, in one case, governments. It has peddled disinformation and called it free speech and it has used corruption for political purposes under the cover of neutral business.

These efforts are not isolated. Rather, they are the products of a coherent unified strategy that was developed at the highest levels of the Russian government.

Mr. Chairman, I am the co-author of a CEPA analytical report that I have submitted for the record. This report details how Russia seeks to weaken democracy by spreading chaos beyond its borders.

Chaos is Russia's strategy. The Kremlin toolkit of financial corruption, disinformation, and influence operations are the means of activating that strategy.

In doing so, Russia targets the things that make us strong—pillars like a solidarity between our allies, the integrity of our political systems, and the unbeatable dynamism of our free market economies.

I would stress for the committee that Russian leaders also exhibit a strong preference for deploying their malign toolkit in the energy arena, and when it comes to the corrupting combination of money and influence, I can think of no better example than Russia's Nord Stream 2 pipeline.

This Congress is aware of that pipeline. It is the crown jewel of Russia's malign offensive in Europe. Vladimir Putin knows exactly what he is doing. He wants to Putinize us by normalizing corruption.

Mr. Chairman, I thank you for sharing that visual aid at the start of this hearing because it offers us an example of what is taking place in Austria.

Meanwhile, in Germany, I can confirm for the committee that the Nord Stream 2 pipeline is not just a commercial deal as project promoters falsely claim. It will normalize a new long-lasting cor-

rupting influence over our friends in Europe, especially our essential ally, Germany.

So what do we do? How do we defeat Putin's strategy against us? Well, first, we need to understand that Russia's use of political corruption, disinformation, and malign influence has a purpose—to divide and weaken us.

Second, the Russian government's strategy reveals to us what its leaders fear—the pillars of our power, especially when used in coordination with allies.

Third, Vladimir Putin wins when our internal debates about Russia become polarized and partisan. As long as we are fighting each other, we are advancing the Kremlin's agenda.

And fourth, U.S. and European policy must be dramatically reordered when it comes to the sequence of carrots and sticks we offer to the Kremlin. We need a lot more sticks and no consideration of carrots or open-ended partnership with Russia until we see undeniable signs that it has changed strategy.

Let us not give carrots to those who would do us harm. When it comes to sticks, the costs we put upon Russia for deploying chaos against us must rise. I would agree with my co-witnesses here.

Vladimir Putin needs to become more uncertain of our next move than we are of his. So what might costs look like?

Well, let us finally show that we are serious. Let us finally put sanctions on Nord Stream 2. America can and should take this action today.

Sanctions on Nord Stream 2 are the first, best, and most immediate way to show the Kremlin that we mean business. And when it comes to money, I would ask the committee to remember this.

Russia's banks are just as dangerous as Russia's tanks. So let us also prepare effective mechanisms to prevent the buying and selling of Russian sovereign debt in our markets should Russia escalate against us in the future.

Last, but perhaps most importantly, I would encourage this Congress to continue its essential support for this administration's commendable efforts to counteract Russian State-sponsored disinformation and the fake news that the Kremlin injects into our Western body politic.

This support is vital in counteracting Russia's strategy. Mr. Chairman, every strategy has a weakness, including chaos. The Kremlin's malign toolkit of chaos can be defeated.

We just have to get a lot smarter about how we go about it. I thank you for the time and I look forward to your questions.

[The prepared statement of Mr. Doran follows:]

Written Testimony of Peter B. Doran

President and CEO

Center for European Policy Analysis

HOUSE COMMITTEE ON FOREIGN AFFAIRS

Subcommittee on Europe, Eurasia, Energy and the Environment

"Undermining Democracy: Kremlin Tools of Malign Political Influence."

May 21, 2019

Good morning, Mr. Chairman, Ranking Member, and Members of the Committee. I am Peter B. Doran, President and CEO of the Center for European Policy Analysis (CEPA). It is an honor and a privilege to speak with you. I want to thank you for inviting me here today.

I have already submitted my written testimony for the record, so I'd like to encapsulate it with one overall message for the Committee:

Right now, the Russian government believes that it is in a battle against the U.S.-led economic and international order. Its leaders believe that they are winning this battle. And they are doubling down on their strategy to undermine Western democratic systems with tools of malign political influence.

Based on the research and reporting at my organization, CEPA, I can confirm for this Committee that the Kremlin aims to undermine western political cohesion by turning the very strengths of our own liberal democratic order against us. Russia has tried to undermine—and even topple in one case—governments, sowed discord and confusion among our allies by peddling disinformation under the guise of free speech, and used corruption for political purposes under the cover of neutral business.

Importantly, these efforts are *not* isolated. Rather, they are the products of a coherent, unified strategy that was developed at the highest levels of the Russian government. That strategy is well funded and—at times—effective. I am confident that we can beat it, but we must deploy a well-planned, coordinated, and serious response.

Mr. Chairman, I am the co-author of a CEPA analytical report that I've submitted for the record. This report details how Russia seeks to undermine democracy by spreading chaos beyond its borders. Chaos is Russia's *strategy*. The Kremlin's toolkit of financial corruption, disinformation, and influence are the *means* of activating that strategy.

Russia's leaders are gambling that global competition with us will mean: the side which can cope best with disorder will win. By activating its malignant toolkit, the Kremlin is attempting to offset its weaknesses relative to our abundant strengths. This is why Russia targets the things that

make us strong—pillars of Western power like solidarity between allies, the integrity of our political systems, and the unbeatable dynamism of our free-market economies.

I would stress for the Committee that Russian leaders also exhibit a strong preference for deploying their malignant toolkit in the energy arena. Moscow hopes that we will simply debate the basic market economics of its energy infrastructure proposals, while turning a blind eye to the corrupting combination of money and influence that Russia builds into each of these physical projects. And when it comes to this combination, I can think of no better example than Russia's Nord Stream 2 pipeline – the crown jewel of Russia's malign energy offensive aimed at undermining transatlantic security.

As this Congress is aware, Russia is presently attempting to build the multi-billion-dollar Nord Stream 2 gas pipeline into Germany. If the Kremlin succeeds, Nord Stream 2 will become a new vector for Russia to spread money and influence across Europe. By completing this pipeline, Russia will make essential allies like Germany more financially and economically dependent on the Kremlin. Vladimir Putin knows exactly what he is doing. Nord Stream 2 is not just a commercial deal, as project promoters falsely claim. It will establish a new, long-lasting, corrupting influence over our friends.

Nord Stream 2 is not about bringing significant new gas volumes to Germany or Western Europe. Nord Stream 2 is about the harming our Ukrainian partners and allies while exporting and *normalizing* malign influence in the form of financial and economic dependency on Russia.

So what do we do; how do we defeat Putin's strategy against us?

First, we need to understand that Russia's use of political corruption, disinformation, and malign influence has a purpose: to divide and weaken us.

Second, it reveals what Russian leaders fear: our power (especially when used in coordination with allies), accountable democratic governance, and a rules-based international order. The Putin regime views all of these as an existential threat to its autocratic kleptocracy.

Third, Vladimir Putin wins when our internal debates about Russia become polarized and partisan. As long as we are fighting each other, we are advancing the Kremlin's agenda.

And fourth, U.S. and European policy must be dramatically re-ordered when it comes to the sequence of "carrots and sticks" offered to the Kremlin. We need a lot more sticks—and no consideration of *carrots* or open-ended partnership with Russia until we see undeniable signs that it has changed its strategy. Let's not give carrots to those who would do us harm. And when it comes to *sticks*, Vladimir Putin needs to become more uncertain of our next move than we are of his. Right now, that is not the case. The costs we put upon Russia for deploying chaos against us must rise. We will know when the costs on the Kremlin are high enough when Putin no longer deploys his malignant toolkit. So far, he is not letting up.

What might costs look like?

Let us finally take a stand and show that we are serious. Let us finally put sanctions on Nord Stream 2. America can take this action—today. Sanctions on Nord Stream 2 are the first, best, and most immediate way to show the Kremlin that we mean business. I would continue to encourage this Congress to do everything in its power to press the Administration, notably the Treasury Department, to use all financial and legal tools at their disposal to stop Nord Stream 2, including sanctions.

Let us also prepare effective mechanisms to prevent the buying and selling of Russian sovereign debt in our markets should Russia escalate against us in the future. As such, let us practice and publicize transatlantic "financial snap exercises." Armies already conduct "snap exercises" to demonstrate their readiness and resolve to deter an adversary. The same must become true when it comes to money. Russia's banks are just as dangerous as Russia's tanks. And the Kremlin will take notice when it sees U.S. and European authorities showing similar readiness to act against Russian aggression via the financial realm.

Lastly, I would encourage Congress to continue its support for this Administration's commendable efforts to counteract state-sponsored disinformation and the "fake news" that Russia injects into our body politic. At CEPA, we often think of Russian disinformation as a virus. In order to defeat a virus, you need to understand what it is and how it evolves. Regular, targeted analysis of the reach and impact of Russian propaganda is essential. People can also inadvertently contract a virus or spread it—unless they are educated on how to protect themselves and others. The same is true of disinformation. And when it comes to developing a cure, I would offer that Americans can learn a lot from our allies in Central Europe and the Baltic States—allies who have long been exposed to disinformation and have developed resistances to it. Therefore, building greater transatlantic networks of experts inside and outside of government will be essential to achieving our end goal: developing a cure.

Mr. Chairman, every strategy has a weakness. The Kremlin's malignant toolkit of chaos can be defeated. We just need to get a lot smarter about how we go about it.

I thank you for the time and look forward to your questions.

Mr. KEATING. Well, thank you, Mr. Doran.

The chair will now recognize the ranking member for 5 minutes of questioning.

Mr. KINZINGER. Well, I thank the chairman and, again, I thank you all for being here.

Ms. Conley, you mentioned, you know, the structure and that is very correct and I think an important point to know. You know, the United States needs to now go from remembering the cold war, kind of a two-front war, to now basically two kinds of war—asymmetric and symmetric and, you know, being able to prepare for the big fight but also understanding we have to execute a fight against terrorism and also economically. So that is where I think some of that flexibility needs to come back.

Just a small point of disagreement. You mentioned ultra-conservative groups, and I would not disagree with that. But I think there is also groups on the left working on behalf of Vladimir Putin.

You just look at Code Pink's occupation of the Venezuelan embassy to support a basically dictator that is a puppet of Vladimir Putin. So I think it is just important to point out that this is really all spectrums and Russia uses all tools.

Mr. Doran, I want to ask you how the Russian tactics are evolving. You know, we have broadly grasped the existing hybrid warfare toolkit but what do we expect in the next generation of tactics?

Mr. DORAN. Thank you, Ranking Member.

I would say this. When we look at the elements of Russian malign influence I think you are absolutely correct to ask the evolution question.

Oftentimes at CEPA we think about these techniques as a virus. In order to understand a virus you have to first understand how it evolves and mutates, what you are dealing with.

Where I would stress for this committee to pay most attention to is the way in which Russia can compete against us for pennies on the dollar. Every single effort we put to counter them costs us more money than they require to attack us.

So on steps of evolving, Russia is limited only by the creativity of the GRU and some of their malign actors in Europe. I would not begin to speculate as to how a virus would evolve as much as I would about how Russia can evolve.

What I can say is that we need to stop playing whack-a-mole with the Kremlin and we need to raise the costs on Vladimir Putin so he does not deploy these techniques against us in the first place.

Mr. KINZINGER. Thank you. I think that builds into the idea of—I mean, look back. We hate this term—mutually assured destruction on the nuclear side was not a good thing. But I think we need to make it clear to the Russians that we can do to you what you can do to us.

That raises the cost on them. Vladimir Putin fears nothing more than losing his grip on power and I think we ought to threaten that that way.

So I also want to ask the whole panel, Russia's use of armed mercenary groups like the Wagner Group to secure their interests and support brutal dictators like Assad and Maduro is another example of their low-cost high-reward strategy to hinder our interests.

Our military has shown that we will respond to Russian aggressions from these groups when provoked as we did when we quickly obliterated a regiment of the Wagner Group in Syria.

However, the sanctions we have on officials connected with the group have not stopped the recent deployment of Venezuela and several sub-Saharan African countries.

I will start with you, Mr. Doran, and we can ask the whole panel. What would you suggest in terms of a more effective response against Russia's use of paramilitary groups like Wagner?

Mr. DORAN. Thank you, Ranking Member.

I would underscore my first position that we need to dramatically raise the financial costs on the Kremlin should we decide that they have escalated. If we determine, as a country, that Russia is using its paramilitary forces against us, I think the ending of the buying and selling of Russian sovereign debt in our markets is a good first step and I know that is a question before this Congress.

Mr. KINZINGER. Anybody else?

Ms. CONLEY. Congressman, I would argue we must make a declarative policy that the Wagner Group we recognize as a branch of the Russian military and treat it as a hostile action.

What is making Wagner so effective is that Vladimir Putin can immediately send those forces—he can achieve his political objective with military means. He is not threatening it.

He is doing it and stopping the U.S. He is stopping any advancement of the U.S. and its objectives and then we have to confront whether it is worth lives to fight that, and that is what he is banking on.

We have to make the costs greater. We have to—Russia right now is so extended in Syria and Central African Republic, within Venezuela. We have to make that—squeeze those costs and make them greater.

If they are going to expend themselves then we have to make that as painful as possible. But we also have to get our policy house in order and have clear policies with allies that can be more anticipatory rather than simply responding to Russia's quicker action.

Mr. KINZINGER. And I notice it got pretty quiet after the Syrians. Ms. Rosenberger?

Ms. ROSENBERGER. Yes, I was just going to add I agree with Heather that we need to recognize the role that Wagner is playing vis-a-vis the Russian government.

I would also note, though, that the key suspected financier and one of the key founders of the Wagner Group are actually both under U.S. sanctions already.

But what I think we need to do is look at how Wagner operates. It actually seems to operate based on resource contracts. So if we look in Syria, reports have indicated that Prigozhin and the Syrian government maintain a contract to grant Prigozhin a cut of profits from oil fields retaken by Wagner.

In Sudan, the group is reportedly providing security for gold mines. The group is also reportedly acting as personal security as military trainers in Africa.

So it speaks to the systemic nature again of the entire financial ecosystem and the corrupt nature that groups like Wagner are able to exploit in order to get these kickbacks.

Mr. KINZINGER. Thank you.

Dr. Carpenter, no offense, but I am out of time. So I will skip you, if you do not mind.

Thank you.

Mr. KEATING. Thank you. The chair will now recognize himself for 5 minutes. I just want to deal with something specific, if I can.

Hungary recently allowed a small Russian bank, the International Investment Bank, to open their new headquarters in Budapest. One of the chairmen of the bank has a longstanding tie with Russian intelligence agencies. What are the risks of this bank being headquartered in an EU and NATO-member State, No. 1?

No. 2, what can the United States and the EU do to respond to decisions by EU member States or non-EU members, for that matter, to increase these actions that increase the vulnerability in our overall financial systems?

Third, what tools do we have at our disposal, whether the U.S. alone or with allies, what tools do we have to eliminate or lessen these vulnerabilities?

I would like to just jump ball—whoever wants to go first.

Dr. CARPENTER.

Mr. CARPENTER. I am happy to start, Chairman.

I think this is a huge vulnerability for not just Hungary but for the entire EU because it is a potential Trojan Horse for Russian money laundering and covert influence.

So what can we do? Well, a number of things. A European wide anti-money laundering institution is probably the most important step that the Europeans themselves could take to regulate these sorts of—this sort of behavior and then investigate financial institutions like this one that emerge in their jurisdiction.

For us, we need to push back on Hungary more than we have been so far. Hungary has become a mini version of Russia. It is a kleptocratic and increasingly authoritarian system and we have—because it is an ally and because it is important, and it is, we have refrained from criticizing and from exerting leverage over Budapest. I think that is a mistake.

So I think on the geopolitical front we need to apply pressure on Hungary at the same time as we pursue some of these broader systemic solutions to money laundering and covert influence.

Mr. KEATING. All right.

Ms. Rosenberger.

Ms. ROSENBERGER. I would firmly endorse the need for creation of an EU wide anti-money laundering mechanism. Right now we have a gap between the European-wide financial system and the national level regulatory bodies. And so we do not—there is a mismatch in between the regulatory system and that needs to be urgently addressed.

And, again, I would completely endorse the need to push back much harder on Prime Minister Orban. I think the kind of treatment that he received here in the U.S. last week exactly undercuts what we need to be doing and the message we need to be sending.

Ms. CONLEY. So, Chairman, the IIB and the fact that the Hungarian government gave the IIB diplomatic immunity is a U.S., NATO, and EU policy failure.

It is quite interesting that even Mr. Strache mentions in the video about following Orban, Orbanism, and the play book that Mr. Orban has created.

I think it is time to now contemplate sanctioning select Hungarian officials. I think it is time to contemplate, as much as it grieves me, to limit Hungary's access to NATO classified information.

I think the—I think the risk now has become so great that we have to contemplate measures that would just be the last thing I would wish to contemplate.

But if we do not get serious about this, all it does is grow the problem. The Hungarian government has been warned by Members of Congress and the Senate about this and it goes absolutely unheeded. We have to take action.

Mr. KEATING. Well, the we that we are talking about I think is important, and I just want to drill down on NATO as a whole. You know, we all are aware of the enormous information sharing that is going on in regards to security and terrorist threats that exist with our NATO allies.

It is extraordinary. It is strong. It remains strong. Yet, we are not breaching this area of attack at all in terms of what our defences could be. We are not—we are not discussing it. So what can NATO do together? This, to me, seem critical. What can NATO do together to deal with this?

Ms. Rosenberger.

Ms. ROSENBERGER. I think it is a really critical question. So NATO has done more to look at nontraditional threats as part of its mandate. But I think it needs to go further.

No. 1, I think it needs to strengthen cooperation with the EU including on intelligence sharing. No. 2, I think that NATO needs to reemphasize what—this is an idea proposed by former U.S. Ambassador to NATO, General Doug Lute—needs to reemphasize Article 3, which is about resilience.

It is about every member of the alliance actually having the resilience to withstand and provide for the kind of defense needed and so many of the tactics that we see the Kremlin using are actually targeting these internal vulnerabilities. So resilience has to be a key part of the strategy.

Finally, I think the hybrid threat center that the EU and NATO have set up in Helsinki needs to do more to prioritize the kinds of tools and tactics that we are talking about today, it is doing great work on information operations and cyber attacks but energy and economic coercion is part of its mandate and it needs to take a higher priority on that.

Mr. KEATING. Thank you. I agree fully. We cannot do this alone. Since we reversed order of the opening questions, we will go—now go to Representative Albio Sires, who chairs the Western Hemisphere Subcommittee in the Foreign Affairs Committee.

Mr. Sires.

Mr. SIRES. Thank you, Mr. Chairman, and thank you for being here.

You know, all my life I keep saying this. While we sleep, the Russians plot—try to hurt us. And I have spent most of my life trying to wake people up and say hey, let's start paying attention.

You know, now they are playing in the Western Hemisphere. Look what is happening in Venezuela. If you look at Nicaragua, they sold Nicaragua 50 tanks last year—$80 million. I mean, that is the poorest country in the Western Hemisphere. They are playing in some of the other countries.

Where do you—now we also have in the Western Hemisphere the Chinese. Do you see any coordination between the Chinese and the Russians in the Western Hemisphere to destabilize some of these places?

Dr. Carpenter.

Mr. CARPENTER. So I would say in terms of overt coordination, I do not think we have evidence of that. But we, clearly, see mutually aligned interests in terms of supporting dictators like Maduro. Also the same thing happens in Syria.

In Europe, we see, for example, malign influence channels where the Chinese piggyback on Russian malign influence networks, and vice versa.

The closest example to coordination against a democratic State is, I believe, in June 2017 there was a series of coordinated cyber attacks against the South Korean government that were originating from Russia and China at the same time.

It is circumstantial evidence as to whether that was coordinated or just, again, they happened to have the same target. But, clearly, their interests align in terms of propping up teetering authoritarians and then also undermining democratic regimes whenever they can.

Ms. CONLEY. Congressman, I think what we are seeing across the board is Russia trying to re-enliven its former Soviet relationships certainly through arms exports. We are seeing that across the board—Middle East, Africa—as well as some of its economic contacts.

This is an area of understanding Chinese and Russian interaction, which is an area of research that we all I think have to do a much better job.

I would observe they are staying out of each other's way, to an extent, but what they are trying to do is prevent any change of regime. This is what frightens both Xi Jinping and Vladimir Putin the most. It is their own internal unrest unseating them someday.

So this is all about regime status quo and they will do what they need to do economically or militarily to try to preserve regime status quo wherever it may be, and certainly where it is important to the United States that is even a higher priority.

Mr. SIRES. Anybody else?

Ms. ROSENBERGER. I would agree, that I do not think we have seen enough evidence yet of overt coordination. But I do think, No. 1, there is the alignment of interests.

I do think it is important to understand that China and Russia have different long-term games. So whereas chaos and disruption is the goal of most of the Kremlin's activities, you know, that is in part driven by the fact that Russia is an objectively declining power.

I think that Heather was absolutely right to emphasize we cannot give Putin and his cronies more credit than they are due. This is largely a disruption strategy and that is relatively easy.

What Beijing is trying to do is actually a much longer-term, more strategic, and therefore, I think, even more nefarious game. It is harder to detect.

China is actually trying to not just weaken the international order in the short term but to construct something alternative in the long term, and that means that they are more careful.

They do not want to be caught. Putin often wants to be caught. And I think that that has different implications for the policy response.

Nonetheless, I completely agree with what Dr. Carpenter said. The Chinese often piggyback on the Russians' tactics and I think that is something for us to be very aware of.

Mr. SIRES. Do you see the rise of the right wing and populist parties in some of these countries as a result of Russia's effort?

Ms. CONLEY. I am sorry, Congressman. Can you repeat that, just at the very end? I did not——

Mr. SIRES. You have the rise of all these right wing or these extremists in some of these countries. Do you see the rise in that as a result of Russia's hand in some of these countries?

Ms. CONLEY. So, again, I would say the weakness exists already in this society. Many of these groups a decade ago would have been polling at 1 or 2 percent.

The economic crisis—the global economic crisis—fuelled great uncertainty. The migration crisis in Europe fuelled it even more.

So these groups—where Russia had made some long-term investments and funding them and encouraging them because they were against the European Union—they were against the United States—these parties now, because of the conditions, have grown and Russia is amplifying their message.

So it is not the Russians that are causing this. It is because of the internal dimensions in European societies. But Russia is amplifying it, helping those messages, helping to instill more division in the society and this is the creation of the chaos, the disruption—anything to make the West look bad—because the last thing President Putin wants is the Russian people to want what the West has because he can never give that to them and remain in power.

So he has to make the West look the absolute worst. And so he is just showing how horrible it is, how divided it is, how decadent it is, and then the Russian people will never want the West.

Mr. SIRES. Thank you. My time is up.

Mr. CARPENTER. If I could just add to that.

I think there is a pattern of evidence that shows that Russia is financially and also through other means supporting right wing groups, especially across Europe.

So if you look at the Jobbik far-right party in Hungary, if you look at a tiny little pro-Russian party in Poland called Zmiana, which was funded through laundered money that went through the Russian laundromat that was funnelled through banks in Moldova, ended up in Zmiana's coffers as a means of supporting this little fringe party but on the right to throw chaos, again, in the Polish political system, and we see this across the board.

The video of Strache and what has happened in Austria recently also indicative. So Russia bets on many horses but they look to the far right as one of the most disruptive elements in European politics.

Mr. SIRES. Thank you.

Mr. KEATING. Representative Greg Pence from Indiana.

Mr. PENCE. Thank you, Chairman Keating and Ranking Member Kinzinger.

I am going to actually ask a followup question to Congressman Sires but I am going to get there a little bit—in a different sort of way.

On May 9th, Chairman Keating and Ranking Member Kinzinger held a meeting on China's expanding influence in Europe and Asia—Eurasia. The witnesses laid out in detail how China, through the Belt and Road Initiative and their use of State-owned enterprises undermine U.S. interests and those of our European allies and partners.

As a member of the Transportation Infrastructure Committee, we even spoke about Chinese SOEs and BDYs specifically in the context of our domestic infrastructure work just 2 weeks ago.

But China is not alone in these types of activities. As we are talking about today, Russia is right there with them. This theme of Russia and Chinese convergent in Europe was my biggest and most concerning takeaway from our previous hearings.

Ms. Rosenberger, you addressed Russian ownership of assets in Europe States in your prepared testimony when you cite your fellow witness, Ms. Conley, saying, quote, "At a strategic level Heather Conley found in CSIS's 'Kremlin Play book' that countries where Russia's economic footprint was greater than 12 percent of GDP were valuable to Russian influence in State capture."

Here is my two questions as a takeoff. One, have Russia and Chinese found new ways to invest in countries' infrastructure to continue to hurt U.S. allies like private corporations, and two, to what degree are we observing Russia and Chinese cooperation in these private coercive economic tactics?

Start with you, Dr. Carpenter.

Mr. CARPENTER. So, again, Congressman, I would say that we have seen a certain degree of perhaps tacit coordination. When the Chinese government was looking at investing in the Port of Piraeus in Greece, one of the biggest ports in the world, the Russians were also very much interested in this as an infrastructure project.

I think the key for the Russians was to ensure that Piraeus was not bought by Western, especially American, investors, and so they were happy to see the Chinese move in there.

And then since, of course, there has been a huge tax evasion scandal that has surfaced as a result of Chinese goods flowing through that port.

Mr. PENCE. And you are referring to private investment of China and Russia?

Mr. CARPENTER. Correct. Well, investment by Chinese State-owned companies. So sort of parastatals, if you will.

We see competition now as U.S. investors are poised to develop the Anaklia Deep Water Port on the Black Sea coast of Georgia. Again, this interferes with the Chinese One Belt, One Road initia-

tive. They would like to be involved there. The Russians are also not happy about this investment.

So their interests often align and then we see sometimes a tacit coordination but, again, nothing overt at this stage.

Ms. ROSENBERGER. Thank you, sir. I think it is a really important question. I would caution personally that I do not believe there is such a thing as a private Chinese company that is engaged in overseas investment.

There are different kinds of arrangements. Some of them are State owned. Some of them have different kinds of relationships with the party State.

But I certainly do not believe, as somebody who has spent a good bit of my career on China, that there is such a thing of a private Chinese company that has the ability to engage in foreign investment and foreign trade activity.

Much of what we see through the Belt and Road Initiative is the use of market-distorting tactics in order to help provide for or facilitate foreign investment in targeted States.

This then provides a distortion in the market for other firms that are trying to compete so that the Chinese firms gain a foothold. They then are able to create dependencies.

That creates leverage—things like the debt trap, which I know you heard about in your hearing last week. These are all an ecosystem that becomes created that gives the Chinese Communist Party and its proxies a foothold in these countries.

In my testimony, I spoke specifically about an example from the Czech Republic where a company called CEFC China Energy had done a lot to cultivate Czech President Zeman and create potentially some connectivity similar to what we see Russia doing.

So I think it is really important to understand the very holistic strategy and the way that it is in fact targeting our European allies.

Last point—I was in Brussels last week. I got off the plane, was heading through Customs and the very first thing I saw was an electronic billboard that was advertising for Huawei—vote Huawei 5G—it is our values. It is our values.

So I am particularly concerned not just about the broader strategy, not just about the dependency created, but the dependencies that are going to be created through investment in the technology sector.

These are going to be transformative kinds of investments that will affect not only our economies but our strategic interests in the decades to come.

Thank you.

Mr. PENCE. Thank you, Mr. Chairman. I yield.

Mr. KEATING. Thank you.

Representative Dina Titus from Nevada.

Ms. TITUS. Thank you, Mr. Chairman. Thank you for holding this hearing.

You know, the Mueller report concluded that the Russian government had interfered in our election—I think the quote was "in a sweeping and systematic fashion"—and you all, in your very expert ways, have laid out a number of examples of Russian interference in Europe from Greece to Lithuania.

Yet, we have a president who seems to just pooh-pooh all this. He sides with Putin over our own intelligence. He says he believes Putin when he did not say—when he tells him he did not do it or he does not bother to ask about the 2020 elections.

He just minimizes at every turn this Russian engagement. He seems to think that Russia could be a buddy of ours if we just find the right interest.

Now, that is totally contrary to a lot of scholars who have said that—and I think you just mentioned it earlier—Putin needs the U.S. as an enemy in order to maintain his position at home.

So my first question would be to you, where do you fall? Do you think that that is an accurate description or do you think we can just kind of work out a few of the details and then be friends with Russia down the road?

And then the second part of the question is you have laid out for us things we need to do—stronger sanctions, campaign finance reform, cracking down on LLCs, money laundering.

But I would ask you is not all of that undermined by the president's position, by his attack on the free press, turning them into the enemy when they could be a good anecdote to this sort of activity with the real fake news coming out of Russia?

The lack of the State Department doing anything kind of that parallel's the EU's action plan against disinformation and also just his general antipathy toward multilateral arrangements so we are not working with our allies in Europe?

So, one, how do you feel about Russia being a buddy, and second, do you think all these suggestions that you make are being undermined by what's coming out of the White House?

Doctor, you want to start?

Mr. CARPENTER. Happy to start, Congresswoman. I think there is this myth that we have a range of potentially cooperative interests with Russia when in fact Russia's primary interest is to undermine U.S. democracy.

They see their role, for example in Syria, as undermining our ability to create regime change or political transition, if you will, in Syria. The scope for cooperation is minimal to nil, there and across the board, whether it is CT, whether it is in any other sphere, other than potentially in arms control with the extension of the New START Treaty. That is about the only potential overlapping interest that I can see. Everywhere else Russia's primary goal is to undermine us.

Now, in terms of your second question, I completely agree. The narrative that Russia is pushing here is precisely a narrative that you cannot trust the media: the media are biased.

You know, so when the president says things, calls the media the enemy of the people, he is playing into Putin's narrative.

That is exactly what Russia wants, and that is why Russia also cultivates various populist politicians across Europe, because they advance that very same narrative of undermining democratic institutions and trust in them—law enforcement, tax authorities, all of this.

It is not just the Putin play book. It is the Orban play-book. And then when we see it happening here in this country, absolutely,

this undermines our ability to build resilience against these subversive tactics.

Ms. TITUS. Thank you.

Ms. ROSENBERGER. I would just agree that I think we need to be very clear-eyed on what Putin's strategy is and how that does not in fact line up with an attempt to be friendly.

But on the—on your question about whether or not some of these suggestions can exist without a broader strategy, I would say they can certainly be a little bit of a patchwork and I think that is what we see cropping up right now by a lot of dedicated folks in government who are trying to do the right thing.

But this is a whole of society problem. Many of the challenges that we are talking about today by their asymmetric and evolving nature fall in gaps and seams of our government.

It requires an integrated, coordinated, and holistic approach that requires leadership from the top, strategic messaging, and I think we need to take some very clear steps in order to make that possible.

Ms. CONLEY. Congresswoman, Mr. Putin needs the conflict with the West. That is his entire point of survival. There can be no Russia without Mr. Putin and he will protect it from the West.

Unfortunately, what Mr. Putin needs to protect Russia from is from China and China's growing encirclement of Russia.

I think exactly to Laura's point, every one of the departments and agencies are doing their best to do their best. We just do not have a focused White House bipartisan priority on this very important task.

And the last thing I will say is even when President Trump does meet with Mr. Putin and he has expressions of strong support, what happens is that there is a real reaction against that. There is an antibody. Congress passes more powerful sanctions. There is an outcry.

So even when the president takes positions that seem very much at odds with where our policy is, where our national interests are, there is a reaction against what that is and I think that demonstrates we are very uncomfortable.

When President Putin is very pleased with something the U.S. does we know instinctively that that works against the United States.

Ms. TITUS. Thank you, Mr. Chairman.

Mr. KEATING. Thank you.

Representative Ron Wright of Texas.

Mr. WRIGHT. Thank you, Mr. Chairman.

Ms. Conley, I want to go back to energy policy for a moment and, Mr. Doran, I would like for you to also comment, given your earlier comment about Nord Stream 2. It has to do with Russia weaponizing its energy resources against European countries.

Earlier this year, we passed Mr. Kissinger's European Energy Security and Diversification Act—let's see if I can get that word out—which provides support to European countries to diversity its energy resources.

Tomorrow we are going to consider my bill, the Energy Diplomacy Act, which will authorize an assistant secretary State for en-

ergy resources within the State Department, dedicated to advancing our energy security interests and those of our allies.

Apart from those things, what would you recommend that we do—Congress do—to help countries end their dependence on Russian oil and gas, and particularly in Europe?

Mr. DORAN. Thank you, Congressman.

I think your question is perfectly phrased and well timed. I would say this. Because we have heard a lot about perhaps the vacuum that has been created in the past in Europe and a lot of questions about what the United States does about it on energy or diplomacy, and I think the merger of those two things is important.

First and foremost I think it is essential that we offer free market alternatives to Russia's monopolistic forms of competition in the energy space in Europe.

As I said earlier, that means sanctions on Nord Stream 2 while simultaneously providing market-based alternatives through U.S. LNG and other sources.

I think the United States can and should take a greater leadership role in rallying our European allies in Europe to create a—what I would call a shield wall against Nord Stream 2. I would stress this for the committee. Many European allies look to Germany as a weather vane for what is and is not acceptable when it comes to their relations with Russia.

We have heard a lot of testimony this morning about how this ally or that has been too cozy with the Russians, and I would stress Europeans look at what Germany is doing as a signal for what is acceptable in their relations with Russia. The United States can and should create—use its bully pulpit and its leadership to say there is an alternative.

It is free market based. The Russians are not your friends. We need to slam the door on their energy competition—monopolistic competition in Europe.

Ms. CONLEY. Congressman, we have documented both in the Kremlin Play Book 1 and the Kremlin Play Book 2 that energy is a key source of Russian malign influence. It is sort of the joke of why did the robber rob the bank—well, that is where the money is. That is where Russia's source of power and its money is.

So the Bulgarian case which Congressman Pence had mentioned about this threshold that we saw of Russia's economic footprint in a given country, Bulgaria has been unable and unwilling to diversify its own energy, which is crazy.

It pays some of the highest costs of Russian oil and gas and it is one of the closest neighbors to Russia. It cannot diversify. There are so many influential tools of, you know, fictitious NGO's that come up where it has influences with the g government. It refuses to diversify.

Now, yes, the United States can certainly provide alternatives. U.S. LNG is a perfect example. Almost overnight when Lithuania imported U.S. LNG it dropped Gazprom's price by 30. So we need competition, absolutely.

But we need transparency into how Russia is using its energy leverage in Bulgaria, in Hungary. We need to be as concerned about Nord Stream 2 as we are about Turk Stream, which is going to do the exact same thing that South Stream, which, thankfully, ended

due to a lot of American leadership and European leadership, but it is coming back again.

So we have to work with our European partners. The challenge that we have is we need to keep our allies in a strong position. Whatever policy response cannot weaken our allies. It has to strengthen them.

So I would recommend doing a much more of a deeper dive financially and to the banks that are supporting Nord Stream 2, the energy companies.

If they were to completely be transparent about the nature of their transactions, we may have a different view and maybe a different tool than sanctioning them, which is, I understand, certainly under contemplation. But we have different tools and transparency is one of the biggest.

Mr. WRIGHT. Thank you very much. I am out of time.

Mr. KEATING. Representative David Cicilline from Rhode Island.

Mr. CICILLINE. Thank you, Mr. Chairman. Thank you to our witnesses for your testimony.

Dr. Carpenter, I want to focus for a moment on the dark money that is supporting political candidates. As you know, the Russians have provided funds through illicit means directly to pro-Russian political parties and individuals.

As an example, an obscure Russian bank provided the French political party National Rally with a multimillion dollar loan before the last French Presidential election. That is just one example.

I wonder if you could just tell us what your sense is of the magnitude of this problem of how pervasive this kind of dark money is and whether the existing European governments have the tools at their disposal because of existing laws to prevent that.

Can the U.S. be doing more to support that work? Should we be working more closely with them and how should we be doing that?

Because it seems to me if those resources remain available, that becomes a very substantial source of Russian malign activity when they have the ability to prop up and even help be successful certain candidates.

Mr. CARPENTER. Thank you, Congressman, for the question.

I think this is crucial. This gets at the heart of Russia's influence operations how it finances them via dark money, and we really do not know how much of this money flows into Europe or into our own system.

In 2015, the Treasury Department estimated that some $300 billion is laundered annually into the United States. But that is from a variety of different sources.

Now, other estimates have said that Russian private holdings abroad are between $800 billion and about $1.3 trillion. So there is a vast amount of resources that are held by oligarchs, tycoons, businessmen, Russian companies that is available for use in dark money operations and influence operations.

We do not know—the bottom line is we do not know the extent of it. But what we have to do is empower the Europeans to go after anti-money laundering regulations and with a regulator that exists across the EU and we ourselves desperately need to address the issue of shell companies and beneficial ownership, exposing that

ownership so that we have more transparency about what the Russians are doing in our own country.

It is so easy to establish layer upon layer of shell companies through Delaware, Nevada, North Dakota, other States, and then to siphon money into our political process. It is just simply all too easy and we do not know the extent of the dark money that flows through that process.

Mr. CICILLINE. And in addition to that, I know there has been some effort most recently by the French but I know other European countries have engaged in some effort to reduce the dissemination of fake news or fake information on social media and really hold service providers accountable.

And I do not know whether any of those—there is enough information to determine whether those have been successful. Are there lessons we can learn about their effort—and this is for any of the witnesses—to respond to this other substantial source of power in these elections that has been misused and wide dissemination of inaccurate and false information?

Ms. ROSENBERGER. Thank you.

Yes, I think the EU is actually really leading in this space and is leading in a way that, frankly, the United States has not been.

I think there are a number of steps that the EU and its various institutions have taken that are worth considering. One is it has created a rapid alert system amongst its member States, particularly in advance of the parliament elections that is sharing real-time information among the different States about what they are seeing in their information ecosystem so that they can alert one another to possible trends.

Two, they have taken on this Code of Practice that is a sort of self-regulatory agreement with the platforms. Some of the platforms have signed up. Not all of them have. But it is an interesting model that is then actually giving some accountability and transparency to what the platforms are doing.

They are required to provide monthly reports to various parts of the EU in advance of the parliament elections and hopefully continuing beyond that.

The one thing I would caution about what we are seeing in terms of a number of the proposals coming out of Europe and other parts of the world dealing with information operations and information manipulation is a focus on content, and I have argued that in fact what we see engaging in certainly the Russian style information operations is not properly seen as a content problem.

It is a problem of bad actors—nefarious actors and manipulative behavior. Most of the content that we have actually seen pushed by the Internet Research Agency and similar outfits is not actually information that is demonstrably true or not.

It is engaged in manipulation, polarization, and other kinds of operation under false pretenses.

So I would caution about going down that road. If I could add just one last point as well on your prior question. I would just like to note you asked about laws on foreign financing, and actually we did a survey of the legal frameworks in EU member states with regard to foreign financing and in fact only half of EU member states

have a complete ban on foreign financing of political parties or candidates.

So while the dark money problem is a huge issue, in a number of States there are either major loopholes or no prohibition whatsoever. So we actually have a problem as well of just inviting the Russians in through the front door.

Mr. CICILLINE. Thank you so much. My time has expired.

Thank you, Mr. Chairman. I yield back.

Mr. KEATING. Representative Michael Guest.

Mr. GUEST. Thank you, Mr. Chairman.

I want to talk about one specific portion of the Russian foreign policy, which is their Arctic strategy. We have seen increased Russian military footprint in the Arctic. Media outlets have reported that in recent years Russia has unveiled a new Arctic command for new Arctic brigade combat teams, 14 new operational airfields, 16 deep water ports, and 40 icebreakers with an additional 11 in development.

So we see increased military bases, increased military ports, a dominant ice breaker fleet—when compared to America, 40 to 2. Other media reports have said that Russia has deployed the S–400 surface-to-air missile as well as the Bastion anti-shipments.

And so my question is in light of this increased military buildup—and this is going to be to the entire panel so I will start with you, Dr. Carpenter—one, I would ask you to speak to the importance of the Arctic strategy to Russia's overall global policy, and then two, what should be done to combat Russia's growing military presence in the Arctic?

Mr. CARPENTER. Thank you for the question, Congressman.

This is an area of the world that Russia is rapidly militarizing. With each year, there are more, as you say, airfields, more military capabilities put into the Arctic in order for Russia to be able to dominate the Northern Sea Route and the transit of commerce through that region as well as to ensure that the Russians have a leg up in terms of developing hydrocarbon and other mineral resources beneath the Arctic sea bed.

So this is an area where we have, frankly, lagged. You mentioned the ice breaker fleet comparison. We have—two is actually a generous guess. It is more like one and a half, depending on when that other breaker is able to operate, and the Russians are just—you know, they are miles ahead of us.

So we need—you know, we have had this mantra of we do not want to militarize the Arctic. But the reality is that Russia is militarizing and so we have to respond, not necessarily by putting in place offensive capabilities but we need to ensure freedom of navigation.

We have been actually rather reticent to push that in the Pentagon and I feel that we should be doing a lot more to assert our rights in those northern sea passages because Russia has a long-term strategy and they are banking on it. And the Chinese are looking very enviously also at what Russia is doing, and we are the—we are caught behind.

Ms. ROSENBERGER. I would just underscore the strategic importance of the Arctic and, as Dr. Carpenter ended up there at the end, China has also been well ahead of us in terms of the way that

it is using and exploiting the various resources and the strategic passageways there.

So it is of incredible importance. But I am going to let Ms. Conley jump in on this because she is the true expert here on this issue.

Ms. CONLEY. Well, Congressman, thank you for the question. Again, sort of rethinking how important the Arctic is to Stalin, the Red Arctic—this was about, you know, man defeating nature. It is very much about heroism in the Russian mindset.

It is the Russian Orthodox Church; we have had orthodox priests sprinkling holy water on the North Pole. I mean, there is lots of myth-making about it.

But they understand it is about—it is strategy, strategy, and strategic location, getting to the North Atlantic and the North Pacific very, very quickly.

We have done some analysis of commercial satellite imagery of Wrangel Island, which is 300 nautical miles from Alaska, which we are seeing a very sophisticated Sopka–2 radar.

We are also noticing with increased interest a whole new set of weaponry that the Russians will test in an exercise this September in Tsentr. We need to pay attention to this. I think your colleagues in the Senate Armed Services Committee certainly understand it.

But no one has the resources. No one wants to put the resources. We do not need 40 Ice Breakers. We do not have the Arctic coastline.

But we need sufficient presence air, land, and maritime to be able to ensure we have access to the Arctic that is freedom of navigation, that is over the air, and to make sure that Mr. Putin, as he just said in April in St. Petersburg at his annual Territory of Dialogues, is suggesting that we do not want the Arctic to turn into another Crimea. Of course we do not.

But we need to make sure that NATO and the United States are positioned to make sure that Mr. Putin does not even contemplate thinking about the Arctic as a place to disrupt or destabilize. We both want mutual peace, security, and collaboration.

But you are asking the right questions, and you also have to look at Chinese and Russian interaction in the Arctic, which is China right now is constructing two ports in the Russian Arctic, the Port of Sabetta and the Arkhangelsk Port.

Their energy interests are intertwined and we are going to see a lot of Chinese LNG carriers going through the Bering Strait. We are not prepared for that future either.

Mr. DORAN. Congressman, can I just jump in here really fast with one final point, which I think is a crucial for this committee to remember?

Right now, we are in a State of competition with China and Russia. We have heard a lot about that today. But if in a sporting competition you are losing 40 to 2, there is no way to spin it. You are losing.

When we look at our competition in the high north, I would encourage the committee to remember the essential element of our allies.

Countries like Norway are power generators for the United States. They are power projectors for the United States. We can do

a lot more to rely upon our essential allies such as Norway and others to listen and be more active in the high north. Something to remember.

Mr. GUEST. Thank you, Mr. Chairman. I yield back.

Mr. KEATING. Thank you.

Representative Tim Burchett from Tennessee.

Mr. BURCHETT. Thank you, Mr. Chairman.

This is for, I guess, Mr. Doran or Ms. Rosenberger, if that is OK, and if anybody else wants to jump in just jump in.

In your all's views, what is the most vulnerable European States to Russian disinformation campaigns and do you project to be the—who do you project to be the next electoral target?

And if you all hesitate it takes up all my time and it makes me——

[Laughter.]

Mr. BURCHETT [continuing]. It makes me look very intelligent. So just hesitate a little bit.

Ms. ROSENBERGER. Well, no, no, no, no. So let me—let me start with the end of it which you asked, which is most likely to be the next electoral target.

I would argue it is all of them and I would argue that we cannot see election interference as a discrete thing in and of itself.

The strategies that all of us talked about today, these tactics, these are ongoing operations and elections are one moment in time.

One of my colleagues has said in fact that election interference or elections are not necessarily the beginning point or the end point of interference operations. They are the flash point.

It is a moment of opportunity for Putin to gain particular strategic gains and where you have a broader target surface. But most of those operations are going on for quite some time and continue for quite some time afterwards. So that is point one.

In terms of who is most vulnerable, it is an incredibly difficult question, hence the hesitation. I would simply say that I think what we have seen is countries that are most vulnerable are those where polarization is high, where independent media has been—where the space has been shrunk and where you have—where you do not have credible voices who are giving people a sense of a shared fact base.

And so I think that those are three vulnerabilities that I would look at when trying to understand who—which countries may in fact be most vulnerable.

Mr. DORAN. Thank you, Congressman.

Rather than saying one specific country, because I think there is more than one, I will give you a region to look at—the Western Balkans, and that applies not just to Russian disinformation but also China.

There was questions earlier about the purchasing by Chinese companies in Europe and what industries should we be afraid of. When it comes to both Russia and China in the Western Balkans and elsewhere, I would encourage the committee to look at the media industry.

It is easy to purchase radio stations, television stations, and other segments of the media and change their editorial policies to

say Chinese policy in Europe is good. Russian policy is good. So I would encourage that focus. Western Balkans—that is a key.

Mr. BURCHETT. Would you encourage us to get into the media business?

Mr. DORAN. I do not think it makes much sense for Congress to start its own television station. I think your C-SPAN ratings are kind of low these days.

Mr. BURCHETT. I know. We would have to do reruns of "Finding Bigfoot." I have always found that does better than the national news.

Yes, sir? I am sorry.

Mr. CARPENTER. If I could just piggyback on that last point, though. What I think we can do much more of is supporting investigative journalists across the region. They are vulnerable in the Western Balkans, as Peter has rightfully pointed out, where there is a soft target for Russian disinformation.

But they are vulnerable across the board. There was a Slovak journalist who was murdered last year. There was a Ukrainian journalist, Kateryna Handziuk, who was doused with a fatal dose of acid. She died later.

Across the region they are under fire and they need both a network of support but also the resources to be able to withstand these attacks from often entrenched corrupt actors in these societies and usually backed by Russia and China.

Ms. CONLEY. I would just offer I think one country that is probably not in our focus for vulnerability is actually Germany, which will be having three launder elections in the fall in the east. It is a political transition that is quite vulnerable and there are a lot of Russian opportunities for influence.

And just a point on investigative journalism, there is some fantastic journalism that is going on in these countries; we have to support it. It is not us making the news. But they are—they are being murdered because they are exposing corruption, which is the power base of Russian influence.

So I cannot begin to tell you we need an offensive strategy on transparency, investigative journalism, civil society—they are demanding something different. We need to help them and be the inspiration we once were.

Mr. BURCHETT. I have one quick question and I know I am running out of time. But how would you all assess Russia's meddling so far in this lead up to this week's European parliament elections and what would you all be considered—would you all consider a win for Russia in these elections?

I know you said it is one point in time. I do not want to go back on those eloquent words you said, ma'am. But if one of you all could fill me in on that.

Mr. CARPENTER. I could start. You know, I think that there is a degree of Russian interference across the board to support anti-establishment nationalist populist parties.

So we recently had, amazingly, an anti-immigrant party come to power as part of a ruling coalition in Estonia where last year there were 5,200 immigrants, most of whom were former Estonian citizens that were coming back.

They do not have a migration problem. But these sorts of parties they play to Russia's interests. And so Russia is supporting nationalist populist parties across the continent.

Ms. ROSENBERGER. I will just pick up on that. One of the challenges, I think, in determining the degree to which we are seeing Russian interference in Europe relates to a point that Ms. Conley mentioned earlier in her testimony previewing what to fear or worry about in terms of the U.S. 2020 elections and that is that these operations as they have been continuing over the years have become more deeply embedded in the networks that are domestic networks.

So whether that is on the financial side, whether that is on the information side, whether that is on the political or sort of social group side, these networks have become more entrenched.

And so witting or unwitting, you have domestic actors that are engaging in activity that is very difficult to distinguish from the foreign activity.

That is going to cause particular challenges over time as well on the information front in dealing with free speech because when it is a domestic actor that is simply carrying the message it has much more significant implications than when we are just dealing with a foreign actor.

So it is very difficult. There has been some great research that has looked at the degree to which there is this confluence of the Russian interference operations and the far right information environment in Europe that just came out a couple weeks ago in particular looking at several countries and I think that is really, as we are thinking about how these problems become compounding over time, why we need so concerned about acting now.

Mr. BURCHETT. Thank you, Mr. Chairman. I have gone way over. I apologize.

Mr. KEATING. That is fine. Thank you. Good questions.

Representative David Trone from Maryland.

Mr. TRONE. Thank you, Mr. Chairman.

The followup on Mr. Cicilline's question—2017 Germany passed novel legislation to put massive fines on social media companies that do not remove obvious criminal content within 24 hours.

2018, based in large part on lessons learned in recent elections, France enacted a law that allows judges to block distribution of fake news, you know, during an election.

So what role can and should social media companies themselves play in deterring disinformation in these propaganda campaigns?

I will just start with Mr. Michael Carpenter.

Mr. CARPENTER. Well, I think Laura alluded to this point earlier that the platforms have an obligation to take fake content, fake accounts and bots, that engage in malicious behavior off of their—off of their platforms.

It is not so much—if we are into policing content, you know, as an American with First Amendment concerns, that makes me squeamish.

But when we look at fake activity, activity that is generated by robots, that is where the platforms need to be devoting the resources to weed that information out—weed those fake accounts off of their platforms—because that is sort of what often generates the

news cycle by amplifying some of the fake content that otherwise would just sort of fall into a void.

Ms. ROSENBERGER. One of the most important things that we could do, and Congress can play a role here, is to create a sustained information-sharing mechanism between the government, law enforcement and intelligence community, and the platform companies.

Basically what we have right now, if you want to go at this in a systemic way, the way that Dr. Carpenter just talked about and that I alluded to earlier—going after the actors and their behavior—you need to have insights on what the bad guys are doing over in St. Petersburg or wherever they are and that is law enforcement and the intelligence community that has particular insights into the nodes, networks, and pathways.

But it is the platforms that have the information on what is actually happening—what the actual activity is and how it is manifesting. You have to bring those two puzzle pieces together.

Right now that is happening on an ad hoc basis between certain parts of the U.S. Government and certain platforms. It needs to happen on a sustained and formalized basis in ways that protect privacy and speech.

We have examples of this from the cybersecurity domain, the counterterrorism domain, and the financial integrity domain. It is beyond time for us to take these steps. I think that it is absolutely urgent and Congress can actually take that step.

Ms. CONLEY. Congressman, I would just say again that we need a fusion center. We are not structured to combat this. We need private sector engagement and we need the combination. It is Treasury. It is Justice. It is Intelligence.

We have to restructure ourselves. The other part of the equation is that we have to do a much better job of public awareness. In my written testimony I sort of suggested, you know, during the Second World War we had a big public campaign, "Loose lips sink ships," which is sort of ridiculous.

But if it is, you know—if it is not factually correct you have to delete—we have to warn the American people. They have to know that this is about them and they have to be much more proactive.

So it is getting our structural house in order, but it is also helping the American people understand that this battle space is taking place on their computers.

Mr. DORAN. Congressman, one idea to take from your question here is that some of our CEPA analysis has demonstrated if we spend too much time obsessing about what the bots are doing it is going to be a losing strategy.

Like I said, it costs the Russians pennies on the dollar to compete with us in this sector. What I do think we could do is to increase the networks between, as we have heard, U.S. Government and outside of government, between experts.

Information sharing is key but also the public—if you think of this disinformation as a virus the public needs to be better equipped to protect themselves and each other from communicating these kinds of information viruses.

Mr. TRONE. Thank you.

Have you seen any ideas the EU or NATO have done to help voters distinguish, you know, what's disinformation from fact and opinion that has worked?

Mr. CARPENTER. I think the model for us to follow is the model from Finland and the Baltic States, which have been used to receiving Russian disinformation for decades and decades and they—you know, so much so that Russia had a Finnish language service on Sputnik that they canceled in 2014 because it simply was not getting through.

So that is the ultimate sign of success is when they pull their programs because they are not getting through. But it comes from—it comes from sort of being inoculated over the course of many, many years to the fact that if there is questionable content in the media that hey, that may not be real—that it may be a propaganda item that has been put into the public narrative.

And so it takes a sort of sustained public awareness-raising campaign to get that level of inoculation within the society.

Mr. TRONE. Thank you.

Mr. KEATING. Thank you.

It is clear from this morning's testimony that it is not enough to just take down a site. We are playing whack-a-mole in that instance and we have to really treat it as a much deeper fusion effort that we have in so many other areas.

Now I would like to Representative and former Ambassador to Luxembourg, Representative Wagner.

Mrs. WAGNER. Thank you, Mr. Chairman, for hosting this hearing and thank you to our witnesses for their time.

In Bosnia-Herzegovina, Russia has cultivated relationships with the Bosnian Serb community including Milorad Dodik, a Bosnian Serb politician currently chairing Bosnia's rotating presidency.

Mr. Dodik has embraced and authoritarian Serb supremacist ideology, and just last month claimed the 1995 Bosnian genocide at Srebenica was a fabricated myth.

Although Dodik and other Russian allies in the Bosnian Serb community oppose NATO membership, NATO foreign ministers agreed in December to begin the advice and assistance program for Bosnia-Herzegovina.

The Bosnian, Croat, and Bosniak presidents support NATO membership.

Dr. Carpenter, how is Russia exploiting ethnic divisions to stall Bosnia's ascension to NATO and what can the United States do to combat these very dangerous tactics?

Mr. CARPENTER. Well, Russia has always seen Bosnia and Herzegovina as a soft target for its influence operations and certainly President Dodik has travelled extensively to Moscow to confer and to consult with President Putin about the strategic direction of the country.

He essentially presents a veto over Bosnia's ability to move forward with its Membership Action Plan and actually join the NATO alliance.

And so far as he is in power or people like him in Republika Srpska, it is hard to envisage that the country will actually be able to 1 day join either NATO,or, by the way, the EU because although they say that the EU is still a long-term strategic priority, I am

not so sure that when it actually comes to it that people like Dodik will encourage the country to move forward.

So we have to—you know, we have to try to work with those people inside Bosnia that want a better future. But for right now, you know, Dodik is fully supported by Putin.

The latest example was the Night Wolves motorcycle gang which is a Russian sort of Trojan Horse. It is an intelligence front. Was in Banja Luca with Dodik supporting him and offering that sort of information support.

So this is a long-term effort. But, unfortunately, it is the goal that Putin sees, by the way, for Ukraine and for Georgia is to have sort of Republika—mini-Republika Srpskas in these other countries, too, because they are a veto on the Euro-Atlantic integration.

Mrs. WAGNER. To that point, as some of our witnesses have pointed out, Russian policies in the Balkans are largely opportunistic and not strategic.

In light of this, it is important not to overestimate Russia's ability to control events in foreign countries. But in aggravating ethnic tensions in the Balkans, Russia is playing with fire.

Ms. Conley, how likely is it that Russia will inadvertently ignite a conflict in the Balkans that it cannot control?

Ms. CONLEY. Thank you, Congresswoman.

Many times Russia creates problems that only it can, uniquely, solve and I think this is very true in the Western Balkans. Former Supreme Allied Commander in Europe, General Scaparrotti, has highlighted year after year his concern that the Western Balkans is particularly vulnerable not only to Russian malign influence but to instability.

Many Americans do not know we have 800-plus forces in Kosovo today as part of a NATO mission in K–4 and we cannot take stability in the Western Balkans for granted.

The challenge is, I think, for both the EU and the U.S. we have allowed our presence to atrophy and others—Russia, China, as well as Turkey, Qatar—have reintegrated and reinfluenced the region.

We do not have—the Western Balkans is not a top priority in our foreign policy toolkit. In Bosnia, in particular, which you highlight, the Dayton Accords now, which was designed to stop violence, which it did, it has now imprisoned Bosnia—that it cannot move forward. It cannot reform, which in large is Dodik's ability to prevent Bosnia from joining the Euro-Atlantic community.

So I believe this will be fuelled by Russia to distract, to disrupt, to potentially fuel a migration push toward Europe—whatever it can do to distract.

But this is unfinished business. This is weakness that Russia is simply exploiting and because the U.S. and EU do not have clarity and strength of policy, it is being allowed to happen.

So this is an area of huge concern. The problem is Mr. Dodik is getting so much play because there is not a lot of forces to push against him.

Mrs. WAGNER. I have got some questions about Latvia and Estonia, which I will submit especially to you, Mr. Doran, but my time has lapsed, and I yield back.

Mr. KEATING. Well, thank you, Representative, and I think that this committee will be focusing on those areas that you brought

up—very important areas, going forward, that need greater attention and we will be delving into those issues as this committee goes forward in this Congress.

I would like to call upon the vice chairman of the committee, Representative Abigail Spanberger.

Ms. SPANBERGER. Thank you, Mr. Chairman, and thank you to the witnesses for being here today.

My question is to followup on the discussion related to civic engagement that I know has been the thread of a lot of the discussion in question so far.

I am directing these specifically to Ms. Conley and Ms. Rosenberger but I welcome the other two witnesses to add anything to this discussion.

The European Union's East StratCom Task Force established in 2015 seeks to raise awareness of Russian disinformation and to educate the public about disinformation and improve media literacy overall, particularly when it comes to the internet and social media.

The Swedish government, for example, instituted a nationwide digital competence curriculum for elementary school-age children teaching them how to spot fake news and discern the difference between reliable and unreliable sources.

As a former intelligence officer with CIA but also as a mother of three young children, I do believe our national security strength begins with the American people, especially with our children, and that means ensuring they have the necessary education and tools to make objective evidence-based decisions.

So do you all believe the European Union's approach in focusing on education and public awareness training and especially with a pivot toward programs focused on children can be or is an effective strategy to counter disinformation and are there any other countries pursuing this type of program that you have been aware of that you think are successful that we should try and learn from?

Ms. ROSENBERGER. Well, thank you. I think those are really important questions.

I would note just a couple of points. The first is that I think this idea of building resiliency here at home is absolutely critical to dealing with so many of these challenges.

Whether that is resiliency of our financial system on some of the tactics we were speaking about earlier or resilience on the information side, these are vulnerabilities in our own societies that are being exploited and we need to recognize that.

Public awareness in education is absolutely a big part of that. I would sort of parcel them out into two different pieces. Public awareness about the threat requires real consistent strategic messaging.

Ms. Conley mentioned earlier, you know, some of the programs we have seen on the counterterrorism front. I think it is very important that we think about simple messages that we can replicate.

Sweden, I think, may have been mentioned earlier as an example to look at for some of the tactics that they have used. You mentioned the awareness campaigns. But they have also done a lot of really good work up and down the board at raising public awareness.

The one thing I would say that the East StratCom team has focused a good bit of their energy on is on debunking specific stories, false narratives.

I would suggest that the research shows that that is of limited utility and that in fact it sometimes it risks actually amplifying the content you are seeking to debunk.

I believe there is a threshold level at which it is imperative for governments to step in and sort of demythologize some of those narratives. But I would argue that that is not path to go down.

The last point I would make, though, is while I think that focusing on our children is extremely important, most of the research shows that in fact it is senior citizens—people age 60 to 65 and older, depending on which study you look at—that have been the most vulnerable to mis-and disinformation.

And so I think we cannot discount looking at that part of the population, which has not grown up with so much technology in their lives that may not be as accustomed to using it, and that we need to make sure that we do not focus so much on just the younger generation that we lose sight of the other parts of the population that remain vulnerable.

Ms. CONLEY. Thank you again for the question, I think the EU StratCom is a good thought. It is so under-resourced, sort of buried. It is not proactive.

NATO's Strategic Communication Center, I would argue, is certainly giving us leading tools of what is happening. But you are right, the public education component is missing.

Sweden is the perfect model. I do not know of other EU countries that have done sort of a similar education at the grade school level. I think they see it as a part of what they—their defense concept, as you may well know, is total defense.

It is about civilian defense—that everyone is responsible for defending the Nation and it begins with them individually. That is preparing your home in case of disaste,r but that is also preparing your mind for being influenced inappropriately.

So we have to somehow message that patriotism and public awareness, that this is something that goes together. As I mention in my written statement and my oral statement, we are at war.

It is just a different kind of war and we have to convince people that they have to take personal responsibility, making sure that what they are reading and what they are hearing from families and friends—is that right?

Do I have the right information? How can you be a truth detective, if you will? That is part of our patriotic duty. But we have to put it, I think, in those terms.

Ms. SPANBERGER. Thank you very much.

I yield back.

Mr. KEATING. Thank you very much.

I believe that, given its history, Estonia as well has instituted from the first grade level even some of this education on young people as well.

So I just want to thank our witnesses here. We have touched upon the surface. Yet, I think we have done so in a way that actually had us arrive at solutions and paths forward that we can have.

So I want to thank all of you for making that part of your testimony as well. There is a path forward. There are things we can do domestically. There are things we can do, particularly, information sharing with our allies in Europe. There are lessons learned there that we can go forward to deal with what is a major threat.

And today, we had the opportunity to amplify something that is so often overlooked as a threat—the involvement of Russia in public corruption, political corruption, and financial corruption.

There is much to do going forward. But your testimony here I think created a great foundation for us to pursue.

So with that, I want to adjourn this hearing and thank all the members that took time out of an extremely busy day. You saw people coming in and coming out. But we had great participation.

I want to thank you and adjourn this hearing.

[Whereupon, at 11:53 a.m., the committee 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

May 21, 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, May 21, 2019

TIME: 10:00 am

SUBJECT: Undermining Democracy: Kremlin Tools of Malign Political Influence

WITNESS: Michael Carpenter, Ph.D.
Senior Director
Penn Biden Center for Diplomacy and Global Engagement
(Former Deputy Assistant Secretary of Defense with responsibility for Russia, Ukraine, Eurasia, the Balkans, and Conventional Arms Control)

Ms. Laura Rosenberger
Senior Fellow and Director of the Alliance for Securing Democracy
The German Marshall Fund of the United States
(Former Chief of Staff to Deputy Secretary of State Tony Blinken)

Ms. Heather Conley
Senior Vice President, Europe, Eurasia, and the Arctic
Director, Europe Program
Center for Strategic & International Studies
(*Former Deputy Assistant Secretary of State in the Bureau of European and Eurasian Affairs, U.S. Department of State*)

Mr. Peter Doran
President & CEO
Center for European Policy Analysis

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** *May 21, 2019* **Room** *2172*

Starting Time *10:04* **Ending Time** *11:53*

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:

Undermining Democracy: Kremlin Tools of Malign Political Influence

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.)*

Michael Carpenter's Testimony
Laura Rosenberger's Testimony
Heather Conley's Testimony
Peter Doran's Testimony
"Policy Blueprint for Coutering Authoritarian Interference in Democracies" Submitted by Mr. Keating
"Chaos as a Strategy: Putin's 'Promethean' Gamble" Submitted by Mr. Keating
QFRs from Mrs. Wagner

TIME SCHEDULED TO RECONVENE _____
or
TIME ADJOURNED *11:53*

Subcommittee Staff Associate

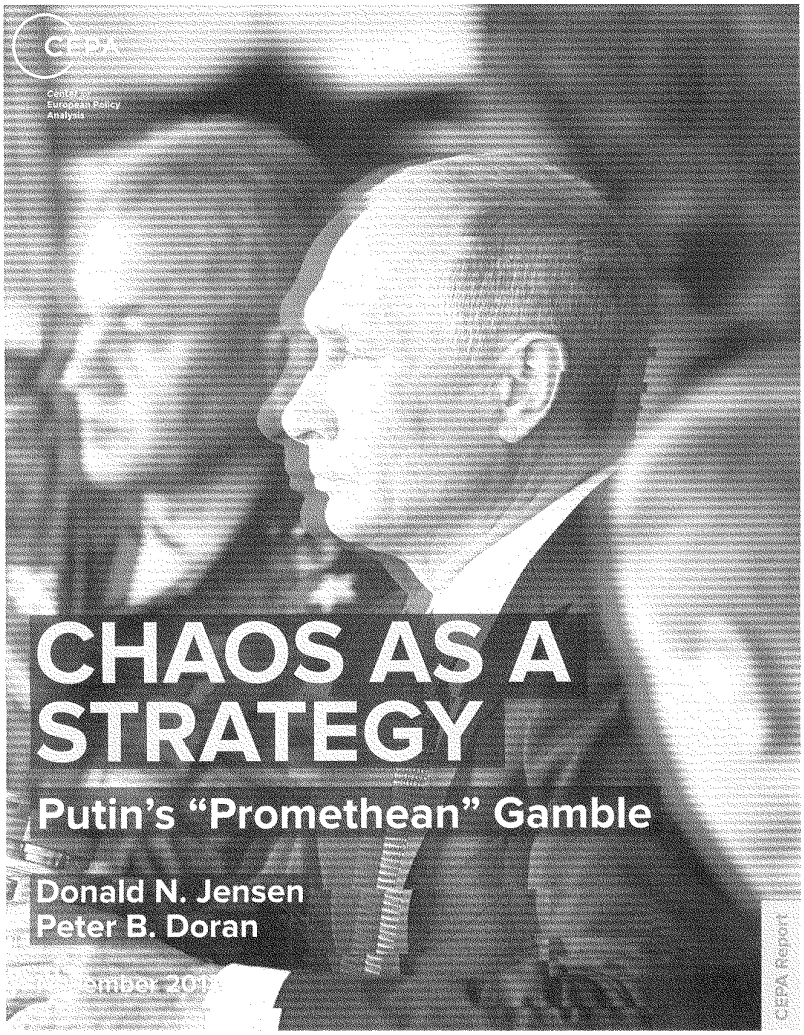
HOUSE COMMITTEE ON FOREIGN AFFAIRS

EUROPE, EURASIA, ENERGY, AND THE ENVIRONMENT SUBCOMMITTEE HEARING

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

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

ADDITIONAL MATERIALS SUBMITTED FOR THE RECORD



Center for European Policy Analysis

Center *for*
European Policy
Analysis

About CEPA

The Center for European Policy Analysis (CEPA) is a 501(c)(3), non-profit, non-partisan, public policy research institute. Our mission is to promote an economically vibrant, strategically secure, and politically free Europe with close and enduring ties to the United States. Our analytical team consists of the world's leading experts on Central-East Europe, Russia, and its neighbors. Through cutting-edge research, analysis, and programs we provide fresh insight on energy, security, and defense to government officials and agencies; we help transatlantic businesses navigate changing strategic landscapes; and we build networks of future Atlanticist leaders.

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
E-mail: info@cepa.org
www.cepa.org

Cover image: Edited version of Russian President Vladimir Putin with Russian Defense Minister Sergei Shoigu and Chief of the General Staff General Valery Gerasimov at Vostok 2018. Credit: kremlin.ru.

Center for European Policy Analysis

CHAOS AS A STRATEGY

Putin's "Promethean" Gamble

Donald N. Jensen
Peter B. Doran

November 2018

Table of Contents

SUMMARY OF FINDINGS AND RECOMMENDATIONS

Findings

- Kremlin leaders regard themselves as players in a great power competition with the United States and Europe.
- In order to compensate for Russia's long-term internal decline, the Kremlin increasingly is willing to take risks—sometimes recklessly—to balance its relative weakness against the West's relative strength.
- The Kremlin is attempting to offset its weakness by committing to a competitive strategy in which the side that copes best with disorder will win.
- In order to facilitate this strategy, Russia is seeding chaos in the West via asymmetrical means—i.e. disinformation, subversion, and "political warfare" operations.
- The strategy combines both old and new. It combines a 20th century concept for asymmetrical competition popularized by Poland's famed statesman Józef Piłsudski with Russian General Valery Gerasimov's concepts for conducting 21st century warfare.
- The result is a nonlinear means of competing against the West only in areas where Russia has advantages.
- A central element of this strategy is information warfare. This has become one of the main battlegrounds between Russia and the West and a prime vector where the Kremlin has implemented its "Promethean" strategy.
- Russia's authoritarian system enjoys strengths and weaknesses when executing its strategy. A chief strength is Russia's authoritarian system—granting the Kremlin a partial competitive advantage in managing the psychology and politics of disorder. A primary weakness is blowback—efforts at sowing instability abroad can have a ricochet effect.
- Given the success of Putin's "Promethean" gamble—and the Kremlin's sustained reliance on it—Russian leaders are likely undervaluing the inherent risks of their strategy. This can be exploited.

Recommendations

Dangers that we can see are easier to admire than those that we do not understand. In particular, U.S. leaders must consider how the concept of a bloodless "disordering of the far frontier" has figured in past Russian political-military strategy. Likewise, the Kremlin's chaos-seeding strategy shows us what its leaders fear: Western power. To date the West has not fully considered how its power can be brought to bear against the Kremlin's vulnerabilities. Every strategy has a weakness—even chaos.

In combatting the threat of Russia's chaos strategy, the United States and Western democracies have not fully considered how their full toolkits of national power can be brought to bear against Kremlin vulnerabilities. We can begin by removing the predictable and permissive conditions that enabled Russia's chaos strategy in the first place; and work toward a sustainable end state in which Russia returns to "normal" strategic behavior patterns. We can begin to accomplish this in four steps:

- First, realize that Russia sees the international system very differently than we do, even

though our interests on specific issues may coincide (for example, counter-terrorism).

- Second, approach our dealings with Moscow with the understanding that its use of terms like "international law" and state "sovereignty" are invoked primarily to advance Russia's interests. Kremlin leaders evoke these concepts for *ad hoc* advantage, not because it endorses a rules-based international system.

- Third, understand that Russia's use of information warfare has a purpose: reflexive control. (Such control is achieved by subtly convincing Russia's opponents that they are acting in their own interests, when in fact they are following Moscow's playbook.)

- Fourth, prioritize the sequencing of the "carrots and sticks" offered to the Kremlin. Sticks first. This means initially increasing the penalties imposed on Russia for continued revisionist behavior and the sowing of chaos. We can start with tougher sanctions, wider travel bans, greater restrictions on access to the global financial system, and financial snap exercises. Presently, some of these tools are used—but they are underutilized in most cases. This needs to change.

Particularly, in the domain of information warfare, the West must hit back harder. Although the EU's East StratCom, NATO's StratCom, and the newly established national StratComs in Europe can be effective tools, they still lack resources, coherence, and full coordination to stop Russia's malicious activities. We are in a technological contest with Russia. We should aim to win it. The Western response must be superior in impact and sophistication.

Russia relies on harnessing bursts of "sharp power" to succeed in its competition with the West. In response, Western leaders must set as a collective goal their intention to outmaneuver, outplay, and contain the damage of Russia's strategy with our overwhelming diplomatic, informational, military, and economic power. This response must be both public and private, and include the government, media outlets, the tech and private sectors, and civil society. Experience shows that an independent message is more credible and effective, and people are ultimately more receptive when these messages come from non-state actors. Investing more in these non-state domains holds a great deal of untapped potential in the

> "To date the West has *not fully considered how its power can be* **brought to bear against** the Kremlin's vulnerabilities. *Every strategy has a weakness—even chaos*."

Russian President Vladimir Putin. Photo Credit: kremlin.ru.

West. Finally, these measures must all go hand-in-hand with coordinated economic sanctions and be backed up with Western military power.

Unfortunately, we in the West—particularly in the United States—have been too predictable, too linear. We would do well to consider ourselves the underdog in this contest and push back in nonlinear ways. Perhaps the only thing that Kremlin leaders fear more than Western power is the rejection of their rule by Russia's own people. While our final goal should be to ensure that Moscow becomes a constructive member of the Euro-Atlantic security community, our responses for now should serve the shorter-term goal of forcing Russia to play more defense and less offense against the West. For this purpose, we should lessen our preoccupation with "provoking" the Kremlin. It is hardly a basis of sound policy to prioritize Putin's peace of mind. The Russian government will work with the West if that path suits its goals. Otherwise, it will not. We should do the same.

INTRODUCTION

Can Vladimir Putin's nonlinear strategy succeed against the West? For all of Russia's weaknesses as a Great Power, the Kremlin increasingly is willing to take risks—sometimes recklessly—to balance its disadvantages against the relative power of Western competitors like the United States. Risk taking is a dangerous business for any state—declining or otherwise. But what if the Kremlin believed that it could stack the odds of success in its favor? Could chaos be a strategy in itself? Inside some corridors of power in Moscow, the answer is: yes.

In recent years, Russian leaders and strategists have developed a set of methods aimed at spreading disorder beyond their borders for strategic effect. Their goal is to create an environment in which the side that copes best with chaos wins. The premise is Huntingtonian: that Russia can endure in a clash of civilizations by splintering its opponents' alliances with each other, dividing them internally, and undermining their political systems while consolidating its own population, resources, and cultural base. Such a strategy intentionally avoids competing in those areas where Russia is weak in hope that, should a direct confrontation occur, Russia will enjoy a more level playing field.

Strategies of chaos are not new. Sun Tzu, Clausewitz, and Haushofer all advocated the use of what would now be called information warfare to confuse and weaken a foe before attacking militarily. In Russian strategic history in particular, there is a tradition of stoking chaos on the far frontier to keep rivals divided and feuding internally rather than combining their forces to fight against Russia. What is new is that Russia has married an old idea (chaos) with 21st century technology and means. It is an exceptionally potent combination.

> "In recent years, **Russian leaders and strategists** *have developed* **a set of methods** *aimed at spreading disorder* beyond *their borders* **for strategic effect.**"

The catch is that risks can outweigh the rewards when courting turmoil. Indeed, a major disadvantage of chaos strategies is that they tend to backfire: efforts at sowing instability in a neighbor's lands can ricochet, generating

instability that eventually affects the initiator. Another problem with chaos strategies is that they involve a form of behavior—e.g. the purposeful use of disinformation—that becomes inherently more escalatory with time. Subversive moves that are initially surreptitious become more recognizable with use. And since these tools are ultimately part of war, it is hard to know when a state sponsored disinformation operation campaign is intended for every day, low-threshold "political warfare" or is a prelude to high-end kinetic operations. Worse, the preparations and countermoves that such actions prompt on the part of their targets can trigger tests of strength, the avoidance of which was the starting aim of the strategy.

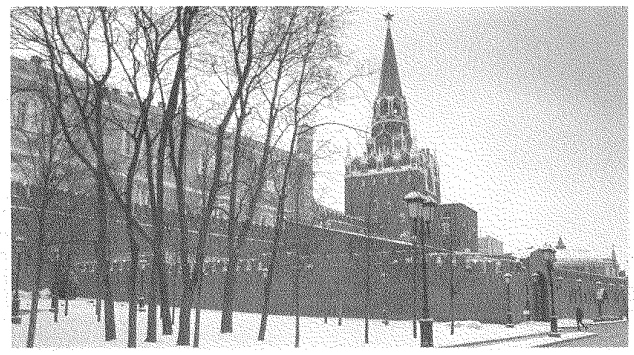
In this context, considerations of Western security competition with Russia have not focused enough on the strategic motivations behind Moscow's efforts to foster disorder, to obscure its objectives, and to make its actions seem unpredictable. Rather, a great deal of attention has been focused on what can easily be observed: what its social media "bots" are saying or what conspiracy theories its news outlets are purveying. The underlying strategic motivations of Russian leaders are undervalued or missed. In the West, the result is a mindset of *reaction*. Experts and leaders fail to anticipate next moves or evaluate Russia's endgame goals in this contest. While we remain subjected to continual surprise, Western states are fixated on the threats of chaos instead of looking for opportunities that the weaknesses in Russia's strategy could generate. This can—and should—change. The following report offers a means of understanding the purpose behind Russia's strategy—and for altering our response to it.

SECTION 1—CALM BETWEEN STORMS: RUSSIA AND THE INTERNATIONAL SYSTEM

Russian Thermidor

Under President Vladimir Putin, the Russian government has embarked upon on a multi-decade effort to rebrand its past and renegotiate its future. These efforts are linked, since they both arise from the same underlying problem: the foundational instruments of Russian power are no longer in the ascent. Confronted with a declining population, chronic social problems, weakening economic competitiveness, the corrosive effects of the "resource curse," and the persistence of institutionalized corruption, the Kremlin faces power impediments in all directions. The subsequent response by the Putin regime to this challenge has been the prioritization of one goal: survival.

In conceptual terms, Kremlin policies are "Thermidorian." They are much like the famous pause in the French Revolution that introduced more conservative policies to stabilize the state after a period of great political turmoil. Following the end of communism and the tumult of 1990s, Putin took power from the hands of earlier post-Soviet leaders. He subsequently buttressed state structures against disruptive impulses at home and used the country's wealth from natural resource exports to increase the standard of living and buy popular acquiescence to his authoritarian



The Kremlin. Photo Credit: pxhere.

rule. Simultaneously, Putin burnished his political credibility by invading Georgia and Ukraine.[1]

The results of this approach are now prevalent across Russia. The revival of Soviet military rituals and iconography, the re-writing of the past, the rehabilitation of dead dictators like Joseph Stalin, the rote repetition of narratives like "Russia the besieged fortress," or "Russia the victim of the West," and the copious consumption of consumer goods are all intended to excite and mobilize society against the bottom-up forces that could threaten the current state.[2] And while this effort may have provided Putin and his elites with political breathing space, it has not resolved their underlying dilemma: weakness.

Behind the facade of "Thermidorian" Russia, the Kremlin's assets of national power are dwindling—fast. The most obvious example is its demographic challenge. Russian men continue to die young and in alarmingly large numbers (when compared to their European neighbors). Russia's falling birthrate also shows few signs of slowing down. Today's Russian youth, born around the time when Putin first took office in 2000, now constitute the smallest generation in the country. The "missing millions" from Russia's falling birthrate are also beginning to have a negative impact on the structure of the economy. Because Russia's youth are so relatively few in number, they will decrease the total size of the Russian workforce by an expected 4.8 million people over the next six years. Overall, the total size of the Russian population is projected to shrink by 11 million between now and the midpoint of the century.

By 2050, only 133 million Russian citizens will be left to populate an eighth of the Earth's inhabited land area. The overwhelming number of these residents are likely to be concentrated into just three cities: Moscow, St. Petersburg, and Novosibirsk.[3] Outside of Russia's urban centers, its remaining territory will seem

comparatively empty when contrasted with the teeming polities of peer competitors like India (1.7 billion) and China (1.4 billion).[4] If demography is destiny, then Russia's shrinking population and ever-smaller workforce will mean that future jobs may be available in the country. However, there may not be enough Russians to fill them. This will be a tremendous handicap to Russian competitiveness in the 21st century.

Perhaps energy resources will be Russia's saving grace. Since at least the 1970s, the energy sector has been Russia's economic afterburner. It has supercharged the country through good years. In lean economic years, it has provided at least a minimal degree of support to the other elements of national power: diplomacy, information, and the military. The trouble is that Russia is now suffering from the deep decay of the resource curse ("Dutch disease").[5] This is the process by which Russia's energy wealth has steadily undermined its long-term economic competitiveness. Petrol rubles may have enriched elites and filled store shelves with imported luxuries, but these trappings of affluence have come at a cost: the sustained decline of Russia's manufacturing and non-energy export sectors (particularly in the regions).[6] Unfortunately for the Kremlin, the decline in manufacturing and economic prowess on account of Dutch disease is far advanced. Worse yet, it shows no signs of correction or remediation.

The problem with Dutch disease is structural. Under Putin, the Russian state has become the *de facto* property of a small group of decision-makers who maximize their power and profits through a reciprocal process of export revenue, state patronage, and "value destruction"—e.g. the institutionalization of corruption and waste within the economy. The process is particularly apparent in the natural resource sector.[7] This segment of the economy, and the state-owned companies within it, are a prime source for "running the engine" of power and profit distribution among elites. But breaking Russia's export dependence, systematically reforming the energy sector, or denying elites ready access to lootable capital would all risk shutting down that engine. The resource curse is thus a feature—not an abnormality—of the Russian economy.

In order to maintain the system that directs national wealth to elites, Russia's political and national security structures have developed a heightened sensitivity to any trend or event that might topple the regime. The Color Revolutions in Ukraine, Georgia, and Kyrgyzstan—as well as the Arab Spring in the Middle East—remain prime sources of concern. Russia's leadership has interpreted these revolts not as genuine acts of popular discontent against authoritarian regimes, but as manufactured political events from afar. A common refrain in elite circles is that such events were 'instigated' by the West (especially the United States) in order to encircle and contain Russia and, ultimately, topple the Putin regime itself.

Operating under the logic of "if it could happen there, it can happen here," the Kremlin rolled out a series of revolutionary counter-measures in the wake of the Color Revolutions. Their purpose was to cement the regime's hold on power by mustering pro-government demographics around emotional themes to strengthen its legitimacy. The counter-revolution, moreover, would need rallying cries, so the Kremlin set out to create them. This was the catalyst for the government's political mobilization strategy, its cultivation of nostalgia for bygone national "greatness," for the rewriting of textbooks, the revival of potent Soviet symbols, and for its youth education program targeting the United States as an

enemy in a worldwide conspiracy against Russia.[8]

For Putin, the tide of anti-authoritarian revolutions appears to have struck a nerve. His angst and frustration over this trend were particularly memorable hallmarks of his 2015 address to the United Nations. Putin used this global platform to publicly assail Western support for the Arab Spring and other revolts, asking the General Assembly, "Do you at least realize now what you've done? But I'm afraid that this question will remain unanswered, because they [the United States] have never abandoned their policy, which is based on arrogance, exceptionalism, and impunity."[9]

Context matters. When Putin delivered his 2015 General Assembly address, revolution had just returned to Russia's doorstep. In neighboring Ukraine, the "Revolution of Dignity" had toppled the Kremlin's proxy government in that country. Leaders in Moscow blamed the United States and the EU for having supported and facilitated this transition. They described how it created "deep divisions in Ukrainian society and the occurrence of an armed conflict." Moreover, they warned that it added to "deep socio-economic crisis in Ukraine [which] is turning in the long term into a hardening of instability in Europe"—and all on Russia's border.[10]

Embedded within Putin's warning to the United Nations, and associated Kremlin protestations over Ukraine, was an inadvertent revelation. Despite Russia's relative weaknesses, its leaders still view themselves as players in a Great Power competition with the United States and Europe—and they harbor a grudge. They believe that the international system treats Russia unjustly, even though Russian citizens have benefited from the international order that both sides—East and West—helped to establish after the collapse of the Soviet Empire. They see the pillars of the post-1991 order—universal human rights, democratic norms, and the rule of law—as a pretext for foreign meddling in their internal affairs. And they fear that such ideas could undermine the legitimacy of their regime and threaten its survival.

"Viewed through the lens of **those who rule Russia**, *the world is first and foremost* an alien and hostile place in which the *strong prosper over the weak.*"

Viewed through the lens of those who rule Russia, the world is first and foremost an alien and hostile place in which the strong prosper over the weak. For all the assumptions of "win-win" solutions which are embodied in the Western approach to international relations,

the world, according to Moscow, is divided into winners and losers. This has intensified the strong zero-sum mentality that has informed Russia's traditional approach to international affairs.[11] What's more, such zero-sum thinking fits into the Kremlin's preferred interpretation of the present: Russia is a beleaguered fortress, surrounded by subtle and cynical enemies who are determined to isolate, humble, and homogenize it.[12] (See Appendix I.) This is a grim world.

Adding to the zero-sum thinking that has shaped Russian statecraft is a relatively recent calculation that the international system is profoundly changing. In this assessment, the moment of American "hyperpower" after the Cold War is over. The United States and other Western powers are no longer able to exert the same dominance over the world economy, international politics, and collective norms as in past decades.[13] Kremlin leaders might denounce what they see as Western meddling in the world (specifically under the guise of democratization), but they also sense an opening—one that can facilitate a new international order.

This perceived opportunity is based on a series of postulates, including:

1. The U.S.-led Euro-Atlantic order is eroding.

2. This process is ongoing.

3. Increased social pessimism and tension will result from upheavals in the old status quo.[14]

4. The emergence of new power centers, especially in the Asia-Pacific region, will be one consequence.[15]

5. A weakening of the rules and norms of the previous order will be another outcome.

6. States which rely upon the old rules to buttress their sovereignty will be weaker—not stronger.

As Director of the Carnegie Moscow Center Dmitry Trenin has noted, "As long as all of the leading world powers, including China and Russia, agreed with the rules and regulations of this [old] order, and in the case of China also benefited from it, it represented a true Pax Americana... When Russia broke with the system that developed after the end of the Cold War, the period of peaceful relations between the main players became a thing of the past."[16]

Viewed from this perspective, the recent accumulation of disagreements between Russia and the West are *systemic*.[17] They are rooted in a fundamental quarrel over the new rules that should govern the international system. What's more, the old order still has a capable champion: the United States. Editor-in-Chief of *Russia in Global Affairs* Fyodor Lukyanov captured this sense when writing that Moscow "never took seriously the arguments in favor of a liberal world order: a game with a positive sum, where interdependence softens rivalry, the economy is primary, and politics is secondary."[18] However, Lukyanov went further, arguing that the Western vision of the world should be rejected, since neither democracy nor values promotion were possible anymore. Lukyanov criticized the "second-class Europeanism" offered by the EU—which was hardly a "worthy offer" for Russia—the West's expansion into Eastern Europe, its intervention in Serbia, its decision to "force" Ukraine to choose the EU over Russia, and its continued devotion to worldwide democratization. He asserted that Russia must now use an "Iron Fist" abroad to defend its interests. Like many other Russian commentators, Lukyanov returned to zero-sum calculations. He viewed efforts by

the United States and its allies to bolster their global position as inherently limiting Russia's influence. By exerting political, economic, and military "pressure"—Lukyanov was especially critical of NATO expansion—Western states created a "threat to Russia's national security."[19] There could be no win-win with an "Iron Fist."

One area of difference between Russian officials and experts is how Russia can manage its two-pronged challenge: maintaining sovereignty during a perceived change in the international system (on the one hand), and coping with the putative "threat" from the West (on the other). Lukyanov has argued that Russia should seek a return to 19th century balance of power constructs, "which never disappeared from the Russian political thinking, but which in the West at some point...was considered an anachronism."[20] Trenin has echoed this point, claiming that Russia should help create a system from several major world powers and to reaffirm itself as a "great power whose influence extends to the whole world."[21]

Some Russian scholars are more skeptical about the prospects for a reboot of the 19th century model. Nikolay Silaev and Andrey Sushentsov are representative of this perspective, arguing that the Kremlin's emphasis on the defense of its national sovereignty, and on its own unique "values," have no deep underpinnings. Consequently, they could be swept away by other changes in the global system. The "conservative roll, which has been outlined in the rhetoric of Moscow in recent years, has a protective, in a direct sense, reactionary character: it is only intended to create another barrier against attempts to undermine the national sovereignty and interference in internal affairs, and not to propose a new global agenda."[22]

Despite its ambitious rhetoric, the Kremlin's employment of terms like "sovereignty" and "values" boil down to one animating concept: survival. Importantly, the Kremlin has not offered an actionable and concrete proposal for what should replace the existing structure of international relations. Rather, its emphasis on Great Power concepts ultimately comes

"Despite its ambitious rhetoric, **the Kremlin's employment of** terms like 'sovereignty' and 'values' boil down to one animating concept: survival."

down to the proposition that Moscow should be accorded an entitlement to suzerainty over states that have rejected its rule (like Ukraine), and not least the United States should support that right.

Influential commentator Sergey Karaganov finds that Russia so far has neither a positive picture of the future world order nor an attractive strategy for its own development:

> "We (like China) do not fill the ideological vacuum created by the collapse of almost all international systems. Multipolarity is not the desired state of the world, but a chaos. The concept works only as the antithesis to the previous unipolarity. But what's next?
>
> Russia does not have a coherent strategy (apart from strengthening its own deterrent forces) of increasing levels of international security, which currently is in a state of severe stress if not under the threat of failure. The level of relations with the West is extremely bad, albeit largely not through our fault... the current nature of the relationship is counterproductive and harmful, we need a change of coordinates, a different angle of view, and a rejection of the obsession with the West in both pro- and anti-Western ways..."[23]

He concludes that the current situation is very dangerous:

> "Chaos and the lack of a dialogue between the world powers, not only Russia and the US but all others as well, make the situation much more dangerous than during the Cold War...this is a transitional period. It can last a very long time. And if we survive it, then in ten, fifteen or twenty years in the world there will be another system in which most likely there will be two large centers: one, conditionally, Eurasian with China's leadership, but with China balancing a number of powers, including Russia, Iran, India, South Korea, Japan, and the other, which will form around the United States. But this is if there is not a big war that can just finish the story."[24]

"If we survive it." These four words capture Russia's core challenge in the 21st century. But what if there were a way to balance the Kremlin's multiple disadvantages against the relative power of Great Power competitors like the United States? Such thinking would be premised on a Huntingtonian view of the world. If Russia indeed faced a clash with the West, would it be possible to stack the odds of success in its favor? The Kremlin's response to this question is to bet heavily that can minimize Western strengths. This requires the splintering of opposing alliances, the dividing of states against each other, and the undermining of their political systems. All the while, Russia's top-down authoritarian system must consolidate its own population, resources, and cultural base. Such a strategy intentionally avoids competing in those areas where Russia is weak in the hope that, should a direct confrontation occur, Russia will enjoy a more level playing field. Survival is the goal. Chaos is the means.

SECTION 2—CHAOS FOR STRATEGIC EFFECT

What is Chaos? In the realm of the physical sciences, chaotic systems possess a nearly infinite number of components. When these components interact, they produce seemingly unpredictable or highly complex behavior. The weather, stock markets, and even the diffusion of creamer in a cup of coffee are all examples of "nonlinear dynamic systems" in action.[25] While humans tend to think of these systems as chaotic, there is an underlying order within the disorder. There is an organizing structure to the randomness.[26]

In military science, chaos also has a well-established pedigree. Practitioners and

theorists have long advocated its use as a strategy. Great Powers across history have continually sought to sow instability in neighboring states—often through the use of what we now call information warfare—to enhance their own security. When Great Powers employ chaos strategies, they tend to be peripheral to other, more conventional forms of state competition. Since Great Powers usually have superior resources at their disposal, the defining question in such cases typically comes down to the best use of those resources—either directly or indirectly—against an opponent.

For weaker powers, chaos strategies tend to hold the greatest appeal. The strategy promises to compensate for a weak actor's strategic inferiority. In Russian history in particular there is a tradition of the state stoking chaos on the far frontier to keep rivals divided and feuding internally—and thus unable to combine forces against Russia. Since direct engagement by Russian forces with the modern U.S. military would prove extremely costly, "the [Russia] chaos strategist, by contrast, must manipulate the scenario to his best advantage while striving to prevent the introduction of American military force" into a conflict.[27] Chaos can offer an edge.

Sun Tzu

One of the first scholars to extensively consider these kinds of questions in warfare was Sun Tzu. As a starting premise, his *Art of War* postulates that all warfare is first based on deception:[28]

> "Thus although you are capable, display incapability to them. When committed to employing your forces, feign inactivity. When your objective is nearby, make it appear as if distant; when far away, create the illusion of being nearby. Display profits to entice him. Create disorder (in their forces) and take them. If they are substantial, prepare for them; if they are strong, avoid them. If they are angry, perturb them; be deferential to foster their arrogance. If they are rested, force them to exert themselves. If they are united, cause them to be separated. Attack where they are unprepared. Go forth where they will not expect it. These are the ways military strategists are victorious. They cannot be spoken of in advance."[29]

Notably, Russian military thinking long has been close to Sun Tzu when it comes to the conduct of warfare.[30]

Sun Tzu derived several related concepts from the idea that strategy should unbalance an enemy—e.g. create disharmony and chaos.[31] He focused on manipulating an enemy. In this way, a practitioner of the military arts created opportunities for easy victory. An enemy was weakened through confusion about one's own position, through the subsequent dislocation of opposing forces, and by putting those forces in a state of disorder. Sun Tzu offered a number of strategic and tactical factors that, together with grand strategic factors, combined to put an enemy off balance. Sun Tzu's goal was to maneuver an opponent into a position against which the potential energy of one's own army could be released with the maximum effect and to attack where an opponent was not prepared. One should avoid a battle, Sun Tzu cautioned, until a favorable balance of power was created. In his famous counsel to strategists across millennia, "One who knows when he can fight, and when he cannot fight, will be victorious. One who knows the enemy

and knows himself will not be endangered in a hundred engagements. Subjugating the enemy's army without fighting is the true pinnacle of excellence."[32] Among Sun Tzu's methods to put an enemy off balance, he emphasized the importance of surprise through deception and deceit. He also introduced the concept of *formlessness* (e.g. maintaining a high tempo, ensuring variety and flexibility in actions) and of using both orthodox and unorthodox methods.[33] Another concept that was applicable to chaos in the military arts was Sun Tzu's *yin*—the notion that a general must be responsive to context. They should adapt to any situation in such a manner as to take full advantage of its defining circumstances and avail themselves to all the possibilities of a given situation.[34] In Sun Tzu's thinking, "Do not fix any time for battle, assess and react to the enemy in order to determine the strategy for battle.[35]

Clausewitz

Alongside Sun Tzu, another titan of strategy who considered the use of chaos was Carl von Clausewitz. In *On War*, Clausewitz defined warfare as a "remarkable trinity" composed of (1) the blind, natural force of violence, hatred, and enmity among masses of people; (2) chance and probability, faced or generated by the commander and his army; and (3) war's rational subordination to the policy of the government.[36] Clausewitz recognized the need for a theory of war that would maintain a "balance between these three tendencies, like an object suspended between three magnets."[37] For Clausewitz, warfare was a mix of order and unpredictability.[38] It resembled the form of a nonlinear dynamic system in that its rhythms and outcomes were shaped by many competing, interactive factors. From this came one of Clausewitz's conclusions about war: "The second attribute of military action is that it must expect positive reactions, and the process of interaction that results. Here we are not concerned with the problem of calculating such reactions—that is really part of the already mentioned problem of calculating psychological forces—but rather with the fact that the very nature of interaction is bound to make it unpredictable."[39] Hence, Clausewitz became one of the first scholars to perceive and describe "unpredictability" as the key feature of nonlinearity in war.[40]

Enter Prometheus...

Despite its use and repetition throughout time, not all strategies of chaos are the same—nor are they created equally.[41] During the first half of the 20th century, Poland's famed statesman Józef Piłsudski executed one of the more innovative nonlinear chaos strategies in the history of statecraft. He dubbed it "Prometheanism" in homage to the mythological Greek hero who rejected the authority of the more powerful Zeus. Prometheanism was Piłsudski's answer to the enduring question: How can a relatively weaker power successfully compete against a much stronger one? Today, an updated form of Prometheanism is allowing an aggrieved Russia to overcome its specific strategic disadvantages in the 21st century.

In the case of Piłsudski, Poland's solution was to exploit the vulnerabilities of neighboring Russia by creating divisions and distractions across this rival's territory. Compared to Russia, Piłsudski's Poland was relatively weak. However, he could level the playing field by stoking the troublesome legacy of the former Czarist empire: Russia's nationalities problem. By supporting potentially disruptive independence movements across Russia, Piłsudski intended to keep his rival off balance. Chaos was his strategy. Fostering disorder inside Russia was his means. Keeping an

Józef Piłsudski with Supreme Command of Polish Military Organization in 1917. Photo Credit: Wikimedia.

aggressive Bolshevik state at bay was his goal. Unfortunately, Piłsudski's Prometheanism may have had unintended, adverse consequences: It probably informed the USSR's own subsequent strategy of exploiting its opponents.

In the contemporary context, definitions matter. Here we define Prometheanism as the calculated application of nonlinear statecraft (e.g. the use of disinformation, subversion, etc.) to weaken an opponent by the creation of internal divisions at home and external isolation abroad. We consider Prometheanism as a specific member of a larger family of chaos strategies used throughout history. While Prometheanism is not the only form of a chaos strategy, it can be highly effective under the right circumstances. It can also fail—sometimes spectacularly. Prometheanism is also not specific to Poland. It has often been used by actors against strategically stronger adversaries. Indeed, it existed before Piłsudski gave it a fabulous brand.

One example of a Promethean strategy in action was Germany's successful attempt to back Russian revolutionaries against the Czarist government during World War I. Berlin's strategy supported Lenin and his Bolsheviks. Facilitating their activities in Russia had a purpose (in Berlin's view): to destabilize the Czarist Empire from within and weaken its alliance with Western powers. Germany provided the Bolsheviks with propaganda support and weapons; and it helped Lenin re-enter Russia from his exile in Switzerland. In 1917, Germany's top army command reported to its Foreign Office that, "Lenin's entry into Russia was a success. He is working according to your wishes."[42]

After unleashing Lenin on Russia, Germany's strategy succeeded against improbable odds—and perhaps even beyond Berlin's highest hopes. As German Minister of Foreign Affairs Richard von Kühlmann pointed out following Lenin's successful seizure of power

in the October Revolution, the "disruption of the Entente and the subsequent creation of political combinations agreeable to us constitute the most important aim of our diplomacy." Von Kühlmann confided to the Kaiser on December 3, 1917: "It was not until the Bolsheviks had received from us a steady flow of funds through various channels and under varying labels that they were in a position to be able to build up their main organ *Pravda*, to conduct energetic propaganda and appreciably to extend the originally narrow base of their party."[43] Peace with Germany followed.

> "***An updated form of Prometheanism*** is allowing an aggrieved Russia *to overcome its specific strategic disadvantages in the 21st century.*"

Upon consolidating power in March 1918, Lenin's Bolsheviks signed of the Treaty of Brest-Litovsk. It was the peace accord that Lenin had long promised to sign with Germany. And while the Brest-Litovsk peace talks reflected the Bolsheviks' own interests, the ensuing peace came at great cost, with the surrendering of vast and important agricultural regions. With this peace, Germany effectively won World War I on the Eastern Front. Alas, the Kaiser's military fortunes were less sanguine on the Western Front. The overall war ended badly for Germany.

During the interwar period of the 20th century, Soviet policy in the Baltics represented a form of Prometheanism in action, especially in the Kremlin's use of disinformation and political subversion against its neighbors. By this time, Soviet leaders had learned much from grappling with Piłsudski's Promethean gambit against them. Moscow had internalized the value of chaos and mastered the technique. The Kremlin's subsequent Promethean campaign against the Baltics underscored an additional aspect of the strategy: it need not be an end in itself. It can also be preparation for more kinetic forms of warfare. Upon the signing of the Molotov-Ribbentrop Pact in 1939, which divided the territory between Germany and the USSR into respective "spheres of influence," the Soviet Ambassador to Tallinn reported with satisfaction that Estonians were left "bewildered" and "disoriented." The Kremlin's subterfuge was complete. Its calculated use of disinformation in the Baltics had disguised Moscow's true hostile intentions in the run-up to war, leaving its neighbors strategically off balance. Prometheanism had worked.[44]

In the early phases of the Cold War, the Soviet Union again used Prometheanism against West European states—creating fifth columns and intentionally pitting discrete political factions against one another. The attempt to weaken the West had a number of purposes: to

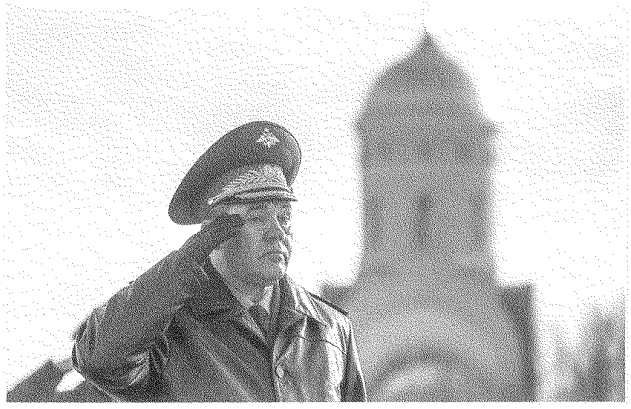
prevent rearmament in Germany; to discredit pro-British and American leaders in Italy; to engender beneficial political chaos for local communist parties to exploit; and to win *de facto* recognition for Moscow's solidification of power in the eastern half of the continent. The postwar era likewise revealed an inherent danger of Prometheanism: blowback. Soviet policy in Europe eventually backfired dramatically by becoming a major stimulus for the Marshall Plan.

...Gerasimov Updates

Two decades after the Cold War, Russian General Valery Gerasimov, Chief of the General Staff, took the next major step in the history of Promethianism by fusing chaos to Russia's contemporary strategic goals. In February 2013, Gerasimov articulated his theory of modern warfare in a now-famous article for the *Military-Industrial Kurier*.[45] (The article was based on a speech he had presented at the Russian Academy of Military Science the month before.) The modern concept of chaos would thereafter be different thanks to Gerasimov.

Gerasimov started from the beginning. He took tactics developed by the Soviets, blended them with strategic military thinking about total war, and laid out a new theory that was more akin to hacking an enemy's society than attacking it head-on. In the article, Gerasimov wrote: "The very 'rules of war' have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness... All this is supplemented by military means of a concealed character."[46] Sun Tzu would be proud.

While discussing the Arab Spring and NATO's intervention in Libya, Gerasimov highlighted,



Russian Chief of the General Staff Valery Gerasimov. Photo Credit: Russian Ministry of Defense.

and apparently endorsed, general trends in Western approaches to warfare starting with the 1991 Gulf War. To him, the key element of change in the current operating environment was the increasing importance of non-military tools in conflicts, such as political, economic, informational, and humanitarian instruments. Gerasimov suggested that "in terms of efforts employed in modern operations, the ratio of non-military and military operations is 4 to 1."

> "*Still channeling Sun Tzu,* Gerasimov specified **that the objective was to** *achieve an environment of* **permanent unrest and conflict** within an enemy state."

Goals would be achieved by using clandestine military operations and Special Forces (among other means). By contrast, visible military force would only be used in the form of peace-keeping and crisis management operations.

The article, considered by many to be an outline of Russia's modern hybrid strategy, laid out a vision of total warfare. It placed politics and war within the same spectrum—philosophically, but also logistically. The approach was guerrilla and waged on all fronts with a range of actors and tools—hackers, media, businessmen, leaks, and fake news, as well as through conventional and asymmetric military means alike. Thanks to the internet and social media, all kinds of psychological operations—including upending the domestic affairs of nations with information alone—were now plausible. In building a framework for these new tools, Gerasimov declared that non-military tactics were not *auxiliary* to the use of force. They were the war. Chaos was the strategy. Still channeling Sun Tzu, Gerasimov specified that the objective was to achieve an environment of permanent unrest and conflict within an enemy state.[47]

Importantly, Gerasimov did not exclude conventional forces from his thinking. On the contrary, he stressed Russia's need for innovation and the wider modernization of its armed forces. By including this additional point, he scattered Western assessments of his writing into different directions. Some Western readers of the text wondered if his key message was to outline a new Russian approach to war, or simply to reproach Russian military leaders for not sufficiently studying contemporary war as it was waged by others. The proponents of the latter approach argued that Gerasimov did not refer to a new Russia "doctrine," nor did he outline future approaches. In this interpretation, he intended to highlight the primary threats to Russian sovereignty in an attempt to suggest that the Kremlin's political leadership needed to be more open to innovative ideas on future security challenges.[48] Writing on the Gerasimov doctrine, analyst Charles Bartles has argued that it should not be seen as a proclamation of the strategies of the Russian military and security services, but an outline of what *Russia believes is being done by the West*, and how Russia can hope to understand and

counter *what they believe the West is doing to them*. For this reason, Bartles contended that Gerasimov was really expounding upon the alleged use of asymmetric warfare via the various Color Revolutions of the 2000s-2010. He concluded that the West used massive disinformation campaigns to destabilize non-Western friendly nations by means of NGOs within, combined with a barrage of sensational or outright fictional news coverage from friendly media outlets without.[49]

By contrast, scholars who viewed the Gerasimov doctrine as prescriptive emphasized the strong correlation between his concepts and the Kremlin's subsequent military action in Ukraine. Such analysts argued that Gerasimov outlined a Russian model of war which integrated all elements of national power with a military capable of using both deniable irregular and high-technology conventional forces.[50] They pointed out that Russian operations resembled the ancient military thinking of Sun Tzu, rather than a more contemporary Western method of warfare.[51] Thus, Gerasimov's article was too thorough a preview for Russia's subsequent actions in Ukraine to have been a mere descriptive article. Instead, they claimed it represented a form of "mirror imaging"—something designed to mask Russia's method of conducting "hybrid war" with references to an alleged American approach.[52] In this sense, Gerasimov was suggesting a specific approach: to turn the playbook of Western adversaries against them via nonlinear war.[53] It is notable that Putin has personally employed similar mirror imaging. For example, he used the term "controlled chaos" in a pre-election article on defense in 2012. In that article, Putin argued that Russia was under attack from the West, which by various means—political as well as economic—was destabilizing Moscow's strategic neighborhood, and ultimately Russia itself.[54]

Two key events support the conclusion that Gerasimov was being *prescriptive*.

First, the comprehensive military reform in Russia, ongoing since 2008, integrated the two strands—civilian and military—of hybrid warfare. This was in line with Gerasimov's argument that the prevalence of information systems made them useable as warfighting tools, and they had decreased the "spatial, temporal and information gap between the armed forces and government."[55] In effect, Russia's reform of the armed forces shrunk the barriers between the civilian and military output of information warfare (and other tools of hybrid warfare) to create a requisite degree of synergy between them.[56] These reforms were thus probably based on an updated Russian warfighting concept that:

> "...put a new face on hybrid warfare by incorporating non-military measures into the battlefield in intensive ratios effectively, conducting a good refinement of the Soviet legacy 'reflexive control' concepts to disguise Kremlin's campaigns abroad, and also by linking strategic, operational, and tactical levels of a campaign efficiently within the context of full spectrum operations, proxy war, special operations, and subversive activities. This strategic perspective is supported by a new force posture, renewed doctrinal order of battle, and robust combined arms capabilities for elite units at permanent readiness levels."[57]

Second, Russia's aggression against Ukraine a year after the publication of Gerasimov's article demonstrated the intense use of the elements of hybrid warfare methods that he had already discussed. Several related terms have been used to describe Russia's military action there: "hybrid warfare," "gray zone strategies," "competition short of conflict,"

"active measures," "unconventional warfare," and "new generation warfare."[58] Despite differences in vocabulary, these terms all focus on the Kremlin's use of multiple instruments, as Gerasimov highlighted, with an emphasis on non-military tools to pursue Russian national interests outside its borders.[59]

> "While Gerasimov and his generals **may think of 'active measures'** *primarily as a prelude to armed operations,* **the Kremlin's own national security specialists** *still regarded them as an alternative.*"

While in previous post-Cold War conflicts Russia employed its traditional doctrine and was not impressively successful, Crimea was different: it might either have been an exception to the pattern of Russia's past performance or it was a "new norm" with which the West must now contend.[60]

Some analysts have highlighted the key elements of "hybrid warfare" that were successful in Crimea (and in the Donbas). These were:

1. Capturing territory without resorting to overt or conventional military force—exemplified by the infamous "little green men" operating in Ukraine in 2014.

2. Beginning a proxy war with a key role assigned to the security services and special forces, and creating a pretext for overt, conventional military action.[61]

3. Using hybrid measures to influence the politics and policies of countries in the West and elsewhere, in Gerasimov terms, to make "use of internal opposition throughout the adversary's area as a permanent front."[62]

Still other analysts have argued that the conflict in the Donbas was a "hybrid war" mostly during its early stages, before the introduction of large numbers of regular Russian troops bolstered the faltering prospects on the battlefield of the pro-Russian "separatist" fighters.[63] In those early days, armed "volunteers" supported by the Russian security services led a wave of occupations of Ukrainian government buildings in Eastern Ukraine. They organized "militias" and announced the goal of the region's independence and eventual unification with Russia. The Russian government then relied on gray zone tactics that reflected its desire to conceal direct involvement in the fighting. All the while, it provided pro-Moscow fighters with weapons and logistical support. Its regular soldiers stripped of any identifying signs to fight in the insurgents' ranks, making them the iconic "little green men" of the conflict.[64]

In the case of the war in Ukraine, analyst Mark Galeotti has injected a key, often overlooked point into the discussion about Gerasimov's intentions:

> "...we should not be thinking of this primarily in military terms. What we call 'hybrid war' in Russian thinking is actually separate things. What Gerasimov was talking about was the use of subversion to prepare the battlefield before intervention... Breaking the chain of command, stirring up local insurrections, jamming communications—these are all classic moves that hardly began in Crimea."[65]

It is a reasonable point. Generals think like generals. And while Gerasimov and his generals may think of "active measures" primarily as a prelude to armed operations, it is important to remember: the Kremlin's own national security specialists still regarded them as an alternative.

Once again, the organizing problem is survival. The National Security Strategy of the Russian Federation makes abundantly clear: the Kremlin views NATO as a formidable enemy. Consequently, this strategic document takes pains to prevent small-scale, localized conflicts from ever inviting the arrival of NATO forces into a contested theater. Implanted here is Russia's recognition of its weakness—and Western strength. Kremlin strategists therefore faced a dilemma: how can a country with a relatively small economy, an army that is still going through an expensive modernization, and little positive soft power compete with a larger, richer coalition of democracies to achieve its foreign policy goals?[66]

Prometheanism in Action

The Kremlin's answer to the question of competition has been contradictory, opportunistic, and often effective.[67] But there is an answer at the bottom.

Clearly, it is possible to showcase examples of Russia acting as a Great Power. This behavior pattern is most apparent when Russia applies its traditional political, diplomatic, economic, and military means to various global or regional conflicts for the purpose of creating the *impression* of strategic relevance. In this way, the Kremlin tries to demonstrate that it still deserves to play an important role in international politics and that without Russia it is impossible to resolve many global problems.[68] When it serves Moscow's purposes, the Kremlin often uses these forays to insist that a cardinal rule for solving international problems must be non-interference in the internal affairs of other states. There are two reasons to be cautious about Moscow's words and motivations. First, such rhetoric bolsters Russia's larger goal of defending itself against outside regime change (i.e. survival). Second, the Kremlin has no qualms about breaking its own non-interference rule in the case of Ukraine or Syria.

As a contradictory opportunist in the international system, Moscow also has begun to reorient its diplomatic priorities. While Europe remains important, the Kremlin has pursued closer relations with China, and granted high priority to relations with CIS and BRIC countries. Russia has emphasized the development of the Eurasian Economic Union, which came into existence on January 1, 2015, and used its veto power in the UN to advance an anti-Western agenda and defended other rogue regimes like Iran and Syria.

A Soviet platoon in 1992. Photo Credit: United States National Archives.

Hard power still matters. The Kremlin has thus invested heavily in modernizing its armed forces. Its purpose is to thwart Washington's ability to project power into Moscow's self-proclaimed sphere of influence. Russia's military, although no match for the United States on paper, carries out frequent large-scale exercises. It is capable of conducting high-intensity warfare at short notice across a narrow front against its neighbors and NATO forces. Lest anyone forget, Russian military aircraft regularly probe Europe's air defenses and execute dangerous maneuvers around Alliance warships, risking an escalatory incident. Here too, hard power capabilities (and their use) are a means to an end. Abroad, they assert the impression of Russia's Great Power status. At home, they generate strong political benefits to the regime in the form of enhanced public support.[69]

The power imbalance between Russia and the West is nevertheless real. In the situations where Russia enjoys a weaker hand against its adversaries, the Kremlin employs the Promethean approach. It sows chaos and confusion, even if its strategic objectives are vague.

For all of Russia's weaknesses as a Great Power, leaders in Moscow still think that they possess a decisive advantage in long-term competition with the United States and its allies—and that they can miscalculate. They can consider that Russia is more cohesive internally and might outlast its technologically superior but culturally and politically pluralistic opponents. This working assumption is predicated on the fact that the West may have more capacity but it lacks the will to use it to the fullest; Russia, by contrast, has the will, and can thus do more with less, so long as it retains the initiative and the psychological advantage.[70] The Kremlin's goal is therefore to cause trouble for its own sake—to create an environment in which the side that copes best with chaos (that is, which is less susceptible to societal and geopolitical disruption) wins.

This approach has practical applications in current U.S.-Russian relations. For example, a reportedly widespread view among Russian foreign affairs officials is that Moscow should give U.S. President Donald Trump time to overcome anti-Russian sentiment in Washington, and to shore-up his domestic political base. His expressed interest in better relations with Russia can then be used to normalize the U.S.-Russian bilateral relationship and advance Moscow's interests in a traditional, Great Power fashion. A second approach, reportedly widespread in the security services, seeks to encourage chaos. Interpreting Trump as an anti-establishment politician whom the U.S. political class has rejected, they see him as an actor who disorientates the American polity. This view is Machiavellian. It seeks to advantage Russia by spreading disorder in American politics and undermining Western unity. As Russia's influence operations against the West unfold, they will strengthen Russia's ability to probe for deeper weaknesses inside the Atlantic Alliance.[71] The fact that none of these calculations might actually be true is immaterial. Some Russian elites believe it.

Time and Risk

An elemental assumption of Russian Prometheanism is that time is on the Kremlin's side. If only Russian leaders stay the strategic course and remain patient, sooner or later Western unity will crack, U.S.-EU sanctions on Russia will end, disgruntled Western voters will put pro-Russian governments in power across Europe, and Washington will treat Moscow as an equal partner. These hopes have probably strengthened due to the policy disarray emanating from the United Kingdom's decision to leave the EU, and continuing European disagreements over the migration crisis, trade, and defense spending. Especially after Brexit, Russian elites can calculate that it may be politically impossible for the EU to expand further east now that its political house is crumbling.[72] By reading recent events, moreover, it is possible for Russian leaders to also assume that risk taking works. Thus far, this practice has bolstered Putin's standing at home and forced the West to "take Russia seriously." In fact, it is even possible to read from Putin's own words and actions that he sees the West in general as lacking the will to challenge him.

> "As with all risky schemes, *the concept is simple*. **The execution is tricky.** In Russia's case, **Prometheanism requires the Kremlin** *to never make a false step*."

On the surface, Moscow can judge that it derives the most benefit from confrontations which do not result in direct, kinetic collisions. By far the greatest danger of this conclusion is that the Kremlin may ignore (or at least undervalue) the inherent risks of its Promethean strategy.

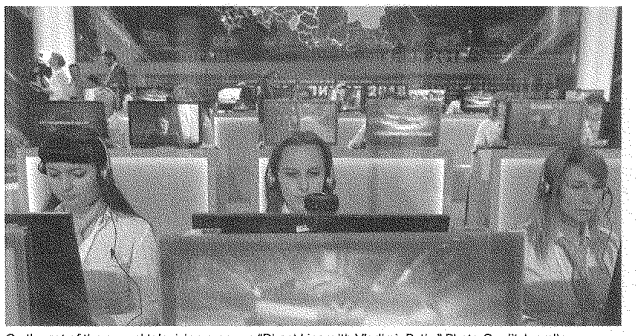
Seeding disorder abroad and picking fights when Russia's advantages seem greatest will always require the West to blink first. Done correctly, however, the Russian regime does not need to spark another Cuban Missile Crisis or Korean War. It can insulate itself from Western "encroachment," and perhaps even renegotiate the future of the international system, without worrying about a full-scale war with NATO. Disorientation and distraction in the West will produce more one-sided concessions for Russia than victory on the battlefield. The key is to never lose control of escalation in a dispute—lest a low-threshold confrontation become highly kinetic.

As with all risky schemes, the concept is simple. The execution is tricky. In Russia's case, Prometheanism requires the Kremlin to never make a false step. Here the working assumption is that, while the West has more capacity, it will never match Russia's willingness to deploy the full instruments of state power. Russia, by contrast, will always have that will, and can do more with less so long as it retains the initiative and psychological advantage. Unfortunately, this thinking requires the Kremlin to perpetually play by "Chicago Rules." That is: "He pulls a knife, you pull a gun. He sends one of yours to the hospital, you send one of his to the morgue."[73] In geopolitical terms, Russia must always be willing to take disproportionate retribution, regardless of the rights and wrongs of a situation, with the hope of forcing less resolute adversaries into backing down.[74] Such a dynamic therefore forces Western leaders to be perpetually more concerned with irritating or provoking Putin instead of pursuing their own national interests. When this does not occur, and leaders break the pattern, then the Promethean gamble collapses. Rapid escalation by an adversary can swiftly follow.

Geography

Within its geographic neighborhood, Russia seeks to maintain its sphere of influence, where its aim is to slow down the pace of democratization and integration into the West and prevent a "spillover" effect that might threaten the Putin regime itself (once again: survival). In the Baltics, the Kremlin tries to drive wedges between ethnic Russians and their governments, NATO, and the EU.[75] In Ukraine, Russia at first largely followed the Gerasimov doctrine: during the 2014 protests it supported extremists on both sides of the crisis—pro-Russian extremists and Ukrainian ultra-nationalists—fueling conflict that the Kremlin used as a pretext to seize Crimea and launch a war in the Donbas. So: "Add a heavy dose of information warfare, and this confusing environment—in which no one is sure of anybody's motives...is one in which the Kremlin can readily exert control."[76]

Farther abroad, Moscow tries to achieve policy paralysis by sowing confusing, stoking fears, and eroding trust in Western and democratic institutions. Its so-called fight against terrorism is one of the most transparent foreign policy pretexts used in recent years to project strategic relevance into more distant regions. Russia uses the counterterrorism narrative to strengthen its foreign policy position and to establish relations on a political and security institutional level. While Russia publicly seeks to show its readiness for international cooperation by invoking the fight against terrorism in Syria, or to restrain North Korea's nuclear ambitions, this is actually a cover for a contrarian policy for its own sake. The larger goal: to flout international conventions and agreements. (See Appendix II.)



On the set of the annual television program "Direct Line with Vladimir Putin." Photo Credit: kremlin.ru.

SECTION 3—THE CENTRALITY OF INFORMATION WAR

Where does information warfare fit into Prometheanism? More than traditional arenas such as economic and military competition, the information battleground between Russia and the West has become a prime area where the Kremlin has implemented its Promethean strategy.[77]

"Information warfare" is defined here as: The deliberate use of information by one party against an adversary to confuse, mislead, and ultimately influence the actions of a target. This definition is inclusive enough to cover propaganda, influence operations, deception, and *aktivka* (active measures).[78] Just as Piłsudski once attempted to balance Poland's weaknesses by exploiting Russia's vulnerabilities, today's Kremlin-backed efforts to manipulate the information space use the openness of Western systems against them. Unlike during the Cold War, today's Russian propaganda does not crudely promote the Kremlin's foreign policy agenda. Instead, it has tried to confuse, distract, and disrupt Western states. Information operations are often used with other forms of hard and soft power—leveraging cultural ties, energy, money, and bribery in non-kinetic "combined arms" operations. The mix of weapons depends on the assessed vulnerabilities of the target or country.

Russia takes a territorial approach to its "information space"—the media, potential audience, and infrastructure—which it views as defined by a country's borders and immediate neighborhood.[79] As SVR head Sergey Naryshkin said on April 27, 2017, "The task of strengthening information sovereignty is as relevant as increasing the defensive potential or developing the national economy" in the 'post-truth' era.[80] This concept reflects the Kremlin's understanding of geopolitics and

the importance of national sovereignty (noted earlier). Although some Russian scholars believe that the expansion of the internet and digital spaces are beneficial, many others—and the government itself—see it as threatening to national security, traditional Russian values, and the legitimacy of the regime. This is especially the case with social media, which is more difficult to control than television or terrestrial radio.[81]

At home, Vladimir Putin has systematically clamped down on internal communications—primarily television, which reaches 99 percent of the Russian population and which 73 percent of the Russian people watch every day—as well as newspapers, radio stations, and the internet.[82] The Kremlin also "tests" new mechanisms on its population. ("Bots" probably were first used on a massive scale in 2011-12 against Russian leaders to discredit anti-Putin protests.) If the new tactics are proven to be effective, the regime upgrades them for use against external targets. Abroad, the Russian president has positioned himself as an international renegade, deploying high-gloss, contrarian media outlets like *RT* (previously *Russia Today*) and *Sputnik*, as well as an army of online trolls, to shatter the West's "monopoly on truth." The sweeping scope and extensive range of this campaign indicates the extent to which the Kremlin has committed to harnessing information in order to amplify existing tensions and divisions in Western societies. As previous CEPA analysis has highlighted, when the "space for a democratic, public discourse and open society breaks down, it can become atomized and easier to manipulate through a policy of divide and conquer." Information operations are therefore a means for prevailing over a perceived adversary.[83] In the case of Western democracies, crucial elements of an open society such as TV channels, social media, civic groups, political parties, or economic actors now regularly serve as the Kremlin's weapons in the spread of disinformation. Sometimes, these actors may even be unaware of it. The net effect is still the same: to use the openness of Western systems against Russia's perceived adversaries.[84]

Examples of Russia's information strategy in action are numerous. In the Baltic States, modern Russian disinformation tries to exploit fears of U.S. abandonment, while simultaneously stoking feelings of alienation among local populations. In Romania, Russia foments animosity toward Western "meddling" and eats away at public faith in NATO. In countries like Ukraine, where Russia claims critical national interests, Moscow tried to incite and exploit ethnic and linguistic feelings to create a prelude for a land grab. It is Russian disinformation that has attempted to cultivate anti-Ukrainian sentiments among the Polish population, and widened internal and public cleavages in Lithuania over energy diversification policies. Facts have become disfigured. Policy debates have become diverted. NATO has become the "enemy" in some corners. Publics are left dismayed, suspicious or inert. Euro-Atlantic solidarity erodes. Disinformation is only a *means*. Chaos is the *aim*. (See Appendix III.)

The Russian practice of information warfare combines a number of tried and tested tools of influence with a new embrace of modern technology. Some underlying objectives, guiding principles, and state activity are broadly recognizable as reinvigorated aspects of subversion campaigns dating back to the Cold War era (and earlier). But Russia also has invested extensively in updating the principles of subversion.[85] These investments cover three

main areas: internally and externally focused media with a substantial online presence (*RT* and *Sputnik* are the best known of these outlets); the use of social media (especially online discussion boards and social pages, e.g. Facebook) as a force multiplier to ensure Russian narratives achieve broad reach and penetration, and language skills in order to engage with target audiences on a wide front. The result is a presence in many countries that acts in coordination with Moscow-backed media and the Kremlin itself. It should be emphasized that Russian disinformation operations visible to English-language audiences are only part of a broader front covering multiple languages. These include not only state-backed media and trolling, but also "false flag" media—sock puppet websites set up to resemble genuine news outlets. These seed news feeds with false or contentious reporting that ties in with Russian narratives. This false flag approach extends in different directions, with *RT* determinedly masquerading as a broadcaster or cloning accounts on social media in order to mimic and discredit genuine Western media outlets.[86] The Kremlin also relies on conferences, cultural activities (concerts and other events), video products (documentaries, art films, cartoons, video games, NGOs, individual speakers, opinion leaders, think tanks, and academia). The level of creativity deployed to undermine the West is certainly impressive.

Externally Focused Media

State-controlled *RT* is perhaps the most prominent mechanism by which Russia disseminates disinformation abroad. The channel plays a critical role in shaping the online and broadcast international media environment, either by openly spreading narratives in host countries' native languages, or by laundering Kremlin narratives through local, "independent" proxy media. *RT* is particularly well-placed to accomplish this task. It has a $300 million budget, online platforms with high visibility on social media, and dozens of foreign-based stations broadcasting in no fewer than six languages: Arabic, English, French, German, Russian, and Spanish. Much of its online content has also been translated into various Eastern European languages. For her part, *RT* chief Margarita Simonyan disputes the assertion that her platform has direct connections with the Kremlin. She has dismissed allegations that *RT* serves as a Putin mouthpiece as "McCarthyism." That said, Putin has asserted that *RT* and related platforms nevertheless exist to "break the monopoly of the Anglo-Saxon global information streams."[87]

Also of significance is *Sputnik*. Since November 2014, the state-owned international network has employed a varied array of disinformation tools such as social media, news outlets, and radio content. In 2017, *Sputnik* operated in 31 different languages, had a $69 million annual budget, and maintained 4.5 million Facebook followers (by contrast, *RT* has 22.5 million). Its primary purpose, much like that of *RT*, is to "ping pong" unreliable information, suspect stories, and pro-Russian narratives from marginal news sites into more mainstream outlets (see Appendix I). As such, despite relatively low readership compared to mainstream media, *Sputnik* has proven useful for Moscow's interests, often pursuing and amplifying conspiracy theories that have already been discredited.[88]

Cyber activities in the broad sense are critical to Russia's offensive disinformation campaigns—whether by establishing sources for disinformation via false media outlets online

or by using social media to address targets of opportunity for subversion and destabilization efforts. These activities are augmented by the ubiquitous activities of trolls (often fake online profiles run by humans) and bots (fake profiles run by automated processes), which exploit the relationship between traditional and social media to plant, disseminate, and lend credibility to disinformation campaigns.

> "***Russia's authoritarian media*** enjoy some *clear advantages in the* **competitive creation of chaos.**"

The large amount of resources devoted to this effort stems from a recognition that digital media is becoming the main—and for a growing number of young people, the only—platform for political information and communication. This trend is so advanced, that such channels are beginning to resemble a 21st century variant of the "town square." They are certainly becoming the primary space for political activities, where citizens receive and share political information, shape their political views and beliefs, and have the opportunity to influence processes related to the functioning of power. Russia's cyber activities consequently also capitalize on the fact that sharable social media has become the most effective tool for influencing the minds of huge communities, even whole nations.[89]

Another related campaign—and one that is commonly underestimated—entails the use of false accounts posing as authoritative information sources on social media. Take Finland for example. Before they were suspended, the Twitter accounts @Vaalit ('elections' in Finnish) and @EuroVaalit looked at first sight like innocent, and possibly even official, sources of election information. No doubt many people, without looking closely, took them for precisely that. In fact, they (and a range of associated accounts) repeated Russian disinformation. Perhaps unsurprisingly, their profiles linked to RT. Multiply this approach by many different languages, countries, and campaigns, and factor in competing Russian successes when closing down opposing social media accounts (noted earlier), and the cumulative effect cannot be other than highly corrosive.[90] More troubling still, the Finnish example is replicable. Russian experts learn and adapt.

Impact: Strengths

Russia's authoritarian media enjoy some clear advantages in the competitive creation of chaos. First, the Kremlin does not need to beat its Western competitors outright—only to keep them confused, uncoordinated, and off balance. Second, Russia's authoritarian system grants its leaders a natural advantage in managing the psychology and politics of disorder—in such regimes, it is easier to make

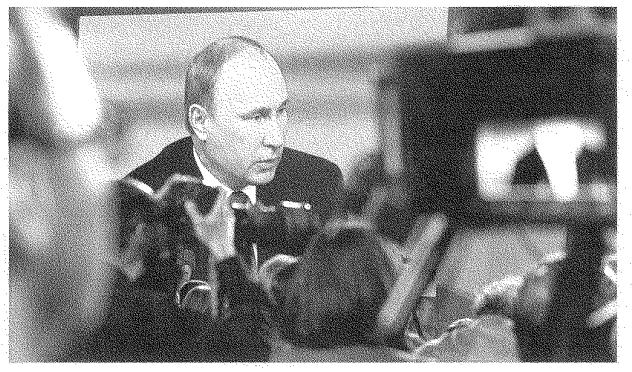
the comprehensive, whole-of-government approach work. A third advantage is stealth: Russia's disinformation (and associated cyber) operations—a prime vehicle for seeding division and distraction—leverage the anonymity, immediacy, and ubiquity of the digital age. As seen in recent Western elections, Russia regularly catches the West off guard.

Judged by these standards, Russia's authoritarian media has made a major impact on many issues and audiences. Within Central and Eastern European (CEE) countries in particular, Russia has successfully exploited the "bitter memories of past territorial disputes, nationalist-secessionist tendencies, and the haunting specters of chauvinist ideologies promising to make these nations great again."[91] In January 2016, the infamous German "Lisa" case, in which a Russian-language channel incorrectly reported that migrants had sexually assaulted a 13-year-old German girl, led to massive anti-immigrant and anti-government protests. Even after the story had been disproven, *RT* and *Sputnik*'s German- and English-language outlets amplified it.[92] More recently, Germany's far-right, anti-immigrant, and Kremlin-friendly *Alternative für Deutschland* (AfD) party received favorable coverage of its candidates and narratives in the run-up to Germany's September 2017 election, which may have helped it become Germany's third-largest party.[93] Favorable *Sputnik* coverage also may have boosted the showing of the pro-Moscow populist parties, the Five Star Movement and *Lega Nord*, in the recent Italian elections.[94] During the 2016 U.S. presidential election campaign, the effectiveness of Russian trolls prompted some U.S. businesses to hire them to run favorable material for $25 to $50 per post. One former troll told *RFE/RL* that employees at a St. Petersburg troll factory were required to remain on duty 24/7, activated for 12-hour shifts, with a daily quota of 135 comments at least 200 characters long on topics and keywords assigned each day.[95] Some salaries were as high as $1,400 per week, according to another former employee who spoke with the *New York Times* in 2018. "They were just giving me money for writing," he said. "I was much younger and did not think about the moral side. I simply wrote because I loved writing. I was not trying to change the world."[96] By mid-2015, the staff had grown from a few dozen to over 1,000. It is a cost-effective means of reshaping the global social media landscape, without the need to necessarily recruit fully committed ideologues.[97]

Kremlin-backed media can, moreover, prove crucial during a political crisis. During and after the 2014 annexation of Crimea, Russian propaganda portrayed Ukraine's "Revolution of Dignity" as a willing ally of fascists who were undertaking an illegal coup. The narratives were many. For example, the revolution was likewise framed as a political operation by the West, as evidenced (according to *RT* and *Sputnik*) by American and European leaders' quick support after the ouster of Putin's proxy leader in Kyiv. Not all narratives were cooked up by Moscow. Some Western media outlets (and even think tanks) unwittingly advance the Kremlin's cause when they framed the popular revolt as a split between Ukraine's "pro-European" west and "pro-Russian" east. This ostensibly made it the *inevitable* product of linguistic, religious, or ethnic divisions. It was not.

Rapid Adaptation

Finally, Russia's information warfare techniques are highly adaptive. One recent development by the Kremlin is the deployment of cluster



Russian President Vladimir Putin. Photo Credit: kremlin.ru.

narratives. This is the bundling of multiple, even contradictory, arguments together. According to experimental research compiled by RAND, this "firehose" propaganda model is effective due to the variety, volume, and views of sources.[98] First, individuals are more likely to accept information when it is received through a *variety* of sources, despite ostensibly coming from different perspectives or different arguments which promote the same conclusions. Second, the persuasiveness of a message is more dependent on the *number* of arguments made than on their quality. Endorsements from large numbers of other readers (even bots) boosts an individual's trust in the information received. Third, views from propaganda sources are more persuasive when the recipient identifies with the source, whether in terms of ethnicity, language, nationality, ideology, or other factors. "Credibility can be social," RAND finds, as "people are more likely to perceive a source as credible if others" do too.[99]

Cluster narratives interact in complex ways. For instance, when the volume of information about a subject is high, people tend to favor views from other users in a social media ecosystem instead of experts (unlike when the volume is low). The variety and number of these generally untrustworthy sources has a significant bearing on their trust in the message received. Overall, however, it is clear that the greater the volume of propaganda, and the more sources available, the more effective Russian disinformation campaigns are at drowning out alternative messages and increasing the exposure and perceived credibility of their preferred narratives.[100]

Impact: Weaknesses

Information warfare has disadvantages as well. Russia's information strategy can backfire: efforts at sowing instability abroad can have a ricochet effect, generating instability that eventually affects Russia itself. In today's war

against Ukraine, Russia has taken the proactive measure of sealing its borders against returning fighters—lest they cause trouble at home.[101] And the interconnected nature of the modern information space makes it harder to achieve effects in a geographically targeted way, heightening Russia's own susceptibility to a "boomerang effect."

The Kremlin's information campaigns can have unintended consequences inside target countries. Take, for example, the United States. While the authors do not believe that Kremlin interference in the 2016 U.S. presidential election altered the final result in any way, the ensuing investigations, hearings, media, and public attention to this attack have placed Russian malign influence operations under unprecedented scrutiny. It is now harder for Russia to fly below the radar with disinformation operations. Its bot networks are easier to identify. Its trolls are easier to ignore. And social media companies are taking unprecedented steps to shut down both. Moreover, Russian observers have noted an increase in the appeal of "anti-Russian" political positions by leaders.[102] This is what blowback looks like.

A second weakness of disinformation is that it becomes inherently more escalatory with time. Subversive moves that are initially surreptitious become more recognizable with use. Since it is ultimately a part of war, it is hard to know when a disinformation campaign is a prelude to more kinetic operations. The preparations and counter-moves that it prompts on the part of a target can trigger tests of strength, the avoidance of which was the starting aim of the strategy.

Although Putin has escalated crises in order to escape them (see 'Chicago rules' earlier), he appears unwilling or politically unable to deescalate in a way that would not look like defeat. In this regard, the shadow of Mikhail

The United States Navy during a military training exercise. Photo Credit: U.S. Department of Defense.

Gorbachev's concessions to the West in the final phase of the Cold War looms large in Kremlin thinking. These are interpreted as signs of weakness to contemporary domestic Russian audiences. Putin also seems to have difficulty in deciding what exactly he wants, and what he can sustain as an end product of his policies (see Section 1—"International System").

"A third weakness of **disinformation operations** is that they are *hard to measure precisely*—and their **actual impact may be exaggerated.**"

A third weakness of disinformation operations is that they are hard to measure precisely—and their actual impact may be exaggerated. Evidence suggests that while Russian media narratives are disseminated broadly in the Middle East, outside of Syria their effect has been limited. The ability of regional authoritarian governments to control the information their societies receive, cross cutting political pressures, the lack of longstanding ethnic and cultural ties with Russia, and widespread doubts about Russian intentions make it difficult for Moscow to use information operations as an effective tool should it decide to maintain an enhanced permanent presence in the Middle East.[103]

Additionally, the audience for *RT* may be overstated by the Kremlin, deliberately obscuring the difference between "reach" and "audience." *RT* claims that it reaches 500-700 million viewers across 100 countries. In 2015, one assessment found that the figures reflected "just the theoretical geographical scope of the audience," not an actual read of *RT*'s real viewers.[104] *RT* and *Sputnik* combined are only watched by 2.8 percent of the residents in Moldova, 1.3 percent in Belarus, and 5.3 percent in Serbia (according to BBG data from June 2017).[105] In the United States, *RT America* has been forced to register as a foreign agent, which means that it must disclose financial information to the U.S. government.[106] *RT*'s UK channel has been reprimanded by telecom regulator OFCOM more than a dozen times for its skewed, false reporting.[107] The key point here: the official attention that *RT* receives may stand in contrast with its actual influence. In Britain, *RT*'s broadcast reach is limited, hovering around 413,000 viewers weekly, as compared to 4.4 million for *Sky News* and 7.3 million for *BBC News*.[108] In the U.S., despite programs made by well-known figures such as Larry King, *RT* is "largely absent" in the Nielsen rankings.

Working in *RT*'s favor is the fact that its social media presence is far more successful than its broadcasting arm. Despite high online

viewership on YouTube and other sites, however, 81 percent of views on *RT*'s top 100 most watched videos were for content relating to "natural disasters, accidents, crime and natural phenomena."[109] Its politics and current events videos received just one percent of its overall YouTube exposure.[110] Pushback from the U.S. government and corporations may have reduced Russia's online disinformation capabilities even further. In October 2017, Twitter decided it would no longer allow paid advertisements from *RT* and *Sputnik*. A month later, in an implicit attempt to "derank" *RT* and *Sputnik* from search results, Google's parent company Alphabet announced it had "adjusted [their] signals to help surface more authoritative pages and demote low-quality content."[111] Even when accounting for Russian propaganda's actual audience, as opposed to its potential reach, most viewers and readers naturally gravitate towards non-political content. Though the Kremlin's goal is to steer *RT*'s audience from such content toward Russian disinformation more broadly, there is little evidence that this strategy has had much success. Still, one compelling point is necessary to stress: the goal of Russian state media actors is not simply to boost ratings or compete one-to-one against traditional broadcasters. Rather, their purpose is to spread disinformation narratives favorable to the Kremlin. As these narratives and false facts "ping pong" between outlets, they are amplified through coordinated social media targeting and the blind fortune of the internet. Despite his considerable powers, Putin still cannot order that a meme "go viral."

Immunity

Lastly, it is important to recall that the diffused, uncoordinated, and self-regulating nature of social media sometimes has facilitated effective self-defense mechanisms. A new alertness to the prevalence of orchestrated troll campaigns has led to the dissemination of self-help guides for dealing with trolls. The growing availability of tools for detection of the less sophisticated troll and bot campaigns through technical and quantitative analysis is assisting in spreading awareness. As a result, according to one Russian assessment, despite the "billions of dollars" spent by the Russian state on attempting to "turn social networks into its obedient weapon...net society has developed immunity in some respects."[112]

> "Russia's use of disinformation ***erodes the trust that other countries or leaders*** might place in their relationship with *Russia and Putin personally.*"

Herein lies the fundamental weakness of the Prometheanism strategy. Since the effectiveness of any chaos strategy depends

Russian Victory Day Parade in Moscow in 2014. Photo Credit: kremlin.ru.

on surprise and uncertainty, Russia's use of disinformation erodes the trust that other countries or leaders might place in their relationship with Russia and Putin personally. The Kremlin has chosen to damage this trust. Russia has affirmed that its relations with other states are guided by zero-sum intimidation, not established rules, good faith treaties, or alliance structures. While these pillars of statecraft may have their own weaknesses, they evolved organically over time. They do not exist because the United States imposed them upon an unwilling world. Rather, they convey real and meaningful value to states which employ them in their relations with others. By undercutting international rules, treaties, and alliances, the Kremlin inadvertently eats away at its own standing in the world. Gerasimov failed to factor this crucial variable into his "doctrine." That failure is now imposing long-term costs on Russia's national interests.

SECTION 4—PROSPECTS: THE EVOLVING THREAT

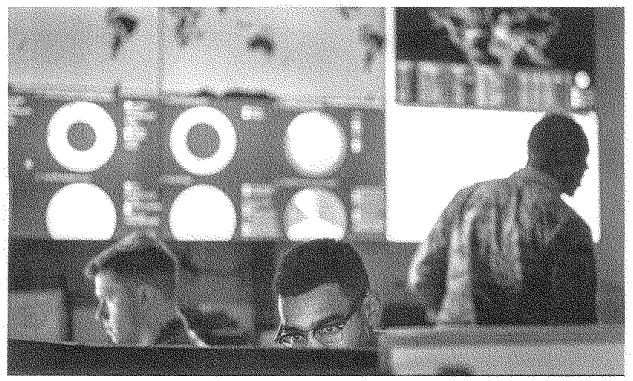
While the Kremlin's end goal is survival, its pursuit of chaos as a strategy has largely been a holding action. It has used Promethean methods to undermine the West and burnish its ambitions as a Great Power—only to buy time as it rebuilds its military and hardens domestic structures against bottom-up discontent. Despite its many risks and drawbacks, Prometheanism has nevertheless been effective for the Kremlin. Its reliance on this strategy has arguably improved the Kremlin's domestic position. Sadly, Moscow's confrontational approach to the West—at the political, economic, social, and propaganda levels—has become a permanent, strategic *leitmotiv* of Russia's foreign policy. It results from

the intrinsic nature of the Russian authoritarian regime, the mentality of its ruling elite, and the Kremlin's time worn way of looking at the outside world.[113] Prometheanism also rests upon a larger tradition of Russian strategic theory, not just that of Gerasimov. The concept of spreading chaos in the lands of others is a deeply rooted idea in Russian behavior. Thus far, Western responses to this activity have been largely weak and uncoordinated. This only encourages more Kremlin meddling. The openness and pluralism of Western societies also provides built-in opportunities for Russian exploitation and probing. These are unlikely to disappear.

On the plus side, the disinformation tools used by Moscow against the West remain fairly basic. They rely on exploiting human gullibility, known vulnerabilities in the social media ecosystem, and a lack of awareness among the public, the media, and policymakers. However, Russia's information warfare capability is not a static project. It is dynamic. It is constantly developing new approaches not yet reflected in mainstream reporting or popular awareness. And it is adaptable to changing political landscapes and technological advancements. This should keep Western states in a heightened state of readiness and awareness. In the very near term, technological advancements in artificial intelligence and cyber capabilities will open opportunities for malicious actors to undermine democracies more covertly and effectively than what we have seen to date.[114]

FINDINGS AND RECOMMENDATIONS

Too much of the West's recent attention to Russia has been dedicated to granular considerations of the "whom" and "how" of Kremlin techniques for creating disorder and



Cyber warfare operators with the Maryland Air National Guard. Photo Credit: U.S. Department of Defense.

distraction. We now know how Moscow makes use of Russian-language and foreign-language media outlets and social media networks to sow doubt about Western security structures like NATO. We also understand now how Russia's military doctrine has incorporated "information confrontation" into its methods of warfare. Thanks to multiple analyses of Gerasimov's writings on the use of "indirect and asymmetric methods" for defeating an enemy, our awareness of Moscow's nonlinear methods for manipulating information and political systems is expanding. The threat is not primarily a journalistic or cyber one, as it is often portrayed. It is an issue of national security.

The problem is that Western states are still perpetually playing defense against Russia's latest toxic narrative or remarkable cyber operation. All too often, they are surprised by the Kremlin's next moves. More work must be devoted to fitting these necessary pieces into a holistic framework that includes the "what for" and "what's next" of Russia's efforts.

Part of the problem is our misunderstanding of Russia's strategic behavior in the first place. Prior to the annexation of Crimea in 2014, Russia was generally viewed as a weak actor with declining power in the global arena. Mired in economic crises, social problems, and plummeting population growth, Moscow's ambition of achieving regional hegemony and global influence seemed to be things of the past. As far as Western leaders were concerned, Russia did not have the wherewithal to support a military or geostrategic rivalry. Western relations with Russia were subsequently premised on assumptions of "win-win" outcomes rather than on zero-sum calculations of "us-versus-them." These assumptions have now been shattered. From its incursions into Georgia and Ukraine to its bending or breaking of treaties (among them the Treaty on Conventional Armed Forces in Europe and the Helsinki Final Act) to its militarization of the Black Sea and Kaliningrad exclave, Russia has ramped up its hostility to the existing Euro-Atlantic security order. In the process, it has also demonstrated that even a weakened competitor can be highly disruptive.

To counteract Russia's behavior, the West must understand the Kremlin's use of information warfare as an example of a chaos strategy in action, and not over-focus on social media and IT-heavy analysis. Dangers that we can see are easier to admire than those that we do not understand. In particular, Western analysts must consider how the concept of a bloodless disordering of the far frontier has figured in past Russian political-military strategy. Using both historical and contemporary assessments of Russian thinking, they can improve the West's own competitive strategies.

Indeed, the Kremlin's chaos-seeding strategy shows us what its leaders fear: Western power. To date the West has not fully considered how its power can be brought to bear against the Kremlin's vulnerabilities. Every strategy has a weakness—even chaos. There are disadvantages as well as advantages to our instantaneous modern communications: the interconnected nature of the modern information space makes it harder to achieve effects in a geographically targeted way, heightening Russia's own susceptibility to a "boomerang effect." What unintended consequences are beginning to occur as a result of its chaos strategy? How aware are Russian leaders of these problems and how willing are they to address them? How vulnerable are they to blowback? Where is the Russian regime weakest? These are questions

that Western policymakers must now answer. Unfortunately, too many policymakers interviewed for this study—especially in NATO and the EU—preferred not to do so, claiming that their organizations "do not engage in offensive operations." At a minimum, this ties our hands at a conceptual level when assessing counter-strategies—it limits our *options*. As this paper also has shown, the Kremlin's view of information warfare sees little difference between offensive and defensive operations. We can and should learn from this behavior.

The stakes are high: Russia's chaos strategy has a potentially far-reaching impact on bilateral relations and on the efficacy of our treaties and agreements with Russia (old and new). It may increase the risk of unwanted military escalation and threaten the future stability of frontline states in the CEE region. It should also prompt caution about the prospects for future agreements with Russia on Ukraine, Syria, North Korea, and nuclear arms control.

In light of these risks, U.S. policy must remove the predictable and permissive conditions that enable a chaos strategy in the first place. Kremlin leaders must worry about our next moves, not the other way around. Second, policy must conceive of and work toward a sustainable end state in which Russia returns to "normal" strategic behavior patterns. Here are four key actions that policymakers can take if they are to accomplish both goals:

- First, realize that Russia sees the international system very differently than we do, even though our interests on specific issues may coincide (for example, counter-terrorism).
- Second, approach our dealings with Moscow with the understanding that its use of terms like "international law" and state "sovereignty" is primarily instrumental. Kremlin leaders evoke these concepts for *ad hoc* advantage—not as ends in themselves.
- Third, understand that Russia's use of information warfare has a purpose: reflexive control. (Such control is achieved by subtly convincing Russia's opponents that they are acting in their own interests, when in fact they are following Moscow's playbook.)[115]
- Fourth, prioritize the sequencing of the "carrots and sticks" offered to the Kremlin. Sticks first. This means initially increasing the penalties imposed on Russia for continued revisionist behavior and the sowing of chaos. We can start with tougher sanctions, wider travel bans, greater restrictions on access to the global

> *"U.S. policy must remove the* **predictable and permissive conditions** *that enable a chaos strategy in the first place."*

financial system, and financial snap exercises. Presently, some of these tools are used—but they are underutilized in most cases. This needs to change.

Particularly in the domain of information warfare, the West must hit back harder. Although the EU's East StratCom, NATO's StratCom, and the newly established national StratComs in Europe can be effective tools, they still lack resources, coherence, and full coordination to stop Russia's malicious activities. We are in a technological contest with Russia. We should aim to win it. The Western response must be superior in impact and sophistication. Russia relies on harnessing bursts of "sharp power" to succeed. The West must set as a collective goal its intention to outmaneuver, outplay, and contain the damage of Russia's strategy with our overwhelming diplomatic, informational, military, and economic power. This response must be both public and private, and include the government, media outlets, the tech and private sectors, and civil society. Experience shows that an independent message is more credible and effective, and people are ultimately more receptive when these messages come from non-state actors. Investing more in these non-state domains holds a great deal of untapped potential in the West. Finally, these measures must all go hand-in-hand with coordinated economic sanctions and be backed up with Western military power.[116]

Unfortunately, we in the West—particularly in the United States—have been too predictable, too linear. We would do well to consider ourselves the underdog in this contest and push back in nonlinear ways. Perhaps the only thing that Kremlin leaders fear more than Western power is the rejection of their rule by Russia's own people. While our final goal should be to ensure that Moscow becomes a constructive member of the Euro-Atlantic security community, our responses for now should serve the shorter-term goal of forcing Russia to play more defense and less offense against the West. For this purpose, we should lessen our preoccupation with "provoking" the Kremlin. It is hardly a basis of sound policy to prioritize Putin's peace of mind. The Russian government will work with the West if that path suits its goals. Otherwise, it will not. We should do the same.

Appendix I

RUSSIA'S WORLD VIEW

Russia's view of the international system includes several core tenets:

- The primacy of hard power. Military strength and "strategic nuclear parity" represent the ultimate guarantee of the world's attention to and respect for Moscow.
- The dominance of major powers in the international system—most obviously the U.S., Russia, and China. Only they act truly independently. Smaller states and multilateral organizations are seen as objects or instruments of Great Power diplomacy rather than serious actors with proper agendas.
- The multipolarity of the international system. This interpretation, first promoted by Foreign Minister Yevgenii Primakov in the 1990s, is one of a world dominated by the interaction between different Great Powers, where no single major actor is allowed to threaten the status quo and act unilaterally without risking reciprocal action.
- Under Putin, multipolarity has been given a civilizational aspect that contradicts Western ideas of moral universalism. Russia's 2013 Foreign Policy Concept presupposes "global competition...on a civilizational level, whereby various values and models of development based on the universal principles of democracy and market economy start to clash and compete with each other."[117] Russia thus presents itself as a normative alternative to the West, with the potential to attract authoritarian elites worldwide.[118]

Appendix II

KREMLIN LESSONS LEARNED

Three events—Russia's war with Georgia in 2008, the invasion of Ukraine in 2014, and intervention in Syria a year later—as well the Obama Administration's failed "Reset" have provided Russia with vital lessons in how to conduct its foreign policy:

- The international community can be slow to respond to surprise military action;
- hybrid warfare can be more effective than conventional operations;
- information operations also can be successful;
- international diplomatic processes can easily be derailed or manipulated; and
- reliance on chaos as a strategy can contribute to the removal of hostile governments.

Russian leaders have implemented these lessons by turning the West's democratic norms and institutions against themselves, opening wider existing fault lines, and taking every opportunity to neutralize the United States and its allies. This approach is what George Kennan called political war: "The employment of all the means at a nation's command, short of war—to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures...and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."[119]

Russia has applied these lessons in a variety of areas:[120]

- In the **Western Balkans**, Russia is actively trying to hinder NATO enlargement. Although Montenegro's accession could not be prevented, Russia is attempting to portray the actions of the EU and the United States as a failed project and maintain a global superpower image through manipulation of its historical ties in the region.
- In **Libya**, Moscow's broader goal is to obtain a new ally on NATO's southern border, whose influence could be used against the Alliance and the West. Russia has actively supported the Libyan National Army led by General Khalifa Haftar, a force opposing the UN-supported Libyan unity government. Alongside trying to bolster his political legitimacy, Russia supports Haftar also in other ways. For example, it has repeatedly taken on the printing of Libyan dinars, which are delivered to the cash-poor territories controlled by Haftar. Russia also maintains ties with the Libyan unity government, which understands that Russia is equally capable of escalating the conflict as it is of defusing it.

Chaos as a Strategy, 39

Appendix II

KREMLIN LESSONS LEARNED

- In the **Persian Gulf**, Russia is trying to undermine the U.S.-led regional security architecture. To do so, Russia is trying to benefit from the frictions between the U.S. and its Arab allies concerning, above all, Iran's role in the region. Russia has courted the monarchies around the Gulf both economically and politically. It is also preparing arms sale transactions with both Saudi Arabia and Qatar. In the same way, Russia has also repeatedly passed itself off as a so-called neutral peace broker in Yemen's civil war. With these steps, Russia tries to undermine the U.S.' regional role and simultaneously transform itself into an indispensable negotiation partner in the Middle East.

- In **Syria**, the Russian narrative trumpets an ongoing fight against terrorism, but the reality is that Russia became involved there to halt a string of defeats for the Bashar al-Assad regime while trying to increase its presence and possibilities to influence developments in the region. In this sense, Russia's intervention in Syria since 2015 has been successful. Although Iran's influence in Syria has grown significantly as a result of the conflict, Moscow has managed to reinforce its own military presence in Syria. In addition, Russia has succeeded in breaking out of the diplomatic isolation imposed on it due to the Ukraine conflict, and achieved a situation where, at least on the Syrian issue, Russia can act as an equal counterpart alongside the leading powers and regional forces.

- In **North Korea**, Russia's ambition is clear: to become an internationally recognized global actor and to undermine the role of the U.S. at the same time. Russia is exploiting the conflict to spread a narrative that the U.S. is principally to blame in the North Korea question. It volunteers itself as a "peace dove" which prefers diplomatic channels and could possibly broker talks.

- In **Afghanistan**, Russia is using counterterrorism rhetoric to justify its activities. Russia is increasing its troop presence under the guise that the U.S.-led coalition is failing in its fight against drug trade and terrorism. Russia maintains contacts with the major parties to the Afghanistan conflict in order to keep its options open for any future scenario.

Appendix III

KREMLIN DISINFORMATION TECHNIQUES[121]

Disinformation and new propaganda can take many forms—from the use of false visuals or misleading headlines, to social media techniques that create an impression that the "majority" understands an issue in a certain way. In the echo chamber of the modern information space, the spreading of disinformation is as easy as a "like," "tweet," or a "share." The following are some of the Kremlin's most commonly used techniques for spreading false stories and disinformation:

- Ping pong: The coordinated use of complementary websites to springboard a story into mainstream circulation.
- Wolf cries wolf: The vilification of an individual or institution for something you also do.
- Misleading title: Facts or statements in the article are correct, or mostly correct, but the title is misleading.
- No proof: Facts or statements that are not backed up with proof or sources.
- Card stacking: Facts or statements are partially true. This occurs when information is correct, but it is offered selectively, or key facts are omitted. The Kremlin typically uses this technique to guide audiences to a conclusion that fits into a pre-fabricated or false narrative.
- False fact: Facts or statements are false. For example, an interview mentioned in an article that never took place or an event or incident featured in a news story that did not actually occur.
- False visuals: A variant of false facts, this technique employs the use of fake or manipulated provocative visual material. Its purpose is to lend extra credibility to a false fact or narrative.
- Denying facts: A variant of "false facts," this occurs when real facts are denied or wrongly undermined. The facts of an event might be reported, but an attempt is made to discredit their veracity. Alternatively, the facts may be re-interpreted to achieve the same effect: to establish doubt among an audience over the validity of a story or narrative.

Appendix III

- Exaggeration and over-generalization: This method dramatizes. raises false alarms or uses a particular premise to shape a conclusion. A related technique is *totum pro parte*.
- *Totum pro parte*: The "whole for a part." An example: portraying the views of a single journalist or expert as the official view or position of a government.
- Changing the quotation, source, or context: Facts and statements are reported from other sources, but they are now different than the original or do not account for the latest editorial changes. For example, a quotation is correct, but the person to whom it is attributed has changed, or a quote's context is altered so as to change its meaning or significance in the original story.
- Loaded words or metaphors: Using expressions and metaphors to support a false narrative or hide a true one; for example, using a term like "mysterious death" instead of "poisoning" or "murder" to describe the facts of a story.
- Ridiculing, discrediting, diminution: Marginalizing facts, statements, or people through mockery, name-calling (i.e. *argumentum ad hominem*), or by undermining their authority. This includes using traditional and new media humor, in order to discredit on non-substantive merits.
- Whataboutism: Using false comparisons to support a pre-fabricated narrative or justify deeds and policies; i.e., "We may be bad, but others are just as bad" or "The annexation of Crimea was just like the invasion of Iraq." This technique is often accompanied by an *ad hominem* attack.
- Narrative laundering: Concealing and cleaning the provenance of a source or claim. When a so-called expert of dubious integrity presents false facts or narratives as the truth. Often, this happens when propaganda outlets mimic the format of mainstream media. A common technique is to feature a guest "expert" or "scholar" on a TV program whose false fact or narrative can then be repackaged for wider distribution. For example, "Austrian media writes that..." or "A well-known German political expert says that..."
- Exploiting balance: This happens when otherwise mainstream media outlets try to "balance" their reporting by featuring professional propagandists or faux journalists and experts. The effect is to inject an otherwise legitimate news story or debate with false facts and narratives. This technique is common in televised formats, which feature point-counterpoint debates. Propagandists subsequently hijack a good-faith exchange of opposing views.

Appendix III

- Presenting opinion as facts (and vice-versa): An opinion is presented as a fact in order to advance or discredit a narrative.
- Conspiracy theories: Employing rumors, myths, or claims of conspiracy to distract or dismay an audience. Examples include: "NATO wants to invade Russia," "The United States created the Zika virus," "Secret Baltic agencies are infecting Russian computers with viruses," or "Latvia wants to send its Russian population to concentration camps." A variation of this technique is conspiracy in reverse—or attempting to discredit a factual news story by labeling it a conspiracy.
- Joining the bandwagon: Creating the impression that the "majority" prefers or understands an issue in a certain way. The majority's presumed wisdom lends credence to a conclusion or false narrative; e.g., "People are asking...," "People want...," or "People know best."
- False dilemma: Forcing audiences into a false binary choice, typically "us" vs. "them."
- Drowning facts with emotion: A form of the "appeal to emotion" fallacy, this is when a story is presented in such an emotional way that facts lose their importance. An example is the "Lisa case," in which Muslim immigrants in Germany were falsely reported to have sexually assaulted a Russian girl. While the event was entirely fabricated, its appeal to emotion distracted audiences from the absence of facts. Common variants of this method evoke post-Soviet nostalgia across Central and Eastern Europe, or stoke public fear of nuclear war.
- Creating the context: Most commonly found on broadcast news programs, it creates the context for a pre-fabricated narrative by preceding and following a news story in such a way that it changes the meaning of the news itself. For example, in order to send the message that recent terrorist attacks in Europe were the result of EU member states not working with Russia—which is helping to fight ISIS in Syria—commentary broadcast before the news on the March 2016 Brussels attacks described Russia's success in Syria and its ability to fight ISIS effectively.

Endnotes

1 Maria Snegovaya, "Reviving the Propaganda State: How the Kremlin Hijacked History to Survive," *Center for European Policy Analysis*, January 2018, https://cepa.ecms.pl/files/?id_plik=4824. "Global Trends: Paradox of Progress: Russia and Eurasia," *Office of the Director of National Intelligence*, January 2017, https://www.dni.gov/index.php/the-next-five-years/russia-and-eurasia.

2 For narratives, see: "The Kremlin's 'Besieged Fortress' Narrative Criticised in Independent Media," *European External Action Service East Stratcom Task Force*, March 4, 2018, https://euvsdisinfo.eu/the-kremlins-besieged-fortress-narrative-criticised-in-independent-media/.

3 For workforce decline, see: Tom Balmforth, "Another Worrying Sign for Russia's Dire Demographics," *Radio Free Europe / Radio Liberty*, September 27, 2017, https://www.rferl.org/a/russia-population-decline-labor-oreshkin/28760413.html.
For country population and urban projections, see: "World Urbanization Prospects: The 2018 Revision, Country Profiles: Russian Federation," *United Nations Department of Economic and Social Affairs*, Population Division, 2018, https://population.un.org/wup/Country-Profiles/.
For birthrate decline see: "Russia's Birthrate Drops By 10.7 Percent In 2017," *Radio Free Europe / Radio Liberty*, January 29, 2018, https://www.rferl.org/a/russia-birthrate-drops-2017/29005373.html.

4 "World Population Prospects, Data Booklet," *United Nations*, 2017, https://population.un.org/wpp/Publications/Files/WPP2017_DataBooklet.pdf. See also: "Global Trends: Paradox of Progress: Russia and Eurasia."

5 Michael Ross, "The Natural Resource Curse: How Wealth Can Make You Poor," Natural Resources and Violent Conflict: Options and Actions, *World Bank*, 2003.

6 Nienke Oomes and Katerina Kalcheva, "Diagnosing Dutch Disease: Does Russia Have the Symptoms?," *International Monetary Fund*, April 2007, https://www.imf.org/external/pubs/ft/wp/2007/wp07102.pdf. See also: Nienke Oomes and Olga Ponamorenko, "The Price of Oil Dependency: Dutch Disease in Russian Regions," *SEO Amsterdam Economics*, December 2015, http://www.seo.nl/uploads/media/DP83_The_Price_of_Oil_Dependency__Dutch_Disease_in_Russian_Regions.pdf.

7 "The Putin Era in Historical Perspective," *National Intelligence Council*, February 2007.
See also: Maria Domańska, "Conflict-dependent Russia: The domestic determinants of the Kremlin's anti-western policy," *Centre for Eastern Studies (OSW)*, August 2018, https://www.osw.waw.pl/en/publikacje/point-view/2017-11-06/conflict-dependent-russia-domestic-determinants-kremlins-anti.

8 Snegovaya. See also: Mikhail Zygar, "Burevestnik cvetnyh revoljucij: Džordž Buš sozdaet special'nyj korpus podderžki novyh demokratij," *Kommersant*, May 20, 2005, https://www.kommersant.ru/doc/579095.

9 "Vladimir Putin Took Part in the Plenary Meeting of the 70th Session of the UN General Assembly in New York," *Kremlin*, September 28, 2015, http://en.kremlin.ru/events/president/news/50385.

10 Jakob Hedenskog, Tomas Malmlöf, Johan Norberg, Susanne Oxenstierna, Carolina Vendil Pallin, Gudrun Persson, Roger Roffey, and Fredrik Westerlund, "Russian Military Capability in a Ten-Year Perspective 2016," *FOI*, December 8, 2016, https://www.foi.se/report-search/pdf?fileName...7fca-451e-bdd6-d0ce7107c38a.pdf, 117-21.

11 *Ibid.*, 114-115.

12 Mark Galeotti, "Russia pursues 'dark power' and the West has no answer," *Raamop Rusland*, March 15, 2018, https://raamoprusland.nl/dossiers/kremlin/894-russia-pursues-dark-power-in-the-skripal-case.

13 Hedenskog et al., 114.

14 Andrey Bezrukov and Andrey Sushentsov, "Contours of an Alarming Future," *Russia in Global Affairs*, September 21, 2015, http://eng.globalaffairs.ru/number/Contours-of-an-Alarming-Future-17693.

15 Sergey Lavrov, "Historical Perspective of Russia's Foreign Policy," *Russia in Global Affairs*, December 8, 2017, http://www.globalaffairs.ru/number/Istoricheskaya-perspektiva-vneshnei-politiki-Rossii-19208; Fyodor Lukyanov, "After Crimea. What Will The New Global World Order Be?," Lenta.ru, June 1, 2016, https://lenta.ru/articles/2016/06/01/after_crimea/.

16 Dmitry Trenin, "Mitigation of the Conflict in a Hybrid war," *Moscow Center Carnegie*, January 25, 2018, http://carnegie.ru/2018/01/25/ru-pub-75296.

17 "The Concept Of Foreign Policy Of The Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016)," *MFA Russia*, December 1, 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248.

18 Fyodor Lukyanov, "Back to Realism: The US Defense Strategy Reflects The Worldview Of Modern Times," *Russia in Global Affairs*, January 24, 2018, http://www.globalaffairs.ru/redcol/Nazad-k-realizmu-19310.

19 Fyodor Lukyanov, "Putin's Foreign Policy: The Quest to Restore Russia's Rightful Place," *Foreign Affairs*, April 18, 2016, https://www.foreignaffairs.com/articles/russia-fsu/2016-04-18/putins-foreign-policy.

20 *Ibid.*

21 Trenin.

22 Nikolay Silaev and Andrei Sushentsov, "Allies of Russia and the Geopolitical Frontier in Eurasia," *Russia in Global Affairs*, June 4, 2017, http://www.globalaffairs.ru/number/Soyuzniki-Rossii-i-geopoliticheskii-frontir-v-Evrazii-18811.

23 Sergey Karaganov, "Russia's Desperation Has Saddled a Wave of History," *Russia in Global Affairs*, December 5, 2017, http://www.globalaffairs.ru/pubcol/Russkaya-otchayannost-osedlala-volnu-istorii-19180.

24 Emphasis by authors. Karaganov, "Russia's Desperation."

25 Stephen H. Kellert, *In the Wake of Chaos: Unpredictable Order in Dynamical Systems*, (Chicago: University of Chicago, 1993), 2.

26 Scott E. Womack, *Chaos, Clausewitz, and Combat: A Critical Analysis of Operational Planning in the Vietnam War, 1966-1971*, (Fort Belvoir, VA: Defense Technical Information Center, Document Number ADA306112), 168.

27 P.H. Liotta, "Chaos as Strategy," *Parameters*, Summer 2002, https://ssi.armywarcollege.edu/pubs/Parameters/articles/02summer/liotta.htm, 47-56.

28 *Ibid.*, 56.

29 Sun Tzu, *The Art of War*, trans. Ralph D. Sawyer, (New York: Barnes and Nobles, New York, 1994), 191.

30 Holger Mölder, Kristiina Müür, and Vladimir Sazonov, eds., "Russian Information Campaign against the Ukrainian State and Defence Forces," *North Atlantic Treaty Organization*, Strategic Communications Centre of Excellence, 2016, https://www.stratcomcoe.org/russian-information-campaign-against-ukrainian-state-and-defence-forces.

31 Frans P. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, (London: Routledge, 2007), 59.

32 Tzu, 191.

33 Osinga, 59.

34 *Ibid.*, 60.

35 Tzu, 224.

36 Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, trans., (Princeton: Princeton University Press, 1976), 87.

37 *Ibid.*

38 Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* 17 (Winter 1992-1993), https://www.fd.unl.pt/docentes_docs/ma/aens_MA_20002.pdf.

39 Clausewitz, 139.

40 German strategist Karl Ernst Haushofer deserves recognition as an additional, later contributor.

41 For example, the Arab Revolt during World War I was a specific chaos strategy executed by the United Kingdom. against Turkey. It is not, however, the type of "Promethean" strategy considered by the authors in this report.

42 "How Germany Got the Russian Revolution off the Ground," *Deutsche Welle*, November 7, 2017, https://www.dw.com/en/media-center/podcasts/s-100977.

43 George Schmid, *Between Ideology and Realpolitik: Woodrow Wilson and the Russian Revolution, 1917-1921*, (Westport, CT: Greenwood Press), 45.

44 See: David Kirby, "Morality or Expediency? The Baltic Question in British-Soviet Relations 1941-1942," in *The Baltic States on Peace and War 1917-1945*, V. Stanley Vardys and Romuald Misiūnas, eds., (University Park: The Pennsylvania State University Press, 1978), 72.

45 Valeriy Gerasimov, "Noviye vyzovy trebuyut pereosmysleniya form i sposobov vedeniya boevykh deistviy," *Voenno-promyshlenniy kur'er*, May 3, 2013, http://vpknews.ru/sites/default/files/pdf/VPK_08_476.pdf.

46 Molly K. Mckew, "The Gerasimov Doctrine," *Politico*, September 5, 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

47 *Ibid.*

48 Bettina Renz, "Russia and 'hybrid warfare'," *Contemporary Politics* 22 (2016), DOI: 10.1080/13569775.2016.1201316, 283-30.

49 Charles K. Bartles, "Getting Gerasimov Right," *Military Review*, January-February 2016, https://www.armyupress.army.mil/Portals/7/militaryreview/Archives/English/MilitaryReview_20160228_art009.pdf.

50 Victor R. Morris, "Grading Gerasimov: Evaluating Russian Nonlinear War through Modern Chinese Doctrine," *Small Wars Journal*, September 17, 2015, http://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine.

51 Mölder, *et al.*, 2016, 113.

52 Morris.

53 N. Inkster, "Information Warfare and the US Presidential Election," *Survival* 58, (2016): 23-32, doi:10.1080/00396338.2016.1231527.

54 Hedenskog *et al.*, 111.

55 Gerasimov.

56 Bettina Renz and Hanna Smith, "Russia and Hybrid Warfare – Going beyond the Label," *Aleksanteri Papers*, 2016, https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf?sequence=1&isAllowed=y.

57 Can Kasapoglu, "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control," *NATO Defense College*, November 25, 2015, http://www.ndc.nato.int/news/news.php?icode=877.

58 Christopher S. Chivvis, "Understanding Russian 'Hybrid Warfare' And What Can Be Done About It," *RAND Corporation*, March 22, 2017, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

59 *Ibid.*

60 Mölder *et al.*, 56.

61 *Ibid.*, 58.

62 Chivvis. Gerasimov. See generally, Donald N. Jensen, "Moscow in the Donbas: Command, Control, Crime and the Minsk Peace Process," *NATO Defense College*, March 24, 2017, http://www.ndc.nato.int/news/news.php?icode=1029.

63 *Ibid.*, Jensen.

64 Evgeny Finkel, "The Conflict in the Donbas between Gray and Black: The Importance of Perspective," *START*, December 2016, https://nsiteam.com/social/wp-content/uploads/2017/01/Ukraine-Qualitative-Case-Study-FINAL.pdf, 12.

65 Mark Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine,'" *Foreign Policy*, March 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

66 *Ibid.*

67 Galeotti, "Russia pursues 'Dark power.'"

68 "International Security and Estonia 2018," *Estonian Foreign Intelligence Service*, 2018, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf, 24.

69 "The Future of War: The New Battlegrounds," *The Economist*, January 27, 2018, https://www.economist.com/special-report/2018/01/25/the-future-of-war.

70 Galeotti, "Russia pursues 'Dark power.'"

71 Dmitry Trenin, "Mitigation of the Conflict in a Hybrid war," *Moscow Center Carnegie*, January 25, 2018, http://carnegie.ru/2018/01/25/ru-pub-75296.

72 "Russian Military Capability," 114-15.

73 The authors thank David Mamet for his contribution to geopolitics via "The Untouchables."

74 Galeotti, "Russia pursues 'Dark Power.'"

75 Todd C. Helmus, et al., "Russian Social Media Influence: Understanding Russian Propaganda In Eastern Europe," *RAND Corporation*, 2018, https://www.rand.org/pubs/research_reports/RR2237.html.

76 McKew.

77 For more, see, Donald N. Jensen, "Russia's Disinformation Offensive," Ilan Berman, ed., *Digital Dictators: Media, Authoritarianism, and America's New Challenge* (Lanham, MD: Rowman & Littlefield Publishing).

78 Herb Lin, "Developing Responses to Cyber-Enabled Information Warfare and Influence Operations," *Lawfare*, September 6, 2018, https://www.lawfareblog.com/developing-responses-cyber-enabled-information-warfare-and-influence-operations.

79 "Doctrine of Information Security of the Russian Federation, (December 2016)," *Ministry of Foreign Affairs of the Russian Federation*, December 5, 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

80 "Foreign intelligence chief says current ideological standoff worse than Cold War era," *TASS*, April 27, 2017, http://tass.com/politics/943501.

81 Natalya Kovaleva, "Russian Information Space, Russian Scholarship, and Kremlin Controls," *Counterdisinfo*, July 24, 2018, https://counterdisinfo.org/natalya-kovaleva-russian-information-space-russian-scholarship-and-kremlin-controls/.

82 Anna Oshkalo, "Top 10 Russia's Media in 2014," *Russian Search Tips*, January 14, 2015, https://www.russiansearchtips.com/2015/01/top-10-russias-largest-media-2014/.

83 Edward Lucas, "Winning the Information War Redux," *Center for European Policy Analysis*, April 24, 2017, https://www.cepa.org/infowar-redux.
See also, Jill Dougherty, "How the Media Became One of Putin's Most Powerful Weapons," *The Atlantic*, April 21, 2015, https://www.theatlantic.com/international/archive/2015/04/how-the-media-became-putins-most-powerful-weapon/391062/.

84 Donald N. Jensen, "Russia in the Middle East: A New Front in the Information War?," *Jamestown Foundation*, December 20, 2017, https://jamestown.org/program/russia-middle-east-new-front-information/.

85 Keir Giles, "Russia's 'New' Tools for Confronting the West," *Chatham House*, March 2016, 27-28, https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf.

86 *Ibid.*

87 Jim Rutenberg, "RT, Sputnik and Russia's New Theory of War," *New York Times*, September 13, 2017, https://www.nytimes.com/2017/09/13/magazine/rt-sputnik-and-russias-new-theory-of-war.html.

88 "Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security," *Minority Staff Report Prepared for the Use of the Committee On Foreign Relations United States Senate*, 42.

89 Giles, 44-45.

90 *Ibid.*, 46.

91 Spencer P. Boyer and Alina Polyakova, "The Future of Political Warfare: Russia, the West, and the Future of Global Digital Competition," *Brookings*, March 2018, https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf.

92 *Ibid.*

93 Simon Shuster, "How Russian Voters Fueled the Rise of Germany's Far-Right," *Time*, September 25, 2017, http://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/.

94 Donald N. Jensen, "The Italian Elections Open the Door toward Russia Wider," *Center for European Policy Analysis*, March 20, 2018, http://infowar.cepa.org/EN/Italian-elections-open-the-door-toward-Russia-wider.

95 "One Professional Troll Tells All," *Radio Free Europe / Radio Liberty*, March 25, 2015, https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html.

96 Neil MacFarquhar, "Inside the Russian Troll Factory: Zombies and a Breakneck Pace," *New York Times*, February 18, 2017, https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html.

97 "One Professional Troll Tells All."

98 Christopher Paul and Miriam Mathews, "The Russian 'Firehose of Falsehood' Propaganda Model," *RAND Corporation Perspective*, 2016, https://www.rand.org/pubs/perspectives/PE198.html.

99 *Ibid.*

100 *Ibid.*

101 Jensen, "Moscow in the Donbas."

102 Liliya Shevtsova, "Vlyapalis'," *Ekho Moskvy*, August 14, 2018, https://echo.msk.ru/blog/shevtsova/2258916-echo/.

103 Jensen, "Russia in the Middle East: A New Front in the Information War?."

104 Katie Zavadski, "Putin's Propaganda TV Lies about its Popularity," *The Daily Beast*, September 17, 2015, https://www.thedailybeast.com/putins-propaganda-tv-lies-about-its-popularity.

105 "Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security," 41.

106 Ginger Gleason and Jack Stubbs, "Russia's RT America Registers as 'Foreign Agent' in U.S.," *Reuters*, November 13, 2017, https://www.reuters.com/article/us-russia-usa-media-restrictions-rt/russias-rt-america-registers-as-foreign-agent-in-u-s-idUSKBN1DD25B.

107 Holly Watt, "Ofcom Investigates Alex Salmond's TV Show on Kremlin-Backed Channel," *Guardian*, December 1, 2017, https://www.theguardian.com/world/2017/dec/18/ofcom-investigates-alex-salmonds-tv-show-kremlin-backed-network.

108 Tim Dowling, "24-hour Putin people: my week watching Kremlin 'propaganda channel' RT," *Guardian*, November 29, 2017, https://www.theguardian.com/media/2017/nov/29/24-hour-putin-people-my-week-watching-kremlin-propaganda-channel-rt-russia-today.

109 Zavadski.

110 *Ibid.*

111 "Putin's Asymmetric Assault On Democracy In Russia And Europe: Implications For U.S. National Security," 43.

112 Giles, 46.

113 Domańska.

114 Alina Polyakova, "The Next Russian Attack Will be Far Worse than Bots and Trolls," *Brookings*, March 22, 2018, https://www.brookings.edu/blog/order-from-chaos/2018/03/22/the-next-russian-attack-will-be-far-worse-than-bots-and-trolls.

115 Annie Kowalewski, "Disinformation and Reflexive Control: The New Cold War," *Georgetown Security Studies Review*, February 1, 2017, http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/.

116 Miro Smith, "Standing Up to Russia's Sharp Power," *Foreign Policy Research Institute*, September 12, 2018, https://www.fpri.org/article/2018/09/standing-up-to-russias-sharp-power/.

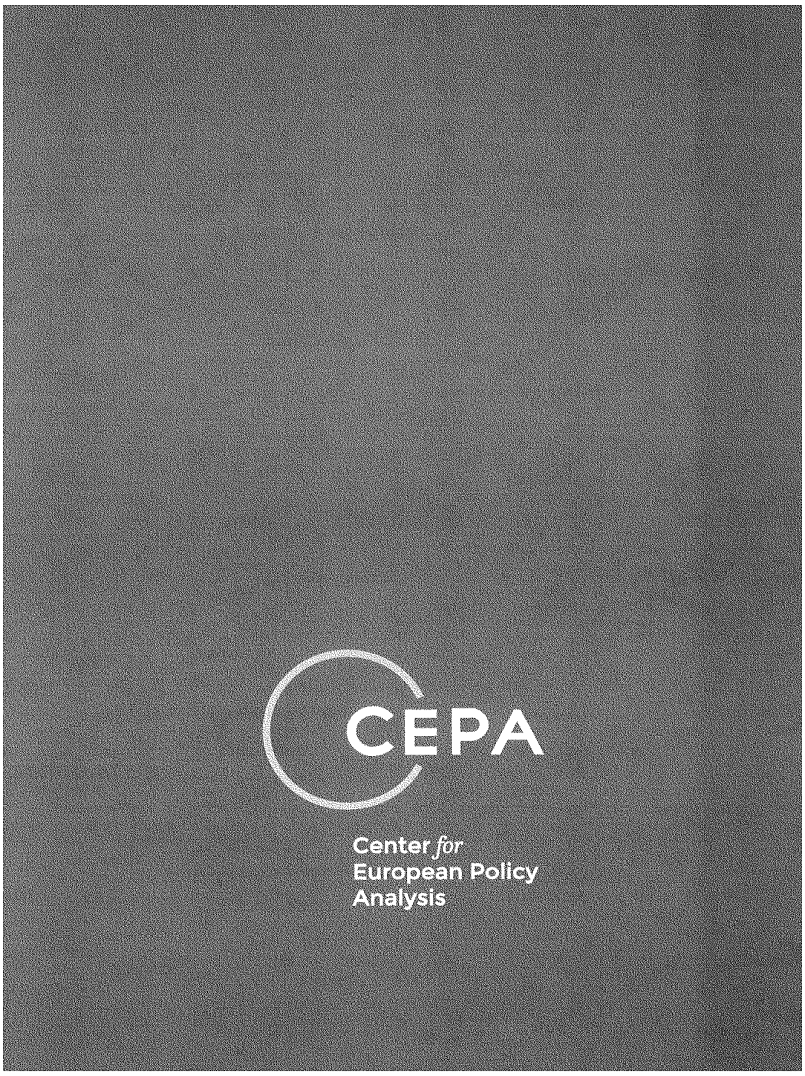
117 Hedenskog *et al.*, 115-16. For more see, Bobo Lo, *Russia and the New World Disorder*, (London: Chatham House), 2015.

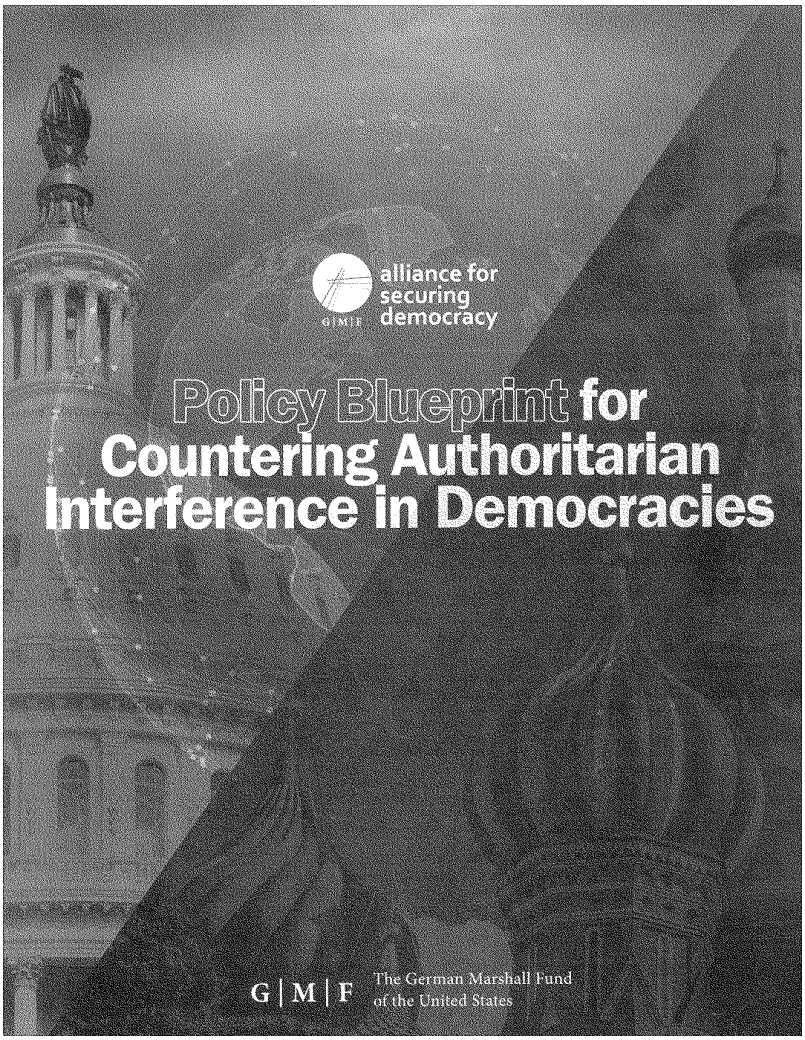
118 *Ibid.*, Hedenskog.

119 Mark Galeotti, "I'm Sorry for Creating the "Gerasimov Doctrine."
"Policy Planning Staff Memorandum," *National Archives and Records Administration*, May 4, 1948, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

120 "International Security and Estonia 2018," 24.

121 "Techniques," *Center for European Policy Analysis*, http://infowar.cepa.org/Techniques.


CEPA
Center for
European Policy
Analysis


alliance for
securing
democracy
G|M|F
Policy Blueprint for
Countering Authoritarian
Interference in Democracies
G | M | F
The German Marshall Fund
of the United States

133

POLICY BLUEPRINT FOR COUNTERING AUTHORITARIAN INTERFERENCE IN DEMOCRACIES

2018 | No.27

JAMIE FLY, LAURA ROSENBERGER, AND DAVID SALVO

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1700 18th Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@securingdemocracy.org

This publication can be downloaded for free at http://www.gmfus.org/listings/research/type/publication.

About the Authors

Jamie Fly is a senior fellow and director of the Future of Geopolitics and Asia programs at The German Marshall Fund of the United States.

Laura Rosenberger is the director of the Alliance for Securing Democracy and a senior fellow at The German Marshall Fund of the United States (GMF)

David Salvo is the deputy director of the Alliance for Securing Democracy

About the Alliance for Securing Democracy

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

About GMF

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

Photo Credits: Unsplash.com/ Shutterstock.com

Executive Summary

In 2014, Russian government operatives began attacking American democracy through a multifaceted operation, a campaign that followed years of similar activity across Europe. A core component of this operation was the Russian government's aggressive interference in the 2016 presidential election, according to the unanimous conclusion of the U.S. intelligence community. Special Counsel Robert Mueller's February 16 indictment of the Internet Research Agency and related individuals, as well as the Senate Select Committee on Intelligence investigation, provided further details on the extent of Russia's interference in American democracy. Through e-mail hacks and leaks of information on politicians and campaigns, cyber-attacks against U.S. electoral infrastructure, and the injection of inflammatory material into the U.S. political and social ecosystems, the Kremlin sought to undermine the integrity of democratic institutions and amplify growing social and political polarization within and between the left and right. This campaign sought to damage Hillary Clinton's presidential campaign and boost Donald Trump's profile during the election. It also targeted prominent members of both parties, including members of the Trump administration, and average American citizens through political ads and disinformation on social media, a trend that continues to this day.

The Kremlin's operation to undermine democracy weaponized our openness as a nation, attempting to turn our greatest strength into a weakness, and exploited several operational and institutional vulnerabilities in American government and society:

- A government that was — and remains — unprepared to address asymmetric threats of this nature;
- Insufficient cyber defenses and outdated electoral infrastructure;
- Tech companies that failed to anticipate how their platforms could be manipulated and poor cooperation between the public and private sector to address technological threats;
- A highly polarized media environment which amplified Russian disinformation without regard for the credibility of the information they reported or the ethics of doing so;
- A porous financial system that allowed dirty or anonymous money to enter the country and facilitate the aims of corrupt foreign elite;
- The polarization of American citizens and the American political system; and,
- A general decline of faith in democracy and the media.

The Kremlin's playbook takes advantage of vulnerabilities and weaknesses in the societies it targets. In the United States, the vulnerabilities that the Kremlin exploited included operational and structural weaknesses in governance, legislation, and corporate policy. But they also exploited existing institutional and societal shortcomings in America. A hyper-partisan climate, declining faith in the ability of government to do its job, festering racial divisions, growing economic disparities, and the increasingly polarized media environment and prevalence of echo chambers, all provide fertile ground for adversaries who seek to do America harm. Addressing the threat of foreign interference requires closing both sets of vulnerabilities.

The tools the Kremlin has used to wage these operations include information operations, cyber-attacks, malign financial influence, support for political parties and advocacy groups, and state economic coercion. In a world increasingly interconnected by technology, state and non-state actors alike will be able to conduct malign interference operations of varying scales and sophistication. Other authoritarian regimes, such as China, have already adopted and begun to deploy asymmetric tools for their own interference operations. Some U.S. partners like Qatar and the United Arab Emirates are now even adopting similar tools as they attempt to influence American debates. As other foreign actors enter the field and as technology continues to rapidly advance, Western institutions, such as the EU and NATO, and democracies worldwide will face additional challenges.

A New Strategic Approach for Government and Society

Successive U.S. administrations of both parties neglected a threat once thought by many to be confined to Russia's periphery and not seen as a direct threat to U.S. national security. Tackling this challenge requires a new strategic approach for government and society to defend democracy against malign foreign interference, one that puts the problem at the forefront of the U.S. national security agenda and brings the public and private sectors together to complement each other's efforts. Rather than emulating the tactics used against us by authoritarian regimes, our responses should play to our strengths and be rooted in democratic values — respect for human and civil rights, including freedom of speech and expression and the right to privacy.

There must be a bipartisan response by the Executive Branch and Congress to improve our resilience, strengthen our deterrence, and raise the cost on those who conduct these operations against us. Defending against and deterring the threat also requires greater transatlantic cooperation at NATO and between the United States and the EU. Finally, Americans must rise above the polarization and hyper-partisanship in our media and civic discourse that exacerbated social and political divisions the Russian government exploited.

This report, representing the consensus of the Alliance for Securing Democracy's Advisory Council, a bipartisan, transatlantic group of national security experts, makes recommendations not only to government, but also to the various pillars of democratic society — civil society organizations, the private sector, including the tech companies, and media organizations — that all have important roles to play in defending democracies from foreign interference.[1] The report also outlines the asymmetric tools and tactics that authoritarian regimes use to undermine democracy, the types of influence operations that have been conducted across the transatlantic space over the past two decades, and the overall strategic approach that government and society should adopt in order to protect our democratic institutions from malign foreign influence.

Recommendations

The effort to tackle the authoritarian interference challenge will need to be as expansive and sustained as the threat, but there are immediate actions that Congress, government, and non-government actors can begin immediately:

1. Raise the cost of conducting malign influence operations against the United States and its allies.

The U.S. government at the highest level should publicly articulate a declaratory policy that makes clear it considers malign foreign influence operations a national security threat and will respond to them accordingly. The Executive Branch and Congress should also impose a broader set of sanctions and reputational costs against individuals and entities that conduct these operations, facilitate corruption, and support authoritarian regimes' destabilizing foreign policy actions. The Executive Branch should also employ cyber responses as appropriate to respond to cyber-attacks and deter future attacks, and consider offensive cyber operations using appropriate authorities to eliminate potential threats. Authoritarians that attempt to interfere in democracies' domestic politics must know that the repercussions for doing so will be severe and sustained.

2. Close vulnerabilities that foreign adversaries exploit to undermine democratic institutions.

From conducting cyberattacks against outdated electoral infrastructure to exploiting legislative loopholes to move money into the United States for covert political influence, foreign actors take advantage of our weaknesses in government. The administration and Congress should take several steps to ensure the integrity of our electoral process ahead of the 2018 midterm elections, as well as the integrity of our political system by closing off illicit finance and covert political influence from abroad. Government should also organize itself to respond to these threats more effectively by appointing a

1 The members of the Advisory Council of the Alliance for Securing Democracy endorse this report, indicating their support for its goals, direction, and judgments. Endorsement does not necessarily denote approval of every finding and recommendation. Advisory Council members contribute to the Alliance for Securing Democracy in their individual capacities.

senior-level Foreign Interference Coordinator ideally at the level of Deputy Assistant to the President at the National Security Council and establish a Hybrid Threat Center at the Office of the Director of National Intelligence to coordinate policy and intelligence across the U.S. government respectively.

3. Separate politics from efforts to unmask and respond to foreign operations against the U.S. electoral process. An incumbent government must be able to respond to an attack on our electoral system without being susceptible to accusations of political machinations. Congress should institute mandatory reporting requirements so that an administration must inform lawmakers of foreign attacks against U.S. electoral infrastructure, including individual political campaigns. Political parties and candidates running for office should also pledge publicly not to use weaponized information obtained through hacks or other illicit means.

4. Strengthen partnerships with Europe to improve the transatlantic response to this transnational threat.

Through bilateral relationships, cooperation with the EU and at NATO, and coordination between NATO and the EU, the United States and Europe can do a lot together to better defend and deter foreign influence operations: strengthen the sanctions regime on both sides of the Atlantic; shut down channels of money laundering and other forms of illicit finance; improve NATO's capabilities to support allies in responding to foreign influence operations; and, increase assistance to civil society within EU member states and in the surrounding neighborhood. The transatlantic community, together with democratic allies and partners worldwide, should establish a coalition to defend democracies to share information, analysis, and best practices to combat malign foreign influence operations.

5. Make transparency the norm in the tech sector.

Tech companies have released some data about the manipulation of their platforms by foreign actors, but the entire tech sector needs to be more proactive in providing Congress and the public information about their technology, privacy policies, and business models. Tech companies should also be more open to facilitating third-party research designed to assist them in defending their platforms from disinformation campaigns and cyber-attacks. Congress should help foster a culture of transparency, for example by passing legislation that ensures Americans know the sources of online political ads. Congress should also ensure that Americans' personal information is protected on social media platforms.

6. Build a more constructive public-private partnership to identify and address emerging tech threats.

The tech sector, the Executive Branch, and Congress need to establish a more constructive relationship to share information and prevent emerging technologies from being exploited by foreign adversaries and cyber criminals. New technologies, such as "deep fake" audio and video doctoring, will make the next wave of disinformation even harder to detect and deter. Platform companies need to collaborate more proactively with each other and with the U.S. government to mitigate threats that undermine democratic institutions.

7. Exhibit caution when reporting on leaked information and using social media accounts as journalism sources. As we witnessed throughout the 2016 presidential campaign, hacking operations by states and non-state actors are now a feature of political life in the democratic world. But the actors behind the hacks have an agenda, and that agenda can be enabled if media are not careful about how they report the story. Media organizations should also establish guidelines for using social media accounts as sources to guard against quoting falsified accounts or state-sponsored disinformation.

8. Increase support for local and independent media.

Today's media environment is dominated by the cable news networks, and, to a lesser extent, the major papers. Local and independent media are dying. That is bad for a number of reasons, including the fact that local media are often trusted to a greater degree than the major national news outlets. Philanthropic individuals and foundations

should support local journalism, as well as initiatives devoted to countering falsehoods propagated by foreign actors.

9. Extend the dialogue about foreign interference in democracies beyond Washington.

Government should help raise awareness about the threat of foreign interference, as exposure is one of the most effective means to building resilience and combating foreign interference operations. However, it should also seek partners in civil society who can combat foreign disinformation and effectively message to American and foreign audiences, and who are devoted to strengthening democratic values worldwide. New initiatives should be established to bring together civil society organizations to strengthen democratic institutions and processes in the United States. Washington-based officials and experts should also engage with Americans outside the Beltway more often to give them the tools they need to distinguish fact from fiction; identify trusted voices in local communities to participate in crafting solutions; and, foster a less politicized civic dialogue.

10. Remember that our democracy is only as strong as we make it.

The polarization of American society, reflected in our politics, contributed to the conditions that the Russian government exploited. All Americans have a responsibility to strengthen our democracy and address our problems at home that malign foreign actors use against us. Improving governance, strengthening the rule of law, fighting corruption, and promoting media literacy will help in this regard. Moreover, we need to instill a healthier respect for one another, regardless of our differences, by improving our civic discourse, practicing more responsible behavior on social media, respecting the vital role of the media, and calling on our elected officials to take action to defend our democracy on a bipartisan basis.

Foreward

"Nothing was more to be desired than that every practicable obstacle should be opposed to cabal, intrigue, and corruption. These most deadly adversaries of republican government might naturally have been expected to make their approaches from more than one quarter, but chiefly from the desire in foreign powers to gain an improper ascendant in our councils. How could they better gratify this, than by raising a creature of their own to the chief magistracy of the Union?" –Alexander Hamilton, writing as "Publius," Federalist 68, March 14, 1788[2]

In May 2016, two groups of protestors faced each other in downtown Houston, Texas. One side was drawn there by a Facebook group called "Heart of Texas" to oppose the purported "Islamification of Texas." The other side was recruited by a Facebook group called "United Muslims of America" and was there to rally for "saving Islamic knowledge." The dueling protests in Houston led to confrontation and verbal attacks between the sides. What neither the protestors nor the authorities understood at the time was that both Facebook groups that spurred the protests were established and operated not by Houstonians, but by individuals posing as Americans from thousands of miles away. For relatively little cost, the Internet Research Agency (IRA), the now infamous troll farm in St. Petersburg, Russia, manipulated the most widely used social media platform to pit Americans in the United States' fourth-largest city against one another. The goal may have been to incite violence between these opposing groups of protestors. That outcome was thankfully avoided due to the presence of local law enforcement.[3]

Fast forward to fall 2017. Across the United States, NFL players were taking a knee during the playing of the national anthem to protest racial inequality and police brutality. On social media, a debate raged between Americans regarding whether the protesting players were disrespecting their flag and their country. Once again, Russian-linked accounts on social media fanned the flames and promoted conspiracy theories.[4] The Alliance for Securing Democracy's (ASD) Hamilton 68 Dashboard noticed a spike in activity from the Russian-linked accounts it tracks weighing in on behalf of both

2 Alexander Hamilton, *The Federalist Papers*, No. 68, http://avalon.law.yale.edu/18th_century/fed68.asp.

3 Scott Shane, "How Unwitting Americans Encountered Russian Operatives Online," *The New York Times, February 18, 2018*, https://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebook-twitter.html.

4 Donie O'Sullivan, "American Media Keeps Falling for Russian Trolls," *CNNTech, June 21, 2018*, http://money.cnn.com/2018/06/21/technology/american-media-russian-trolls/index.html.

sides of the debate.[5] Over the past ten months, the Dashboard picked up similar trends during the protests in Charlottesville, Virginia over the removal of monuments to Confederate leaders, the "Me Too" movement to end sexual harassment and violence, debates about health care, and other hot-button social and political issues in the United States.

These events did not occur in isolation. They were part of a large-scale campaign run over the past several years by the Russian government and its proxies to undermine U.S. democracy and destabilize American society — following a pattern of similar activity to undermine democracies across Europe and weaken the transatlantic community for over a decade. More than a year and a half after the 2016 presidential election, this destabilization campaign continues.

The core component of this operation was the Russian government's aggressive interference in that election, according to the unanimous conclusion of the U.S. intelligence community.[6] Special Counsel Robert Mueller's February 16, 2018 indictment[7] of the IRA and related individuals, as well as the Senate Select Committee on Intelligence investigation[8], provided further details on the extent of Russia's attempted interference in our democratic institutions and society. The intelligence community continues to assess that Russia possesses the capabilities and intentions to interfere in future elections, a claim supported by senior members of President Donald Trump's administration, notably Secretary of State Mike Pompeo[9] and Director of National Intelligence Dan Coats.[10]

The Kremlin's playbook takes advantage of vulnerabilities and weaknesses in the societies it targets. In the United States, the vulnerabilities that the Kremlin exploited included operational and structural weaknesses in governance, legislation, and corporate policy. But they also exploited existing institutional and societal shortcomings in America. A hyper-partisan climate, declining faith in the ability of government to do its job, festering racial divisions, growing economic disparities, and the increasingly polarized media environment and prevalence of echo chambers, all provide fertile ground for adversaries who seek to do America harm. Addressing the threat of foreign interference requires closing both sets of vulnerabilities. The threat of foreign interference is one of several threats to our national security and democracy, but part of reducing its potency must be addressing the underlying conditions at home that allow these tactics to succeed.

Russia's actions to undermine U.S. democracy should serve as a wake-up call to all Americans. Our freedoms are preserved by a democratic system that is built upon free and open debate and the institutions that protect the rights that make such debate possible. Now our freedom and openness are being used by authoritarian adversaries of the United States to attempt to undermine our unity and ultimately our power and ability to engage in the world. We must learn the lessons of 2016 and address the institutional failures that led to the first significant foreign interference in an American election in the modern era.

This is not a question of the legitimacy of the 2016 election outcome. Ongoing investigations into the election should be allowed to run their course and routine congressional oversight of the Executive Branch must continue. Debates about the presidency of Donald Trump will continue to divide Americans. Yet what should unite Americans is the fact that Russia interfered in the U.S. election and continues to attempt to undermine the core of what makes us American — our democratic institutions. Left unaddressed, this threat will only grow as other authoritarians adopt similar tactics and use new technologies to make the threat even more persistent and potentially damaging. A divided

5 "Hamilton 68: Tracking Russian Influence Operations on Twitter," *Alliance for Securing Democracy*, https://dashboard.securingdemocracy.org/.

6 "Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

7 U.S. Department of Justice, "United States of America v. Internet Research Agency LLC," February 16, 2018, https://www.justice.gov/file/1035477/download.

8 U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry.

9 Cristiano Lima, "Pompeo: 'I Have Every Expectation' Russia Will Meddle in 2018 Elections," *Politico*, January 30, 2018, https://www.politico.com/story/2018/01/30/russia-2018-election-meddling.376826.

10 Kevin Johnson, "'The United States Is Under Attack': Intelligence Chief Dan Coats Says Putin Targeting 2018 Elections," *USA Today*, February 13, 2018, https://www.usatoday.com/story/news/politics/2018/02/13/intelligence-director-coats-says-u-s-under-attack-putin-targeting-2018-elections/332566002/.

response to Russia's interference plays into Vladimir Putin's hands and ensures that the Kremlin's original interference effort is successful.

That is why it is so important to address this challenge to our democracy through *bipartisan* efforts by the administration and Congress to improve our resilience, strengthen our deterrence, and raise the cost on those who conduct these operations against us. Rather than emulating the tactics used against us by authoritarian regimes, our responses should play to our strengths and be rooted in democratic values — respect for human and civil rights, including freedom of speech and expression and the right to privacy.

This report, representing the consensus of the Alliance for Securing Democracy's Advisory Council, a bipartisan, transatlantic group of national security experts, makes recommendations not only to government, but also to those that uphold the pillars of democratic society — civil society organizations, the private sector, including the tech companies, media organizations, and ultimately our fellow citizens — who all have important roles to play in defending democracies from malign foreign influence operations.[11] The report also outlines the tools and tactics that authoritarian regimes use to undermine democracy and the broader context of influence operations across the transatlantic space over the past two decades, of which the operation against the United States was only one of the most recent. It recommends a new strategic approach that government and society should adopt to protect our democratic institutions from authoritarian interference.

> ***"It is important to address the challenge to our democracy through bipartisan efforts by the administration and Congress to improve our resilience, strengthen our deterrence, and raise the cost on those who conduct these operations against us."***

I. The Operation against America

How the Kremlin Interfered in the U.S. Election and Targeted American Political Debates

When the Kremlin launched its operation against the United States in earnest in 2014, it did not start with an emphasis on a particular candidate for office. Instead, it adapted tactics out of the Soviet playbook. During the Cold War, the Soviet Union used so-called "active measures," to attempt to exploit divisions in American society. In its modern incarnation, the Russian government's agenda was to further polarize American society, raise doubt about the integrity of the U.S. electoral process, undermine confidence in U.S. institutions, and distract the U.S. government from its responsibilities on the global stage.

Special Counsel Mueller's indictment revealed that Russian operatives from the IRA began visiting the United States in 2014 to assess our political climate. This on-the-ground penetration in 2014 and early 2015 coincided with a flurry of online activity. As ASD Non-Resident Fellow Clint Watts testified before the Senate Select Committee on Intelligence, official Russian news outlets Sputnik and RT started pushing out stories on divisive issues like the Black Lives Matter protests and tensions in the Bundy Ranch standoff in Oregon.[12] They also ran stories promoting deliberately false information and conspiracy theories, such as the bogus claim that the U.S. government would declare martial law

11 The members of the Advisory Council of the Alliance for Securing Democracy endorse this report, indicating their support for its goals, direction, and judgments. Endorsement does not necessarily denote approval of every finding and recommendation. Advisory Council members contribute to the Alliance for Securing Democracy in their individual capacities. For a list of Advisory Council members and their biographies, see Appendix B.

12 Clint Watts, "Clint Watts' Testimony: Russia's Info War on the U.S. Started in 2014," *The Daily Beast, March 30, 2017*, https://www.thedailybeast.com/articles/2017/03/30/russia-s-info-war-on-the-u-s-started-in-2014.

during military exercises in Texas.[13] The Russian government established American-looking social media accounts that amplified these stories, giving them the veneer of credibility and popularity.[14] At the onset of the operation, the Russian government was preparing to undermine the 2016 election, but was more immediately focused on the broader objective of tainting democracy and democratic leaders and weakening the cohesiveness of American society.

As November 2016 approached, the IRA began to focus more specifically on the election and supporting the candidacy of Donald Trump, who Moscow assessed would enact policies more sympathetic to Russia's positions.[15] According to the Mueller indictment, part of the Kremlin's strategy involved "denigrating other [Republican] candidates, such as Ted Cruz and Marco Rubio."[16] The operation diversified in tools and tactics as Russian intelligence operatives conducted well-timed hacks of the Democratic National Committee (DNC) and Hillary Clinton's campaign chairman John Podesta and other campaign aides, hacks designed to deepen wounds between supporters of the two Democratic Party primary frontrunners, Clinton and Bernie Sanders, and to undermine Clinton's candidacy in the general election against Trump.[17] Russian intelligence services were also suspected of sharing those emails with WikiLeaks as well as setting up the website DCLeaks specifically to release hacked e-mails. Russian trolls masquerading as Americans on social media began purchasing political ads to support candidates, boost attendance at political rallies, and inflame debate around our society's most contentious social and political issues.[18] The ads not only supported Trump and far-right positions, but as the Mueller indictment showed, they also supported Sanders and Green Party candidate Jill Stein. Accounts called "Woke Blacks" and "Blacktivist" urged Americans to vote for third-party candidates or not show up to the polls.[19]

Russian operatives also probed American electoral infrastructure by launching cyber-attacks against 21 U.S. states' voting systems and voter registration databases, targeting election officials' e-mail accounts, and breaking into a private election systems company's server and using that position as a launching point to send phishing emails to 122 state and local election officials in Florida.[20] While there is no evidence to suggest these cyber-attacks changed actual votes, the numerous cyber incursions point to vulnerabilities in U.S. electoral infrastructure and indicate Russian hackers may have been gathering information on these systems to exploit in the future. Or, these probes may have been conducted to provide a basis for raising doubts about the integrity of the electoral process if the election result had been different, to accompany Russian disinformation that the election would be rigged. There is also the question of whether the Russian government provided direct financial support to U.S. political actors and organizations, in addition to purchasing political ads and funding rallies supported by genuine U.S. political groups.[21]

What many Americans may not realize is that since the election, the Kremlin's proxies have continued their offensive. On a daily basis, they are repeatedly injecting inflammatory material into the U.S. political and social ecosystems to amplify growing social and political polarization within and between the left and right. These operations have targeted prominent Democrats as well as Republicans, including members of the Trump administration. The continued targeting of wedge issues that divide Americans, from racial equality to immigration, combined with continued cyber-attacks on U.S.

13 "Jade Helm 15: Texans Terrified of Obama-Led US Army Invasion," *SputnikNews, July 7, 2015*, https://sputniknews.com/us/201507071024303072/; Robert Bridge, "Jade Helm 15: One Nation Under Siege?," *RT, July 10, 2015*, https://www.rt.com/op-ed/272920-us-army-jade-helm/.

14 Scott Shane, "The Fake Americans Russia Created to Influence the Election," *The New York Times, September 7, 2017*,https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

15 "Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, p. 1, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

16 U.S. Department of Justice, "United States of America v. Internet Research Agency LLC," p. 17, February 16, 2018, https://www.justice.gov/file/1035477/download.

17 Raphael Satter, "Inside Story: How Russians Hacked the Democrats' Emails," *AP News, November 4, 2017*, https://www.apnews.com/dea73efc013948d39957c3c9a6c962b8a.

18 "The Social Media Ads Russia Wanted Americans To See," *Politico, November 1, 2017*, https://www.politico.com/story/2017/11/01/social-media-ads-russia-wanted-americans-to-see-244423.

19 Rachel Wolfe, "Donald Trump, Bernie Sanders, and Jill Stein All Appear to Have Been Helped By Russian Election Interference," *Vox, February 16, 2018*, https://www.vox.com/policy-and-politics/2018/2/16/17021248/russian-election-interference-sanders-stein-trump.

20 Matthew Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," *The Intercept, June 5, 2017*, https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

21 U.S. Congress, House of Representatives, Committee on Science, Space, and Technology, *Majority Staff Report: Russian Attempts to Influence U.S. Domestic Energy Markets by Exploiting Social Media, March 1, 2018*, 115th Cong. 2nd sess. https://science.house.gov/sites/republicans.science.house.gov/files/documents/115%20Staff%20Report%20-%20Russian%20Attempts%20to%20Influence%20U.S.%20Domestic%20Energy%20Markets%20by%20Exploiting%20Social%20Media%20-%2003.01.18.pdf.

critical infrastructure, is designed to destabilize American society and lay the groundwork for campaigns to undermine future elections.[22]

It is still unclear whether attempts to undermine the midterm elections in November 2018 and the presidential election in 2020 will match the scope and severity of the 2016 operation. However, Russia and other adversaries possess the capabilities and the motivation to interfere in future elections, and the overwhelming consensus among national security professionals, including members of President Trump's cabinet, is that our elections and democratic institutions are at risk of being attacked and our defenses are insufficient.

Operational and Institutional Vulnerabilities: Why the United States Failed to Stop the Threat

The Kremlin operation to undermine democracy weaponized our openness as a nation, attempting to turn our greatest strength into a weakness, and exploited several operational and institutional vulnerabilities in American government and society:

- A government that was — and remains — unprepared to address asymmetric threats of this nature;
- Insufficient cyber defenses and outdated electoral infrastructure;
- Tech companies that failed to anticipate how their platforms could be manipulated and poor cooperation between the public and private sector to address technological threats;
- A highly polarized media environment which amplified Russian disinformation without regard for the credibility of the information they reported or the ethics of doing so;
- A porous financial system that allowed dirty or anonymous money to enter the country and facilitate the aims of corrupt foreign elite;
- The polarization of American citizens and the American political system; and,
- A general decline of faith in democracy and the media.

It took significant time for the various agencies of the U.S. government to connect the dots and understand the breadth and scope of the Russian operation. Even now, more than a year and a half after the election, the full extent of Russian activities is still being uncovered. The Kremlin's interference used tools and tactics that cut across agency jurisdictions. No government agency had a full picture of the disinformation campaign unfolding on social media until after the election. Additionally, there was not a clear understanding that the Kremlin was using cyber-attacks against electoral infrastructure until approximately the summer of 2016. The cyber-attacks triggered alarm bells across the federal government — the Department of Homeland Security (DHS), the Department of State, the National Security Council, the Homeland Security Council, and the intelligence community — but some state officials overseeing their own electoral jurisdictions balked at receiving federal assistance to secure the vote and some local officials still dispute the threat environment for the 2018 elections.[23]

Politics inhibited an adequate response as well. The Obama administration was cautious in its public pronouncement regarding the unfolding attack because of concerns that the White House would be accused of trying to influence the electorate by unilaterally releasing information claiming the Russian government was conducting an operation to elect Donald Trump.[24] The administration's attempts to coordinate with Members of Congress to inform the public on a bipartisan basis were rebuffed, owing to concerns about the veracity of the intelligence

22 "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," *United States Computer Emergency Readiness Team, Department of Homeland Security, March 15, 2018*, https://www.us-cert.gov/ncas/alerts/TA18-074A.

23 Philip Bump, "What Obama Did, Didn't Do And Couldn't Do in Response to Russian Interference," *Washington Post, February 21, 2018*, https://www.washingtonpost.com/news/politics/wp/2018/02/21/what-obama-did-didnt-do-and-couldnt-do-in-response-to-russian-interference/.

24 Edward-Isaac Dovere, "Biden: McConnell Stopped Obama From Calling Out Russians," *POLITICO, accessed June 5, 2018*, http://politi.co/2BpdrQi.

and the possibility of influencing the vote in favor of Clinton.[25] Democrats and Republicans each put out their own versions of the unfolding events, further confusing the electorate. In the heat of the campaign, Donald Trump also encouraged the Russians to hack and leak e-mails of his opponent, and praised WikiLeaks for releasing the content of the e-mails.[2627]

Tech companies missed or ignored warning signs as well. None of the major social media companies had sufficient mechanisms in place to identify and shut down on a timely basis the types of falsified accounts or malicious bot accounts the Kremlin's proxies used. Twitter estimated after the fact that there were over 50,000 Russian-linked accounts during the campaign on its platform alone, while the Democratic members of the House Permanent Select Committee on Intelligence (HPSCI) revealed that there were 3,841 Twitter accounts directly connected to the IRA, some of which were opened and continued to operate after the 2016 election.[2829] The same HPSCI report noted 470 IRA-created Facebook pages with 80,000 pieces of organic content on those pages reaching more than 126 million Americans.[30] The IRA also exploited the social media companies' ethos of providing open platforms for civic and political discourse by purchasing ads in support of candidates and issues. This was a problem that traveled across platforms: Facebook, Twitter, Instagram, YouTube, Tumblr, Reddit, 4Chan, and others were all mediums for Kremlin-linked influence operations.[31]

During the 2016 campaign, social media accounts were rife with information for journalists working for traditional media outlets as a type of *vox populi*. Unfortunately, they were rife with disinformation as well. Thirty-two of thirty-three major American news outlets used information from accounts that were later revealed to be operated by the IRA (the media continued to use IRA accounts as sources for news stories long after the election).[3233] Some of the outlets only used IRA-cited information once, but even one time is too many. In addition, media outlets eagerly reported on the information released by WikiLeaks from the DNC and Podesta hacks, often without confirming the veracity of the information or contextualizing the source of the information as obtained through illegal means by a foreign actor trying to influence the election.

Finally, the polarization of American society, reflected in our politics, exacerbated the divisions the Russian government exploited. The rise of cable news reflecting a particular political agenda, rise of social media as a primary source of news and information for many Americans, the entrenchment of echo chambers on online platforms, the spread of vitriol online, and the general debasement of civic discourse left the United States susceptible to foreign interference. These problems have not abated since the 2016 election, nor has the threat of foreign interference in American democracy. Americans must learn from all of these institutional and societal failures to address this ongoing challenge on a bipartisan basis.

II. New Technologies, Old Tactics: The Longstanding Threat to Democracies

The multifaceted operation to undermine America brought the threat of Russian malign influence operations back to the forefront of the U.S. national agenda, but the threat is not new. Deploying various tools to target foreign governments and to exploit open, democratic societies harkens back to Soviet times. During the Cold War, democracy was the

25 Jennifer Rubin, "McConnell Owes the Country a Fuller Explanation on Russian Meddling," *Washington Post, February 20, 2018*, https://www.washingtonpost.com/blogs/right-turn/wp/2018/02/20/mcconnell-owes-the-country-a-fuller-explanation-on-russian-meddling/.

26 Michael Crowley and Tyler Pager, "Trump Urges Russia to Hack Clinton's Email," *Politico, July 27, 2016*, https://www.politico.com/story/2016/07/trump-putin-no-relationship-226282.

27 David Choi, "5 Times Trump Praised WikiLeaks during His 2016 Election Campaign," *Business Insider, November 13, 2017*, http://www.businessinsider.com/trump-wikileaks-campaign-speeches-julian-assange-2017-11.

28 Jon Swaine, "Twitter Admits Far More Russian Bots Posted on Election Than It Had Disclosed," *The Guardian, January 20, 2018, sec. Technology*, http://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed.

29 U.S. Congress, House Permanent Select Committee on Intelligence Democrats, "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," June 18, 2018, https://democrats-intelligence.house.gov/social-media-content/default.aspx.

30 Ibid.

31 Bradley Hanlon, "It's Not Just Facebook: Countering Russia's Social Media Offensive," *Alliance for Securing Democracy, German Marshall Fund of the United States, April 11, 2018*, http://securingdemocracy.gmfus.org/publications/its-not-just-facebook-countering-russias-social-media-offensive.

32 Josephine Lukito and Chris Wells, "Most Major Outlets Have Used Russian Tweets As Sources For Partisan Opinion: Study," *Columbia Journalism Review, March 8, 2018*, https://www.cjr.org/analysis/tweets-russia-news.php.

33 Donie O'Sullivan, "American Media Keeps Falling for Russian Trolls," *CNNTech, June 21, 2018*, http://money.cnn.com/2018/06/21/technology/american-media-russian-trolls/index.html.

Soviet Union's ideological enemy. Moscow used so-called "active measures" inside the United States and against our allies across the globe to advance the cause of communism worldwide.[34] These tactics, however, were often costly and time consuming with limited reach, in stark contrast to the ease with which technology now facilitates remote manipulation and low-cost individual targeting of any American with a smart phone and a social media account.

Post-Soviet Russia no longer has the same ideological fabric, but democracy remains the enemy of President Vladimir Putin and those who prop up his autocratic, kleptocratic regime. President Putin is concerned, above all, with maintaining his hold on power. To maintain his regime's stability and defuse the internal power struggles that threaten all autocracies, Putin ensures his control over Russia's levers of power by facilitating the enrichment of loyalists in the security services, government, and state-owned enterprises. The population sees little of the spoils of corruption – and even pays for the spoils. To justify its system of government at home, the Kremlin uses state-controlled media to push the narrative that the West is in decline and that democracy is not the superior form of government western officials would have them believe. The Russian government's operations to weaken democracies give Putin examples to highlight as he justifies his own corrupt regime to his people and maintains his grip on power.

According to Russian military doctrine, the NATO alliance, led by the United States, represents the primary threat to Russian national security.[35] From the Kremlin's perspective, NATO's mission to maintain peace and security in Europe and representation, along with the EU, of a community of transatlantic democratic states, runs counter to the Kremlin's interests. Putin employs a combination of low-cost tools to weaken others in order to provide Russia with greater relative power on the world stage. The Russian government's operations beyond its borders, especially campaigns waged in European countries over the past two decades, aim to fracture the cohesion of the EU and NATO, divide European allies from one another and from the United States, and weaken and distract the United States in order to assert a more aggressive posture abroad with less of a challenge from the West. Finally, the Kremlin seeks to change nations' policies towards Russia; through influence operations, it aspires to spread a more pro-Russian worldview among political, financial, civic, and media leaders in other countries that can be advantageous to Moscow's interests worldwide.

The Asymmetric Toolkit

The Kremlin employs a set of asymmetric tools to undermine democracy in other countries. Many of these tools are not new, nor are they specific to Russia, and they are often used in combination with one another to engage in political warfare.

Asymmetric tools are low-cost, often deniable measures that can counter conventional military superiority.[36] This toolkit includes:

1. Information operations: The deliberate use of false narratives through traditional and social media to mislead a population, and the amplification or weaponization of information in order to increase the polarization or undermine democratic institutions of a particular society.

2. Cyber-attacks: The penetration of computer networks to cripple critical infrastructure; disrupt the work of public and private sector actors; and, steal or alter data to inflict damage upon or cause confusion within a government, corporation, or society.

3. Malign Financial Influence: The movement of money into another country to acquire political and economic leverage and fund other asymmetric activities; and, the use of corruption as a means to recruit proxies.

4. Support for political parties and advocacy groups: The backing of politicians and groups, often at the extremes of the political spectrum, inside another country through financial, rhetorical, and

34 U.S. Department of State, "Soviet 'Active Measures': Forgery, Disinformation, Political Operations," October 1981, https://www.cia.gov/library/reading-room/docs/CIA-RDP84B00049R001303150031-0.pdf.

35 Ministry of Defense of the Russian Federation, "Voennaja doktrina Rossijskoj Federacii," December 26, 2014, http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589760.

36 Laura Rosenberger and Jamie Fly, "Shredding the Putin Playbook," *Democracy Journal, Winter 2018, No. 47*, https://democracyjournal.org/magazine/47/shredding-the-putin-playbook/.

other means, designed to promote a friendly agenda toward the government providing support or to support divisive or extremist views inside the host country.

5. State economic coercion: The exploitation of national resources to use as leverage over another country's government to weaken it and force a change in policy.

The use of this relatively inexpensive toolkit offsets conventional weaknesses, particularly economic limitations, and keeps adversaries off balance through their deniable and covert nature. The plausible deniability inherent in some of these measures presents challenges for democracies to respond. Often, these tools are used in the absence of kinetic military force, though in some cases, especially on Russia's periphery, they have been combined with hybrid warfare or kinetic operations, most notably in February 2014, when Russian soldiers masquerading as "little green men" in unmarked uniforms took control of Crimea, in Ukraine, and supported separatist forces in eastern Ukraine; and in August 2008, when Russian soldiers openly invaded neighboring Georgia.

This toolkit is also being used by other authoritarian governments, most notably China, to interfere in democracies. Russia's successful exploitation of democracies' vulnerabilities in Europe and the United States is likely to lead other authoritarians to adopt the Putin playbook. Concerningly, even U.S. partners are now utilizing elements of this interference toolkit. Countries including Qatar and the United Arab Emirates have reportedly used financial influence, cyber-attacks, and disinformation to attempt to influence American politics.[37]

An Overview of Russia's Asymmetric Operations in Europe

The Kremlin Russia's military interventions in Georgia in 2008 and Ukraine in 2014 were the most egregious and deadly operations to foment instability in Europe since the collapse of the Soviet Union. These interventions not only sought a geopolitical goal — to impede the Euro-Atlantic aspirations of these countries — but also directly challenged the fundamental norms and principles of the UN Charter governing the post-war liberal international order for decades, particularly the principle of states' territorial integrity and sovereignty. Along with military occupation, Moscow has used elements of the asymmetric toolkit against Ukraine: disinformation campaigns[38] spread pro-Kremlin propaganda; cyber-attacks[39] have crippled government agencies (including the Central Election Commission during the 2014 presidential elections[40]), infrastructure, private companies, and military systems; energy resources[41] (and the withholding of them) have been used as a form of coercion; and, separatists and extremists who engage in violent and destabilizing activities have been supported.

The Russian government's massive, three-week cyber-attack against neighboring Estonia in 2007 arguably gave the threat of these asymmetric tools a new sense of urgency for NATO and the EU. Since then, the three Baltic States have been hit particularly hard by Russian-originated cyber-attacks[42] and disinformation campaigns,[43] as Russia seeks to take critical infrastructure offline and sow discord between the ethnic majorities and Russian minorities of all three countries. Moscow has used both licit and illicit means to curry favor with political and economic elites in several Central and Eastern European countries, attempting to reorient their governments, economies, and societies from

37 Kevin Collier, "How Two Persian Gulf Nations Turned the US Media into Their Battleground," *Buzzfeed, May 9, 2018*, https://www.buzzfeed.com/kevincollier/qatar-uae-iran-trump-leaks-emails-broidy?utm_term=.eaE29g2aW#.tv5mGqmRL.

38 Ellen Nakashima, "Inside a Russian Disinformation Campaign in Ukraine in 2014," *Washington Post, December 25, 2017*, https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html.

39 Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired, June 20, 2017*, https://www.wired.com/story/russian-hackers-attack-ukraine.

40 Mark Clayton, "Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers," *Christian Science Monitor, June 17, 2017*, https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

41 Vladimir Soldatkin and Natalia Zinets, "Gazprom Seeks to Halt Ukraine Gas Contracts as Dispute Escalates," *Reuters, March 2, 2018*, https://www.reuters.com/article/us-russia-ukraine-gas/gazprom-seeks-to-halt-ukraine-gas-contracts-as-dispute-escalates-idUSKCN1GE2DW.

42 Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-based Hackers Target Baltic Energy Networks," *Reuters, May 11, 2017*, https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5.

43 "Baltics Battle Russia in Online Disinformation War," *DW, October 8, 2017*, http://www.dw.com/en/baltics-battle-russia-in-online-disinformation-war/a-40828834.

the EU to Moscow. We are now witnessing how many countries in Central and Eastern Europe, notably Hungary and Poland, risk democratic backsliding; while anti-democratic forces in these countries initially gained strength without external assistance, the Russian government provides various forms of financial, rhetorical, and political support to many of them.

European nations that aspire to join the EU or NATO are particular targets of Russian active measures. The Kremlin backed a failed coup attempt in Montenegro that sought to install an anti-NATO government in Podgorica.[44] A daily barrage of Russian disinformation demonizing NATO and the United States floods the media space in Serbia, while in Bosnia and Herzegovina, Moscow's support for nationalist politicians through a variety of means helps fan ethnic tensions and undercuts the country's progress toward EU and NATO accession.[45]

More recently, the countries of Western Europe, the bulwark of European values and the heavyweights of the EU, have faced destabilization operations as well. The transatlantic community, including the United States, long viewed Russian asymmetric threats as limited to the countries along Russia's periphery, such as Georgia, Ukraine, and the Baltic states. Few thought Moscow would extend its reach into Western Europe or across the Atlantic to North America. But such assessments were short-sighted and underestimated the threat. Putin may have perceived a lack of transatlantic resistance to Russian aggression in Georgia and Ukraine, and ultimately set his sights westward. Russian disinformation campaigns have fomented separatism and the fragmentation of Europe. In the UK, Moscow targeted the Scottish independence referendum[46] and the Brexit vote,[47] while in Spain, Kremlin-operated and other pro-Kremlin online accounts boosted support for Catalonian secession from Spain.[48] Even a Dutch referendum on the EU's Association Agreement with Ukraine became a target for Russian disinformation; the campaign against the agreement, which ultimately won the vote, used pro-Kremlin narratives pulled from RT and Sputnik and had links to Russian academics parroting Moscow's position against the agreement.[49][50]

Meanwhile, in elections in France and Germany in 2017, Russian government operatives injected disinformation into the ecosystem to promote far-right groups supportive of the Kremlin's agenda, including German far-right party Alternative fur Deutschland (AfD), the first far-right party ever to clear the five-percent hurdle to enter parliament in post-war Germany.[51][52] Germany also faced a Russian-led disinformation campaign, centered around false allegations that a gang of migrants raped a 13-year old German of Russian origin named Liza, that sought to increase anti-migration sentiments in the run-up to the country's parliamentary elections, arguably giving AfD a big assist in the subsequent elections.[53] Hackers likely affiliated with Russian intelligence services targeted

44 Valerie Hopkins, "Indictment Tells Murky Montenegrin Coup Tale," *POLITICO*, May 23, 2017, https://www.politico.eu/article/montenegro-nato-milo-dukanovic-murky-coup-plot/.

45 David Salvo and Stephanie De Leon, "Russia's Efforts to Destabilize Bosnia and Herzegovina," *The German Marshall Fund of the United States*, April 25, 2018, http://securingdemocracy.gmfus.org/publications/russias-efforts-destabilize-bosnia-and-herzegovina.

46 David Leask, "Fake Twitter Accounts Send 400,000 Independence Messages," *Herald Scotland*, November 19, 2017, http://www.heraldscotland.com/politics/referendumnews/15670523.Fake_Twitter_accounts_send_400_000_independence_messages/.

47 Robert Booth et al., "Russia Used Hundreds of Fake Accounts to Tweet About Brexit, Data Shows," *The Guardian*, November 14, 2017, sec. World news, http://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

48 David Salvo and Etienne Soula, "Russian Government's Fission Know-How Hard at Work in Europe," *Alliance for Securing Democracy, German Marshall Fund of the United States*, October 31, 2017, https://securingdemocracy.gmfus.org/blog/2017/10/31/russian-governments-fission-know-how-hard-work-europe.

49 Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," *The New York Times*, February 16, 2017, https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html.

50 Anne Applebaum, "The Dutch Just Showed the World How Russia Influences Western European Elections," *The Washington Post*, April 8, 2016, https://www.washingtonpost.com/opinions/russias-influence-in-western-elections/2016/04/08/9427602a-fcf1-11e5-886f-a037dba38301_story.html.

51 Chloe Farand, "French Social Media Is Being Flooded With Fake News, Ahead of the Election," *The Independent*, April 22, 2017, http://www.independent.co.uk/news/world/europe/french-voters-deluge-fake-news-stories-facebook-twitter-russian-influence-days-before-election-a7696506.html; Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections," *Brookings Institution*, June 28, 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

52 Anne Appelbaum, Peter Pomerantsev et al., "'Make Germany Great Again:' Kremlin, Alt-Right and International Influences in the 2017 German Elections," *Institute for Strategic Dialogue*, December 6, 2017, https://www.isdglobal.org/wp-content/uploads/2017/12/Make-Germany-Great-Again-ENG-061217.pdf.

53 Michael Weiss, "The Kremlin Cries Rape for Propaganda in Germany," *The Daily Beast*, February 2, 2016, https://www.thedailybeast.com/the-kremlin-cries-rape-for-propaganda-in-germany.

French President Emmanuel Macron's presidential campaign's e-mail servers and leaked the contents online in the final days of the campaign.[54]

Using official news organizations like Sputnik and RT, which are amplified by Russian-linked accounts on social media, the Kremlin actively promotes alternative theories in these targeted European countries, all of them dubious and deliberately misleading, to explain away the Russian government's connection to egregious violations of international norms in Europe. Moscow has waged disinformation campaigns to argue the Russian military is not fighting in eastern Ukraine on behalf of separatist rebels and to persuade the European public that the Ukrainian military, and not the Russian-controlled separatists, downed Malaysian Airlines flight MH17, despite an international forensic investigation that unequivocally implicated the Russian military.[55] The Kremlin has also pushed false flag conspiracy theories to explain the poisoning of former British intelligence asset Sergei Skripal and his daughter Yulia in Salisbury, England, an act carried out by the Russian intelligence services, and to claim that the West deliberately staged chemical weapons attacks against Syrian civilians as a pretext to launch missile strikes against Bashar al-Assad's regime.[56] These information operations have a singular purpose: by promoting falsehoods frequently and loudly enough, the Kremlin perpetuates a public discourse that denigrates the value of facts, making it more difficult for Europeans to maintain a united front in the face of Russian aggression on the continent and beyond.

The Russian government has even expanded its activities to regions of the world in which it seeks to regain some of the influence the Soviet Union once enjoyed. In Latin America, for example, senior officials in the Trump administration have warned there is mounting evidence that the Kremlin is again employing its disinformation army to influence public opinion and potentially elections in Mexico.[57]

III. A New Strategic Approach for Government and Society

As the Kremlin achieved success with its tools and tactics in the United States and across the transatlantic community, democratic governments and societies' vulnerabilities to asymmetric operations have been exposed for others to exploit. In a world increasingly interconnected by technology, state and non-state actors alike will be able to conduct malign influence operations of varying scales and sophistication. As other foreign actors enter the field, Western institutions, such as the EU and NATO, and democracies worldwide will face additional challenges. China has moved beyond its economic-driven approach to gain influence in other countries and has started adopting more overt forms of political interference in countries like Australia and New Zealand, as well as in Taiwan and Hong Kong.[58] Autocrats like Philippines President Rodrigo Duterte and Turkish President Recep Tayyip Erdogan are using these tools against their own citizens, with Duterte building his own "keyboard army" to silence dissent and Turkish pro-government trolls hacking, harassing, and threatening journalists.[59][60]

Technology will continue to advance faster than governments and society can adapt. Today's disinformation operations will look amateur compared to what is coming in the future. Tools that allow for precise doctoring of audio, images, and video will make it even more complicated to discern fact from fiction. Algorithms, which already drive much of the operations of major social media platforms, will hold increasing sway as artificial

54 Alex Hern, "Macron Hackers Linked to Russian-Affiliated Group Behind US Attack," *The Guardian*, May 8, 2017, sec. *World news*, http://www.theguardian.com/world/2017/may/08/macron-hackers-linked-to-russian-affiliated-group-behind-us-attack.

55 Mike Corder, "Netherlands, Austria Hold Russia Liable for Downing MH17," *The Associated Press*, May 25, 2018, https://apnews.com/4b05cd0e43c84e74822e8bf1356337cdf; "Defensive Disinformation as Decoy Flare: Skripal and Flight MH17," *EU vs Disinfo*, March 27, 2018, https://euvsdisinfo.eu/defensive-disinformation-as-decoy-flare-skripal-and-flight-mh17/.

56 DFRLab, "#TrollTracker: Disinformation Surge from Skripal to Syria," *Medium*, April 17, 2018, https://medium.com/dfrlab/trolltracker-disinformation-surge-from-skripal-to-syria-f44f92a476cd.

57 "Tillerson Warns Mexico to Watch Russian Election Meddling," *Reuters*, February 2, 2018, https://www.reuters.com/article/us-mexico-usa-russia/tillerson-warns-mexico-to-watch-russian-election-meddling-idUSKBN1FM2MO.

58 Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response | The Asan Forum," May 8, 2018, http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response/.

59 "Freedom of the Net 2017," *Freedom House*, November 14, 2017, https://freedomhouse.org/report/freedom-net/2017/philippines.

60 Maeve Shearlaw, "Turkish Journalists Face Abuse and Threats Online Trolls Step Up Attacks," *The Guardian*, November 1, 2016, https://www.theguardian.com/world/2016/nov/01/turkish-journalists-face-abuse-threats-online-trolls-attacks.

intelligence plays a larger role in the technology that powers our daily lives. Cyber tools may allow foreign actors to penetrate more deeply into government and corporate networks to steal information, disrupt elections, and compromise individual privacy without much of a trace. The challenges we face today will grow by an order of magnitude. That is why all parts of democratic societies must be involved in exposing influence operations, as one of the best methods to preventing future attacks is to shine sunlight on existing ones, and in shaping our responses. The threat to democracies' stability is clear. But our focus now needs to be on not just understanding the problem, but defending against and deterring it going forward.

Whole of Government

Much like the 9/11 attacks demonstrated how government had to reorient itself to confront a potent, unconventional, asymmetric threat in global terrorism, defending against foreign interference operations demands a new strategic approach. The failure to unearth and respond to the operation against the 2016 election in a timely manner revealed how necessary it is for government to detect these threats in an integrated manner, involving all relevant players in the interagency, and to respond to them holistically and strategically, rather than in silos. The Executive Branch and Congress must therefore rectify existing bureaucratic and structural impediments to improve coordination between federal agencies and between the federal, state, and local governments. In particular, the cross-cutting nature of the threat demands the allocation of sufficient resources to address it and the harnessing of expertise across the policy and intelligence communities under one roof. The national security community should also develop greater expertise on asymmetric and emerging threats.

But bureaucratic fixes are only part of the solution. An effective, long-term strategy must start by putting the issue at the forefront of the U.S. national security agenda, with the public recognition that foreign actors' attempts to weaken the United States and our allies by undermining democratic institutions constitute a threat to national security. That will require clear strategic messaging from the top. A decisive signal from the administration at the highest level and from Congress that the United States considers these activities a threat to national security and will respond accordingly is essential for making clear to adversaries and allies alike that the U.S. government takes the threat seriously. A united front by the President, the Cabinet, and leading Members of Congress can help facilitate better coordination between the federal government and state and local governments to bolster defenses at all levels. Strong leadership from Washington can also raise awareness and build resilience in society toward a threat that affects the average American just as it affects the political establishment in Washington. Through effective public messaging, the White House and Congress can also help transcend the politicization of civic discourse that malign foreign influence operations exploit to further divide Americans from one another. It is essential that America's enemies as well as U.S. partners that may be tempted to utilize similar tools in their quest for influence realize that there will be repercussions for violating U.S. laws and undermining American democracy.

Distrust between the Executive Branch and Congress hindered the U.S. government's ability to respond to the Russian operation against the 2016 election. Partisan distrust has prevented Democrats and Republicans, as well as the White House and Congress, from taking urgent action to defend our nation. This distrust and politicization of a national security threat have impeded necessary work by the Trump administration and Congress to fully secure electoral infrastructure, prevent foreign money from influencing public opinion during political campaigns, develop effective means to work with the technology community to address technological vulnerabilities, and close legislative and regulatory loopholes that allow foreign actors to use money to peddle political influence. America's leaders are essentially leaving the country undefended against a threat that is only growing

Removing partisanship from the calculus in responding to this threat is critical to ensuring our elected representatives and government officials take actions to secure our democracy. Legislation that establishes clear indicators of foreign interference in elections and other democratic institutions and processes and mandates that the Executive Branch report to Congress when those

tripwires are crossed would correct two deficiencies from 2016: first, it would allow an incumbent administration to report information to Congress and the public without being accused of trying to affect the results of an election; and second, it conceivably would create conditions for Members of Congress to reach across the aisle and act in the public interest.

Foreign operations to destabilize our democracy will continue to be a threat long into the future. And foreign adversaries will continue to take advantage of a polarized, hyper-partisan political climate, so long as it exists. It is short-sighted — and indeed, emboldens adversaries like Vladimir Putin — when politics gets in the way and political leaders fail to take action to protect the institutions that make America what it is.

Raising the Cost on Our Adversaries

Raising the cost of conducting these operations against the United States must be another essential pillar of government's strategic approach to addressing this threat. Government should resist the temptation of responding tit-for-tat to every active measure. There will be times when a symmetric response is necessary, including proportionate cyber responses to cyber-attacks and potentially offensive cyber-attacks as a deterrent. But government generally needs to breakdown the individual silos through which it addresses each tool in the asymmetric toolkit. Instead, the administration and Congress should define and use our own asymmetric advantages and strategically deploy instruments of national power that will serve as the most effective deterrent. This approach will allow democracies to play to their advantage, rather than responding on an adversary's terms, and provide the best chance of inducing a foreign actor to change behavior.

In the case of Russia, the Putin regime places regime survival above all other objectives and is dependent on the corrupt financial links that tie together the political leadership, security services, and business. To impose real consequences on the Kremlin that could lead to behavioral change, U.S. policy should play to our own strengths and focus on exploiting Russia's comparative economic weaknesses by using sanctions, asset forfeiture, and anti-money laundering tools to target the illicit wealth of individuals and entities that assist the Kremlin's destabilizing foreign policy actions, and by exposing the ill-gotten gains of top Russian officials, including President Putin himself. Such an approach should hit politically important elements of the elite hardest, increasing political pressure and heightening internal dissent. Tracking and disrupting financial stocks, flows, and new investments will make it more difficult for the Kremlin to fund malign influence activities abroad and gain access to sensitive technology or data. Even transparency about legitimate Russian investments in democratic countries is important to limit the danger that Russian economic influence will inappropriately impact politicians and their decision-making in other countries. Such measures will also serve to strengthen our own democracies, rooting out pathways for corruption. To the greatest extent possible, these measures should be multilateral, taken together with our European allies and partners, as well as democratic allies and partners around the world. A transatlantic focus on illicit finance will deny those who benefit from kleptocracy the ability to enjoy its fruits in the West.

Imposing reputational costs on authoritarian powers that employ these tools must also be part of the counter-arsenal. Vladimir Putin values his standing on the world stage. That is why it is so important that Russia not be allowed to reenter normal international fora until Russian behavior changes. Just as Europeans should halt their recent renewed engagement of Russia in the wake of President Trump's withdrawal from the JCPOA, the Trump administration should not encourage Russia's re-admission to gatherings of the world's major economic and democratic powers. Authoritarians need to know that democratic interference brings with it a cost that will not fade with the passage of time. This is as true for China as it is for Russia. The Chinese Communist Party is more sensitive about being exposed for illegal activity and interference operations abroad, as China attempts to sell an alternative model of governance and growth to developing nations.[61] Imposing reputational costs on Beijing must be a pillar of western deterrence strategy.

61 Laura Rosenberger and John Garnaut, "The Interference Operations from Putin's Kremlin and Xi's Communist Party: Forging a Joint Response," *Open Forum, The ASAN Forum, May 8, 2018*, http://www.theasanforum.org/the-interference-operations-from-putins-kremlin-and-xis-communist-party-forging-a-joint-response.

Governments cannot reasonably expect to stop every type of asymmetric operation. Cyber-attacks will continue, as will attempts to mislead public opinion through disinformation campaigns. The challenge of responding to asymmetric threats like foreign interference operations is that the attackers attempt to exploit a gray zone — neither outright warfare that affects hard security assets, nor soft power that seeks to influence a foreign public through benign measures like commerce or educational exchanges. The reality, however, is that these tactics are a direct attack on democracy and should be treated as such.

That said, the U.S. government must resist emulating the tactics used by authoritarian regimes when responding to these threats. We have learned from our history that when we seek to carry out covert subterfuge to undermine democratic processes abroad, including elections, it frequently backfires, undermining our credibility and our values on the global stage.

Moreover, the measures we take to respond to malign foreign influence operations must not themselves undermine democracy. That includes ensuring the protection of free speech and privacy rights while addressing the manipulation of our information ecosystem. We should remain committed to promoting democracy abroad and supporting global actors who are working to make their governments more responsible and societies more open. U.S. foreign assistance is not – and never will be – equivalent to the covert, subversive operations run by the Kremlin and other authoritarian regimes. The U.S. government supports measures to strengthen democracy through transparent governance, anti-corruption, free and fair elections, and empowered citizen participation in all aspects of democratic society. These are the ideals we should continue to support beyond our borders, and we should be proud to defend them from false comparisons to the tools and tactics authoritarian regimes use overseas. And above all, we should be working actively to improve our own democracy at home, which will not only strengthen us as a nation but will also make our institutions and society more resilient to this threat.

The American people deserve a government that has positioned itself to do the best possible job. Treating the problem as an urgent matter of national security, putting aside partisan strife, maximizing efficiency, strategically formulating policy responses, and adhering to the values that make democracy the prevailing global ideal will enable the U.S. government to address this challenge adequately and responsibly.

A Transatlantic Threat Demands a Transatlantic Response

The United States and its European allies make up an integrated, transatlantic community. For decades, this integration through NATO and the U.S.-EU relationship has provided all member states security, material benefit, and leadership in the world. Defending against threats to our democracies therefore requires an integrated, coordinated response. Democracies will rise and fall together. Cracks in democratic institutions in one country contribute to an overall weakening of the liberal democratic order. The United States must maintain its leadership role at NATO and its strong partnership with the EU in order to strengthen the Alliance's capabilities to address asymmetric threats and work in concert with Brussels to deter malign foreign influence operations.

Both the EU and NATO have begun to address how they defend against asymmetric challenges like Russian influence operations. NATO has established Centers of Excellence that analyze components of the hybrid toolkit, while a handful of EU member states support another Center of Excellence in Helsinki, Finland that looks at the problem more holistically. Meanwhile, in Brussels, the EU's East StratCom Task Force counters Russian disinformation campaigns directly, while in April, the European Commission released a comprehensive report with policy recommendations to combat disinformation spread online.[62]

These efforts are a good start, and both organizations have made the hybrid challenge a priority. Like the United States, European nations, along with the EU, will have to do more to build resilience to cyber-attacks, combat money laundering and other forms of illicit finance from Russia and other foreign actors that ends up in the pockets of politicians and other influential Europeans. The EU should also

62 European Commission, "Communication – Tackling Online Disinformation: A European Approach," April 26, 2018, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

guard more firmly against democratic backsliding within member states, which plays into the hands of authoritarian regimes, while also increasing support for independent media, civil society, and other democratic actors in the Western Balkans and Eastern Partnership states.

We must learn lessons from each other to determine the most effective defense and deterrence measures and the most successful responses. This means better bilateral cooperation between the EU and the United States on issues like data privacy and protection, cyber hygiene, policies that address disinformation threats on social media, and transparency with the public on asymmetric threats. It also means NATO and EU member states must show a greater willingness to exchange information on new tactics that Russia and other foreign actors are deploying against us, in multi-nation formats, rather than just bilaterally between governments. The G7's recent commitment to share information and work with social media companies and internet service providers to prevent foreign interference in elections could be an impetus for more efficient transatlantic coordination to share threat information and best practices.[63] Finally, the EU and NATO, individual governments, and non-governmental organizations should combine their respective strengths and expertise and form a coalition to address malign foreign influence operations across the full asymmetric toolkit. A coalition that meets regularly and provides virtual opportunities to share open source information and analysis, and to coordinate responses in real time will enhance our collective ability to secure democracies.

The threat that foreign interference poses to democracies is not limited to the transatlantic community. Democracies around the world – from Latin America to Australia and New Zealand – are increasingly facing challenges from authoritarian governments like China and Russia. The United States and European governments should work with all of their allies and partners to defend democracies, and a public-private coalition to address malign foreign influence operations should ultimately compromise officials and experts from democratic countries worldwide, possibly utilizing existing fora, such as the Community of Democracies, where democracies gather to discuss shared challenges.

Whole of Society Approach

While the government's role is essential, the nature of these threats requires that the private sector and civil society be involved in the solution. The private sector, particularly tech companies, will have a critical role in addressing technological vulnerabilities and building resilience against malign foreign influence operations. The potential of social media companies to transform the way people around the globe interact with one another and how they access information and serve as a democratizing force is important. However, as with any new creation, these platforms have significant vulnerabilities as well as benefits – and our adversaries identified those vulnerabilities before the companies or U.S. government did, weaponizing and turning the platforms against their users in ways the companies never envisioned.

Tech companies thus far have responded slowly and without the full transparency the American people deserve to determine how Russian government operatives exploited their platforms. Much of the companies' response has seemed more focused on damage control than on transparency and a willingness to tackle the fundamental issues at hand. Self-regulation alone to try and tackle the weaponization of social media ultimately will be insufficient. Congress should take narrowly scoped, smart steps, such as the proposed Secure Elections Act or introducing legislation to have bots identified and labeled as such, to ensure that foreign actors do not use social media platforms to interfere in U.S. elections, and protect Americans' personal information online.[64] However, government should avoid overreach, and legislation will never be able to keep pace with technological change. As technologies become more sophisticated over time, the challenge to the tech sector will be even greater. The companies will need to be much more proactive in addressing

63 "Charlevoix Commitment on Defending Democracy from Foreign Threats." G7 2018 Charlevoix, June 10, 2018. https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats.

64 United States Congress, Senate, *Secure Elections Act*, S 2261, 115th Cong., 1st sess., https://www.congress.gov/bill/115th-congress/senate-bill/2261/text.

threats of abuse and misinformation on their platforms and more transparent with their users to detect and deter such activities in a timely manner.

As technology continues to evolve, tech companies should develop processes, including through engagement with outside researchers, national security experts, and civil society, to maximize the upsides of new tools and platforms and minimize the downsides before they are used more broadly, or our adversaries will continue to exploit them before we become aware of vulnerabilities. This should include developing a more constructive partnership with government and outside researchers to share information on influence operations that target their platforms. This is particularly important as malign actors seamlessly move across platforms in order to drive influence campaigns. Meaningful public-private partnerships will help overcome the trust gap that exists between Washington and the tech community and foster consensus on solutions to existing and future vulnerabilities foreign actors exploit.

Social media companies do not operate in a vacuum. In particular, their business models depend on other corporations that buy advertisements. Private companies can play their own part in demanding that tech companies address malign foreign influence operations more thoroughly by using their ad buys as leverage to force change from companies on these issues and threatening to pull their ads from platforms that do not take necessary steps, as several companies have already done. Not only would these corporations put pressure on the tech sector by diminishing the economic value of extreme and highly viral, malign content, but they would help raise awareness among society about the extent of the threat we are facing.

More broadly, American businesses are custodians of democracy, just as government and individual citizens are. Their prosperity has been built on it and benefits from it. The business community can take on a larger role as custodians of democracy by reinforcing the importance of democratic institutions among the American public, investing in civil society organizations that address the problem of foreign interference, and supporting other pillars of democratic society, like free and independent journalism. Businesses have a stake in protecting our democracy; after all, their prosperity will be directly threatened by the weakening of our institutions.

Addressing the societal vulnerabilities that the Russian government exploited is also a challenge for civil society. In the aftermath of the 2016 election, think tanks in Washington, NGOs, and researchers across the country rose to that challenge and began playing an instrumental role in monitoring and exposing disinformation campaigns and other forms of malign foreign influence in the United States, Canada, and Europe. Many of these organizations are playing a leading role in formulating policy and legislative solutions for the U.S. government and Congress, as this report seeks to accomplish.

Civil society can also step in and fulfill functions that government performs less effectively. For example, the State Department's Global Engagement Center (GEC), despite its dedicated staff, budget, and mandate, should not be the primary U.S. messenger for countering disinformation abroad. Foreign citizens already suspicious of or hostile to the U.S. government will be more open to indigenous actors. Therefore, the GEC should fund local civic organizations overseas that expose and raise awareness about foreign influence operations and counter the narratives the Kremlin and other foreign actors spread through traditional and social media. Along with USAID, it should also support independent media and local journalism in countries that are particularly susceptible to foreign disinformation and anti-U.S. narratives.

In the United States, civil society should play a prominent role in raising awareness about such threats and exposing and countering falsehoods propagated by foreign actors, while the government should fund watchdog groups conducting these activities. Across the United States, organizations are also working on building stronger curriculum for public education on the civic virtues of democracy, on developing media literacy programs to help children and adults understand how to discern disinformation in traditional and social media, and on recommending journalistic standards for reporting on weaponized information and using

social media accounts as sources. Congress and state governments should support their efforts as well.

An Urgent Call to Action to Secure Democracy

The number of foreign actors waging malign influence campaigns against the United States and its allies and partners is growing. Absent a concerted pushback by government and the other pillars of democratic society, authoritarian regimes will continue to refine their asymmetric playbook and the use of these new technologies to run more sophisticated, insidious, and far-reaching operations against democracies, making this a core national security challenge.

The adage that a strong national security starts at home has never been more true. Defending against and deterring the use of this toolkit demands urgent bipartisan action. The recommendations in this report represent common sense measures that government and lawmakers — regardless of party affiliation — and other parts of society can take. They are endorsed by the Advisory Council of the Alliance for Securing Democracy, a bipartisan and transatlantic group of former senior national security officials, and were developed in consultation with numerous experts, government officials, and civil society representatives in the United States and Europe.

IV. Recommendations for the U.S. Government

1. Articulate publicly a declaratory policy on foreign interference in democratic institutions and processes. We recommend the President issue the following statement:

> "Malign foreign interference operations designed to destabilize the elections, institutions, and societies of the United States and its allies through asymmetric means constitute a national security threat. There will be consequences for nation states that conduct these covert, corrupting, and coercive operations. The U.S. government will respond utilizing all appropriate tools."

2. Raise the cost of conducting malign influence operations against the United States and its allies. Imposing a broader set of sanctions, cyber responses, and reputational costs against individuals and organizations that support malign foreign influence operations, facilitate corruption, and prop up authoritarian regimes conducting foreign interference would not only impose costs on adversaries, but would potentially serve as a deterrent against future operations.

The Administration should:

- Employ cyber responses as appropriate to respond to cyber-attacks and deter future attacks, and consider offensive cyber operations using appropriate authorities to eliminate potential threats.

- Expand sanctions against wealthy Russian individuals and strategic industries that assist Putin's destabilizing foreign policy actions, as called for by congressional legislation. The Countering America's Adversaries Through Sanctions Act (CAATSA) calls for sanctions against a broader list of individuals and entities tied to Russia's intelligence and defense sectors. The administration, which signed CAATSA into law, should adopt a similarly tougher stance. In particular, the Department of Treasury's Office of Foreign Assets Control has the authority to target foreign persons for providing material support to already-sanctioned actors, as well as targeting foreign persons operating in Russia's energy, defense, financial, or mining sectors. Treasury's Financial Crimes Enforcement Network has the authority to target foreign financial institutions "of primary money laundering concern" operating anywhere in the world. Both of these authorities should be used to target foreign banks that help facilitate illicit Russian financial activity, whether it stems from public corruption, organized crime, or state-backed political interference.

- Impose sanctions against a wider range of individuals and entities not only inside Russia, but also inside Iran, China, and North Korea, who use ill-gotten gains to fund malign influence operations abroad.

Congress should:

- Conduct rigorous oversight of the administration's implementation of CAATSA. To date, the administration has failed to adhere to all aspects of the legislation and Congress is failing in its duty to hold the administration responsible for implementing legislation.

- Pass legislation, such as the bipartisan DETER Act, which would trigger sanctions on Russia if the Director of National Intelligence determines the Kremlin interferes in a future U.S. election, and would prohibit the purchase of Russian sovereign debt and any state-connected bonds by U.S. citizens and entities, plugging a significant loophole Russia could use to evade sanctions.

3. Separate politics from efforts to unmask and respond to operations against the U.S. electoral process. An incumbent government must be able to respond to an attack on our electoral system without being susceptible to accusations of political machinations. Political parties and campaigns should also commit to not disseminate weaponized information illegally obtained by foreign actors.

- Congress should institute mandatory reporting requirements so that an administration must inform lawmakers of attacks against U.S. electoral infrastructure, including individual political campaigns. Reporting requirements should have a low threshold, so administrations can present data to Congress and, if unclassified, to the public, without being accused of politicizing information to swing an election.

- The Democratic and Republican Parties and their candidates, along with other parties and independent candidates running for office, should pledge jointly not to weaponize hacked information during election campaigns. Without such a public, bipartisan promise, foreign state actors and cybercriminals could be emboldened to continue the activity they conducted during the 2016 presidential campaign.

- Parties, candidates, and outside political groups should also pledge to fully uphold existing legal restrictions that outlaw foreign contributions to the U.S. political system.

4) Improve election security and protect other critical infrastructure from cyber-attacks immediately. It is possible to secure our electoral infrastructure without infringing upon states' control of our elections. The federal government must make additional resources and assistance available to states to ensure that Americans know their most fundamental right is protected.

The Administration should:

- Maintain the designation of electoral systems as critical infrastructure.

- Through the U.S. Election Assistance Commission (EAC) and in coordination with the Department of Homeland Security (DHS), assist state and local election officials with conducting post-election audits of election results that provide a high level of confidence in the accuracy of vote totals, adopting cybersecurity standards for electoral infrastructure, and upgrading outdated infrastructure.

- Through the FBI and in consultation with DHS, inform state and local governments, political parties and campaigns, and companies that provide election-related infrastructure, when they have been hacked and help them respond. DHS should also ensure information is declassified quickly and appropriately to share with political parties and campaign staff, and others who may have a need to know but do not possess security clearances. The Belfer Center's Election Cyber Incident Communications Coordination Guide provides an excellent blueprint for DHS' Election Infrastructure Government Coordinating Council to manage communication on cyber-attacks with all relevant stakeholders in the electoral process.[65]

- Through the Office of the Director of National Intelligence (ODNI) and in coordination with DHS, the intelligence community should

65 "Election Cyber Incident Communications Coordination Guide," *Belfer Center for Science and International Affairs, Harvard University*, February 2018, https://www.belfercenter.org/sites/default/files/files/publication/CommunicationsGuide.pdf.

notify Congress, states, and relevant local election officials immediately of potential cyber breaches of their electoral infrastructure.

- Just as the Transportation Security Administration conducts random checks of airport screening systems, DHS should create a mechanism for simulating red team cyber-attacks on state and local electoral infrastructure. These simulations should feed into a policy process involving federal, state, and local officials that identifies and closes cyber vulnerabilities and improves responses to cyber-attacks.

- Through DHS, build a national classified cyber information-sharing network that appropriately cleared personnel of private companies maintaining the nation's critical infrastructure can access, in accordance with the steps outlined in a Council on Foreign Relations report.[66]

Congress should:

- Adopt legislation, such as the Secure Elections Act, to improve information sharing throughout government on election cybersecurity threats; provide technical resources for election agencies; and improve information sharing between the federal, state, and local levels.[67]

- Enact requirements for the federal government to notify states and relevant local election officials of intrusions into electoral infrastructure, and for the Executive Branch to notify Congress — both in a timely manner. Legislation should also require private vendors and operators of electoral infrastructure to report cybersecurity incidents that could impact the integrity of voting systems and databases to the FBI and DHS.

- Require DHS to issue security clearances to senior state government officials in charge of securing electoral infrastructure in order to facilitate access to information on threats.

- Codify into law the designation of electoral systems as critical infrastructure.

- Prioritize federal funding for cybersecurity research and development.

- Pass legislation to elevate the DHS National Protection and Programs Directorate into a full-fledged operational agency under DHS jurisdiction; one bill has already been introduced and is being considered by Congress.[68] The agency should facilitate improved coordination across government on responses to cyber threats to all 16 critical infrastructure sectors.

State and local governments should:

- Accept federal assistance on election security. While it is not a federal government competency to run elections, states lack the resources and expertise that the federal government possesses on cyber threats to critical infrastructure.

- Comply with EAC's voluntary voting system guidelines and the National Institute of Standards and Technology's cybersecurity framework for critical infrastructure.

- Make mandatory the use of electronic voting machines that issue a voter verified paper ballot, and the conduction of post-election audits of paper voting records to corroborate electronic results.

- Conduct an audit and threat analysis of voter registration systems, and upgrade systems as necessary, as recommended in a Brennan Center for Justice report.[69]

66 Robert K. Knake, "Sharing Classified Cyber Threat Information With the Private Sector," *Council on Foreign Relations, May 15, 2018*, https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector.

67 United States Congress, Senate, *Secure Elections Act, S 2261, 115th Cong. 1st sess.* https://www.congress.gov/bill/115th-congress/senate-bill/2261/text.

68 United States Congress, House, *Cybersecurity and Infrastructure Security Agency Act of 2017, HR 3359, 115th Cong. 1st sess.* https://www.congress.gov/bill/115th-congress/house-bill/3359/text

69 Lawrence Norden and Ian Vandewalker, "Securing Elections from Foreign Interference," *Brennan Center for Justice, New York University School of Law, June 29, 2017*, https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference.pdf.

5) Appoint a Foreign Interference Coordinator at the National Security Council and establish a National Hybrid Threat Center at the Office of the Director of National Intelligence. The Coordinator and Threat Center would direct policy formulation and intelligence analysis respectively on the range of asymmetric tools and interference operations designed to destabilize the United States and its allies. A policy decision should be made to elevate foreign interference on the list of intelligence collection and analytical priorities, with responsibility for intelligence coordination residing in the Hybrid Threat Center. The President, Congress, and the American people should have confidence in the intelligence community's sources of information that corroborate an interference operation and an adversary's intent to undermine U.S. democracy.

NSC Foreign Interference Coordinator

- We recommend the President appoint a Foreign Interference Coordinator at the National Security Council (NSC) because the NSC is responsible for coordinating among the many individual agencies that handle a subset of these issues (DOD, State, Treasury, DHS, and others).
- The Coordinator should have sufficient staff from the interagency and be given the authority to coordinate across the NSC and to task agencies on policy and intelligence collection priorities on foreign interference. The Coordinator would be the primary U.S. government official in charge of presenting policy options to the President to address malign foreign influence operations, and for coordinating with allies and partners on these issues.
- To give the Coordinator significant standing in the interagency, the President should appoint a former senior U.S. official — ideally a former Cabinet-level official or former Member of Congress — to the position. This official should ideally be a Deputy Assistant to the President and report directly to the National Security Adviser and through him or her to the President.
- The Coordinator would be responsible for working with Congress to ensure the proper laws, regulations, and authorities are in place to deter and respond to asymmetric attacks.
- The Coordinator and his/her staff should establish strong ties with the private sector — tech companies, financial institutions, and corporations that manage critical infrastructure — and civil society organizations to cultivate an effective working relationship with non-government actors to address various types of asymmetric threats.

Hybrid Threat Center at the Office of the Director of National Intelligence (ODNI)

- The Hybrid Threat Center at ODNI should bring together experts from across the intelligence community who are tracking individual elements of the asymmetric toolkit. Policymakers need to be informed of how foreign adversaries use the various tools in tandem; the Threat Center would ensure experts on cyber, finance, economics, disinformation, leadership, and regional affairs are working in unison to assess influence operations holistically.
- The Hybrid Threat Center should also track influence operations domestically and overseas against the United States and its allies. When possible, it should make information available to the public regarding trends, threats, and tactics deployed by authoritarian adversaries. It would supplant existing task forces at individual agencies, whose mandates and resources are limited by their particular mission and budget. For example, the FBI's foreign influence task force is bound by the FBI's criminal and counterintelligence mandates within the United States. Combining these functions into a center that also has responsibility for overseas collection would give the intelligence community and policymakers greater visibility into nebulous, cross-border operations. The intelligence community and Congress should work together to resolve the existing legal limitations on parts of the intelligence community to monitor disinformation operations. The intelligence community and

Congress should ensure the appropriate legal authorities are in place to protect the privacy and civil liberties of U.S. citizens. The very fact that it is often difficult to distinguish the sources and origins of operations and individual accounts necessitates strict congressional oversight and appropriate authorities to ensure intelligence agencies have the information necessary to protect the homeland while protecting American's privacy rights. Lessons learned from post-9/11 counterterrorism experiences should be applied to the foreign interference threat. Congress should legislate reporting requirements for the Threat Center to report on its activities and implications for privacy and civil liberties.

- The Hybrid Threat Center should allocate significant resources to monitoring open source information, particularly on social media, to analyze disinformation campaigns and the weaponization of information and ensure that open source intelligence is given the appropriate weight in analytic products.

- The Hybrid Threat Center should also monitor technological trends, particularly important in cyber and disinformation, so policymakers can adapt the government's responses accordingly.

6. Close loopholes that allow foreign actors to unduly influence our political system. Foreign actors exploit existing laws and regulations to move money into the United States that can ultimately affect the American political system. There are several measures the administration and Congress can take to update regulations and pass legislative solutions to close off illicit finance and covert political influence from abroad.

The Administration should:

- Track flows of international funds transfers to, from, or through the United States by creating a centralized database at the Department of Treasury of all international funds transfers that transit the country. Large U.S. banks that clear dollars for international payments would report the data on a near real-time basis. The reporting streams could then be combined, providing a complete view of U.S. dollar transactional activity. The idea has been studied by Treasury but never finalized, although Canada and Australia collect similar information. While international funds transfer records are available on an ad hoc basis, only a centralized database would drive the type of powerful analysis that is necessary. Over time, payments data could be married up with securities trade data collected under a new system called the Consolidated Audit Trail that is currently being put in place by the Securities and Exchange Commission; shipping data collected by Customs and Border Patrol; and other information sources that would facilitate illicit finance network analysis.

- Require title insurance companies to report to Treasury the beneficial owners of legal entities used to purchase any residential or commercial property nationwide. This would provide a defense against foreign buyers who purchase a house, condo, or commercial property in the United States without forming a U.S. company or opening a U.S. bank account. A temporary Treasury order now requires purchasers of high-end residential real estate in select cities to report identifying information and has detected a great deal of suspicious activity, but the order is neither comprehensive nor permanent.

- Use existing civil and criminal penalties to punish financial institutions and their employees involved in illicit financial activity, including for violations of sanctions or violations of money laundering statutes. Money laundered into the United States is also potentially subject to criminal or civil asset forfeiture.

Congress should:

- Pass legislation, such as Honest Ads Act, to improve disclosure requirements for online political advertisements so that Americans understand who is funding political ads they see online. Furthermore, as recommend in a report[70] by the Brennan Center for Justice,

70 Ian Vandewalker and Lawrence Norden, "Getting Foreign Funds Out of America's Elections," *Brennan Center for Justice, April 6, 2018*, https://www.brennancenter.org/publication/getting-foreign-funds-out-americas-elections.

Congress should also: Ensure through legislation that the source information explaining the origins of online political ads remains attached to posts when those ads are shared on social media; and mandate that social media companies selling political ads use the credit card industry's address verification system to determine whether an ad buyer has a U.S. billing address.

- Pass legislation to have bots identified and labeled.

- Reform the Foreign Agents Registration Act (FARA) so all agents of foreign governments are appropriately registered in the United States. There are a number of bills introduced by Members of Congress on both sides of the aisle that Congress should consider. [71]

- Establish a beneficial ownership regime for company formation. Passing a law requiring beneficial ownership reporting at the time of company formation, such as this recent House bill, is essential.[72] Importantly, it enjoys the support of the financial services industry.[73]

- Expand the jurisdiction of the Committee on Foreign Investment in the United States' (CFIUS) and provide it additional resources. CFIUS, an interagency body responsible for reviewing inbound foreign investment for national security risks, should be permitted to review a broader range of transactions, particularly in critical technology, artificial intelligence, and the media sector, and from countries that pose national security risks, such as Russia and China.

7. Increase assistance to allies and partners to ensure they have the ability to withstand and respond to attempts to undermine their democratic institutions. Due to historical and cultural ties and resource dependencies, some European nations are particularly vulnerable to Russian asymmetric campaigns. Others are complicit in facilitating illicit financial flows. U.S. allies and partners in Asia are also increasingly vulnerable to Chinese influence operations. The United States must utilize various forms of assistance to strengthen allies and partners' democratic institutions, governments, and societies. The U.S. government should also institutionalize more regular coordination with European allies and partners to address the threat of foreign interference, and should work with democracies in Asia to better understand the threats they face from Chinese interference, help them withstand that challenge, and learn lessons from other countries' experiences.

- The administration should utilize effectively the increase in U.S. foreign assistance to European and Eurasian states that Congress has mandated, particularly through CAATSA. This assistance should be used to build democratic resilience throughout the region and increase societal resistance to the Kremlin's tactics, such as its support for political and social groups and its use of disinformation to exacerbate existing social divisions.

- Congress and the administration should ensure that they appropriate and use sufficient resources to strengthen democratic institutions and civil society in allied and partner countries in order to combat Russian, Chinese, and other forms of malign foreign influence operations.

- The administration should help our European allies and partners reduce energy dependence on Russia by continuing to press key European governments to oppose the Nord Stream 2 pipeline project.

71 United States Congress, House, *Disclosing Foreign Influence Act*, HR 4170, 115th Cong., 2nd sess., introduced in House October 31, 2017, https://www.congress.gov/bill/115th-congress/house-bill/4170/text; United States Congress, House, *Foreign Banker Reform Act of 2018*, HR 5335, 115th Cong., 2nd sess., introduced in House March 19, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5335/text; United States Congress, House, *Foreign Influence Transparency Act*, HR 5336, 115th Cong., 2nd sess., introduced in House March 20, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5336/text; United States Congress, Senate, *Disclosing Foreign Influence Act*, S 2039, 115th Cong., 1st sess., introduced in Senate October 31, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/2039/text; United States Congress, Senate, *Foreign Agent Lobbying Transparency Enforcement Act*, S 3479, 115th Cong., 1st sess., introduced in Senate July 31, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1679/text; United States Congress, Senate, *Foreign Agents Registration Amendments Act of 2018*, S 2482, 115th Cong., 2nd sess., introduced in Senate March 1, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2482/text; United States Congress, Senate, *Foreign Agents Registration Modernization and Enforcement Act*, S 625, 115th Cong., 1st sess., introduced in Senate March 14, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/625/text; United States Congress, Senate, *Foreign Influence Transparency Act*, S 3583, 115th Cong., 2nd sess., introduced in Senate March 21, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2583/text.

72 United States Congress, House, *Counter Terrorism and Illicit Finance Act*, HR 6068, 115th Cong. 2nd sess., introduced in House June 12, 2018 https://www.congress.gov/115/bills/hr6068/BILLS-115hr6068ih.pdf

73 The Clearing House Association et al., "To Representatives Pearce and Luetkemeyer," January 4, 2018, https://www.sifma.org/wp-content/uploads/2018/02/Counter-Terrorism-and-Illicit-Finance-Act.pdf.

- The administration and Congress should reduce European energy dependence on Russia by updating the regulations that allow U.S. companies to export liquefied natural gas (LNG) to Europe to make the process faster and more flexible while maintaining environmental safeguards.

- The Department of Treasury should establish a program to provide technical assistance to countries, like Latvia, seeking to strengthen their ability to combat illicit finance.

- The Departments of State and Treasury should increase diplomatic efforts to convince countries of key concern in facilitating illicit finance, such as Cyprus, to implement critical reforms. Incentives could include additional U.S. foreign investment, extended technical assistance, and support for the re-establishment of direct correspondent banking ties.

- The U.S. government should work with European allies and partners to establish a transatlantic coalition on defending democracies.

- The United States should increase efforts with partners, including Europe, Taiwan, Japan, Australia, South Korea, and India to provide alternatives to China's Belt and Road Initiative.

8. Contribute to efforts to building societal resilience to foreign interference in the United States and abroad. Government should help raise awareness about the threat of foreign interference, as exposure is one of the most effective means to combat foreign interference operations. However, it should also seek partners who can combat foreign disinformation and effectively message to American and foreign audiences, and who are devoted to strengthening democratic values worldwide. This is as important domestically as it is overseas. Thirty years ago in his farewell address to the nation, President Reagan expressed concern about "an erosion of the American spirit" and called on Americans to focus more attention on "American history and a greater emphasis on civic ritual."[74] This challenge is even greater today.

- Congress and the Executive Branch should endorse the work of civil society and private sector groups promoting civics education and media literacy programs in the United States and authorize the Department of Education to work with state governments that establish statewide civics and media literacy programs.

- The Department of State's Global Engagement Center and Office of the Coordinator of U.S. Assistance to Europe and Eurasia, together with USAID, should support civil society organizations in Europe that track and counter foreign disinformation. Similar partnerships should be developed to more effectively track growing Chinese influence operations.

- DHS or the White House, through the proposed NSC Foreign Interference Coordinator, should implement a Public Service Announcement (PSA) campaign that promotes smart cyber behavior and raises awareness about various types of foreign interference affecting U.S. citizens, businesses, and institutions. The federal government has had PSA campaigns on a myriad of issues, from quitting smoking to stopping pollution. Threats of foreign interference that affect all Americans should receive similar treatment.

9. Ensure that data privacy laws protect U.S. citizens' personal information on social media platforms. It is increasingly apparent that the United States needs a legal framework for protecting U.S. citizens' data, given repeated breaches, privacy concerns, and acquisition by foreign adversarial governments. Lawmakers and tech companies will have to find a balance between European-style regulation that potentially stifles innovation and a regulatory framework that protects data privacy and allows free enterprise to thrive.

V. Recommendations for the European Union and NATO

1. Establish an International Coalition on Defending Democracies. European governments, together with the United States, Canada, EU, NATO, and Five Eye allies Australia and New Zealand, should establish a forum for sharing information

74 Ronald Reagan, "Farewell Address to the Nation," *The American Presidency Project, January 11, 1989*, http://www.presidency.ucsb.edu/ws/?pid=29650.

and analysis, exchanging best practices, and coordinating policy and programmatic responses to defend democracies from malign foreign influence operations. Coordination between governments is currently taking place on an ad hoc basis, and tends to be stovepiped by each element of the toolkit — cyber experts conduct exchanges, as do experts on disinformation and strategic communication. What the transatlantic community needs is regular contact between governments assessing the entirety of the asymmetric toolkit holistically, so governments and international organizations can prepare more effective responses. There should also be a formalized Track II channel for non-government representatives and organizations to enter into a dialogue with government officials on policy solutions. Such a channel could be particularly important for the public and private sectors to exchange best practices and lessons learned on data privacy and cyber issues with a view towards developing norms that could be adopted by governments. The coalition should eventually incorporate governments and experts from democracies worldwide, as transatlantic countries can learn much about the experiences of democracies in Asia, Latin America, and elsewhere.

2. Strengthen the sanctions regime to match measures taken by the U.S. government. The Kremlin is counting on European fatigue toward the existing sanctions regime. The best way to demonstrate that the EU takes Russian government efforts to destabilize the transatlantic community seriously is for member states to agree on additional sanctions on Russian individuals and entities that complement the recent sanctions imposed by the U.S. government. The EU should also extend the six-month review period for sanctions to 12 months, reducing the opportunities for member states to break consensus in Brussels. It is essential that the Trump administration and European governments do not remove sanctions or reduce diplomatic pressure on the Putin regime until Russia ceases its malign activities in Ukraine and the rest of Europe as well as the United States. Imposing other reputational costs, such as halting rapprochement with Russia or implementing the European Commission's recent recommendation for member states to improve their capabilities to publicly attribute cyber-attacks, should also be part of Europe's strategy to increase deterrence and raise costs on adversaries.[75]

3. Institute a Joint NATO-EU Task Force on Countering Asymmetric Threats. At the 2016 Warsaw Summit, NATO and the EU agreed to enhance their cooperation on hybrid and cyber threats, relying on their respective military and non-military strengths and capabilities to complement each other's efforts. The upcoming NATO summit in Brussels in July 2018 will likely produce more concrete actions on hybrid threats for the Alliance, while the European Commission, drawing partly on the work of the High Level Expert Group on Fake News and Online Disinformation, has issued recommendations on combatting disinformation online.[76] These are welcome steps. However, at the moment, each organization has disparate elements that monitor aspects of the Russian toolkit, but are not all well-funded or in synch with one another's efforts. A Joint Task Force could better coordinate these various efforts, and would also serve as an important mechanism to keep the United Kingdom integrated in European efforts to strengthen common defenses against asymmetric threats post-Brexit. It should perform the following functions:

- Conduct joint analysis of threats, both at the working level and at the North Atlantic Council, as well as exchanges of technical expertise between the relevant bodies within the EU and NATO, including cyber threats to EU and NATO member state networks. This would require a mechanism for sharing classified information, which currently does not exist between the two organizations. On threats of this magnitude, there should be a medium for NATO Allies and EU partners to exchange threat information.

75 "Joint Communication to the European Parliament, the European Council and the Council: Increasing Resilience And Bolstering Capabilities to Address Hybrid Threats," *European Commission, June 13, 2018*, https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.

76 "Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling Online Disinformation: A European Approach," *European Commission, April 26, 2018*, https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach.

- Coordinate the various lines of effort on hybrid threats, particularly on disinformation and cybersecurity, conducted by the Centers of Excellence at NATO, the East StratCom Task Force at the EU, the European Centre of Excellence for Countering Hybrid Threats in Helsinki, the High Level Experts Group on Fake News and Online Disinformation, and other parts of the EU bureaucracy.

- Monitor disinformation campaigns on social media and in traditional media that seek to undermine the organizations or destabilize a member state, and coordinate responses, as appropriate.

- Develop norms of behavior for cyberspace that would guide NATO and EU member states' own actions, as well as their responses to cyber threats. This could serve as a model for global cyber norms.

- Deploy personnel at the request of member states for assistance in defending against, deterring, or responding to a malign foreign influence operation.

- Bolster public outreach by communicating to the European public within member states and within aspirant countries. NATO and the EU can jointly advocate for the benefits of the transatlantic community and why it represents a superior alternative to the geopolitical orientation and form of government proposed by authoritarian regimes like Russia.

4. Shut down channels for money laundering and other forms of illicit finance. The Russian government exploits lax regulations and corrupt banking practices to move money into Europe and peddle political influence. Just like the United States, Europe too needs to close these loopholes.

- Establish an EU central body to combat money laundering. This central body should have the authority to examine banks, impose fines, revoke licenses, and/or restrict operations of financial institutions without needing to wait for national authorities of a member state to submit a recommendation.

- The European Central Bank (ECB) should apply its existing authorities — including prudential supervision, approval of purchases of "qualified holdings" in banks, and fit and proper review — to illicit finance matters when there is reason to believe that there may be ongoing anti-money laundering violations.

- The EU should explore how to better utilize euro payments data, either via TARGET2 (the leading European platform for processing large-value payments, used by central banks and commercial banks to process euro payments in real time) or at the national level, to detect illicit financial activity and use such information as the basis for targeted reviews or referrals to regulators and law enforcement agencies.

- EU member states should continue to enhance information sharing to combat illicit financial activity, as it is planning to do under the Fifth Anti-Money Laundering Directive. By more robustly sharing transactional data, supervisory information, law enforcement information, and classified intelligence across borders, member states will achieve better results in detecting and disrupting the activity of illicit financial facilitators who operate across member states' borders.

- The European Commission should review current passporting arrangements[77] and consider whether adjustments would be appropriate to prevent the evasion of appropriate supervisory oversight.

5. Support the pillars of democratic society within EU member states and in the surrounding neighborhood. An important way to prevent democratic backsliding in Europe – and buttress resilience to authoritarian regimes' attempts to destabilize the transatlantic community – is to strengthen civil society and free and independent media. The EU should:

77 According to Investopedia, "Passporting is the exercise of the right for a firm registered in the European Economic Area (EEA) to do business in any other EEA state without needing further authorization in each country."

- Maintain pressure on EU member states to uphold European democratic values, such as allowing a free and independent press to flourish, keeping the judiciary independent from political influence, and supporting civil society.

- Increase funding for NGOs that monitor and expose disinformation campaigns and corruption, particularly in vulnerable regions like the Western Balkans.

- Support programs that strengthen free and independent media, particularly in countries that aspire to join the EU but are susceptible to Russian disinformation and destabilization operations (e.g., Serbia, Bosnia and Herzegovina, Kosovo, Montenegro, Ukraine, and Georgia). Pro-Kremlin narratives easily spread through local media outlets through Russian state-sponsored news agencies RT and Sputnik. Only by supporting homegrown journalism can local media outlets report objectively on a broad range of issues without having to rely on Russian propaganda for content.

VI. Recommendations for the Private Sector

1. Be more transparent about their technology, business models, and how platforms can be manipulated. The tech sector has reluctantly and belatedly released information to Congress and the public about the manipulation of social media platforms to undermine democracy, but there are several steps tech companies should take to be more transparent:

- Design platforms so that they provide explanations for users about how and why content appears for them, and make those explanations easy to understand for the public. The companies should also explain what they are doing to refine algorithms and counter efforts to exploit them.

- Make more accessible company policies that determine how user data is collected, and make privacy controls easier for users so they can consent or prevent their information from being collected, including by malevolent foreign actors.

- Facilitate third-party research into disinformation campaigns on and across social media platforms. Most social media platforms make it difficult for researchers to analyze data trends, because their application programming interfaces (APIs) are closed to the general public. While tech companies are engaging in a broader discussion about their policies and technologies in a limited way, they need to remove the blindfold and allow researchers to look at the data, ensure accountability in the tech sector, and recommend cross-platform solutions to prevent the distortion of information online.

- The tech companies should ensure they first involve legal and data protection experts, who can make clear to the public what should and should not be shared with outside experts.

2. Create mechanisms for collaboration on defending against disinformation and cyber-attacks. Many disinformation campaigns and cyber threats do not just manipulate one platform; the information moves across various platforms or a cyber-attack threatens multiple companies' network security and data integrity. There must be greater cooperation within the tech sector and between the tech sector and other stakeholders to address these issues.

- As recommended in a NYU Stern Center report, tech companies should conduct across-the-board internal assessments of disinformation threats. [78] The tech companies are too large for any one individual or department to have the answers. Bringing together engineers, business leads, customer support, legal, trust and safety teams, and policy experts from across the company should lead to changes that protect users and weed out harmful content.

78 "Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," *Stern Center for Business and Human Rights, New York University, November 3, 2017*, http://www.stern.nyu.edu/experience-stern/faculty-research/harmful-content-role-internet-platform-companies-fighting-terrorist-incitement-and-politically.

- Policy changes within individual companies are a meaningful start, but sufficiently addressing these cross-platform threats will require multiple stakeholders. Therefore, all relevant tech companies should participate in a collaborative forum for sharing analysis and solutions to combat disinformation and cyber-attacks. Models for cooperation already exist and can be developed further: Google, Facebook, Twitter, and Microsoft already maintain a common database of digital fingerprints identifying violent extremist videos.[79] These four companies also participate in a Cyberhate Problem-Solving Lab run by the Anti-Defamation League's Center for Technology and Society.[80] Dozens of tech companies participate in the Global Network Initiative, a tech policy forum devoted to protecting digital rights globally.

3. Build a more constructive public-private partnership, particularly to identify emerging technological threats. It is imperative that the tech sector and government develop a more constructive partnership. New technologies, such as "deep fake" audio and video doctoring, will make the next wave of disinformation even harder to detect and deter.

- The tech sector and national security professionals should work together to identify potential vulnerabilities in new and existing technologies that can be exploited by adversaries, and strengthen defenses and deterrence measures. The two sectors should also establish a mechanism to share data to identify nefarious actors on social media platforms linked to foreign nation states, while ensuring protection of Americans' privacy and free speech.

- The data exchanged between the government and tech sector should also be briefed to Congress and made available to the public to maximize transparency.

- There needs to be more funding for research of new technologies and their potential misuse for disinformation. The Pentagon's Defense Advanced Research Projects Agency (DARPA)'s own research on identifying deep fakes, combined with grants it has awarded outside researchers, is a positive development.[81]

- As recommended by Brookings Institution experts, the public and private sectors need to be working together to assess the responsible design and use of decentralized applications, which utilize blockchain technology and other peer-to-peer tools.[82]

4. Enact clear guidelines for verifying users and content and taking down accounts and content that violate Terms of Service (TOS). While some European governments have taken steps to regulate content on social media, the protection of free speech, enshrined in the First Amendment, is paramount in the United States. Companies bear a heavy responsibility to ensure that their platforms are not abused or used as tools to spread the type of disinformation intended to undermine either individual rights or democratic institutions. While European-style regulation may not be the answer in the United States, the companies must take action on harmful content consistent with their TOS. For example, some of Facebook and Twitter's new requirements for political ad purchasers to verify their identity are a good step, though have faced challenges in implementation.[83] The platforms face real difficulties in managing an enormous volume of organic content and an environment where malicious users and accounts linked to nation-state malign influence operations or authoritarian regimes thrive. These bad actors can flood the system with illegitimate TOS complaints, hoping the content or accounts they disapprove of will simply be pulled without deliberation. A combination of human and algorithmic review

79 "Partnership to Help Curb Spread of Online Terrorist Content," *Facebook Newsroom*, December 5, 2016, https://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content.

80 "Facebook, Google, Microsoft, Twitter, and ADL Announce Lab to Engineer New Solutions to Stop Cyberhate," *Anti-Defamation League*, October 10, 2017, https://www.adl.org/news/press-releases/facebook-google-microsoft-twitter-and-adl-announce-lab-to-engineer-new.

81 Taylor Hatmaker, "DARPA Is Funding New Tech That Can Identify Manipulated Videos and 'Deepfakes,'" *Tech Crunch*, April 30, 2018, https://techcrunch.com/2018/04/30/deepfakes-fake-videos-darpa-sri-international-media-forensics.

82 Chris Meserole and Alina Polyakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018, http://foreignpolicy.com/2018/05/25/disinformation-wars.

83 Mark Glaser, "Facebook's Political Ad Disclosures Are a Train Wreck in Progress," *Digital Content Next*, June 7, 2018, https://digitalcontentnext.org/blog/2018/06/07/facebooks-political-ad-disclosures-a-train-wreck.

must be in place to monitor content and accounts. Social media companies should take the following steps:

- Devote more human resources to auditing complaints regarding TOS violations and develop clearer, more rigorous guidelines for removing content while protecting free speech.
- To the best of their ability, more clearly articulate to users the reasons why they removed users' content or blocked their account, and allow for users to appeal the decision.[84]
- Consider ways to amplify verified content and marginalize suspicious content.
- Continue to refine AI tools that can spot bot accounts that are manipulating social media platforms. Many bot accounts are benign or beneficial, such as those that issue Amber Alerts and other public service announcements. Legislation that mandates that bots be identified and labeled will help provide transparency, as will adding additional human resources to managing this challenge. However, the sheer volume of bot accounts makes the use of AI essential. The foreign interference challenge cannot be successfully addressed solely through the hiring of additional personnel.
- Platforms must also permit authenticated accounts operated by human beings to remain publicly anonymous. Maintaining anonymity is important not only for users who wish to have a greater degree of privacy, but also for activists and political opposition figures in authoritarian states.

5. Examine the implications of the business model that underpins these companies. The ad-driven, engagement-focused revenue stream adopted by the major social media companies has also created a medium for malicious actors, like the Internet Research Agency in St. Petersburg, to exploit. Although platforms like Facebook and YouTube have taken some steps to address this, with Facebook requiring disclosures of political ads and YouTube promising to improve algorithms to keep advertisers' ads away from harmful content and vowing to remove more offensive videos, a broader discussion on disentangling advertising from data collection is worth having.[85] Less individualized, more contextual advertising like we see on other media — TV and print, for example — may make it more difficult for nefarious actors to target specific segments of the population with harmful content (violent extremists and terrorists) or falsified content for political purposes (nation-state actors). A report by New America's Public Interest Technology program offers some guiding principles for thinking through this challenge.[86]

6. Invest more in civil society's efforts to combat foreign influence operations. American businesses are custodians of democracy, just as government and individual citizens are. Their prosperity has been built on it and benefits from it, and they should play a role in protecting it from foreign interference.

Corporations that have philanthropic arms, as well as private foundations, should be more involved in defending against foreign actors' attempts to destabilize democracies. Investing in organizations that run media literacy campaigns, expose disinformation and corruption, and conduct free and independent journalism, particularly on the local level, should be a priority for corporations and philanthropists.

84 Erica Newland et al., "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users," *The Berkman Center for Internet & Society and The Center for Democracy & Technology, September 2011*, https://www.cdt.org/files/pdfs/Report_on_Account_Deactivation_and_Content_Removal.pdf.

85 "Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," *Stern Center for Business and Human Rights, New York University, p. 27, November 3, 2017*, http://www.stern.nyu.edu/experience-stern/faculty-research/harmful-content-role-internet-platform-companies-fighting-terrorist-incitement-and-politically.

86 Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," *New America, January 23, 2018*, https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit.

VII. Recommendations for Media Organizations[87]

1. Confirm the veracity of leaked information and be judicious about using it. Hacking operations by states and non-state actors are now a feature of political life in the democratic world. But the actors behind the hacks have an agenda, and that agenda can be enabled if media are not careful about how they report the story. The illegally-obtained information that nefarious actors steal and WikiLeaks and others publish can only be weaponized successfully if journalists publicize the contents of the hacks. Even after the 2016 experience with the DNC and John Podesta's hacked emails, reporters continue to traffic in material hacked by foreign actors, as recently shown in the Qatari-Emirati influence feud.[88] To report responsibly on weaponized information, journalists should:

- Distinguish between reporting on hacking operations and reporting on the content of the leaked information. During the 2017 presidential campaign in France, French journalists covered the story of the hack of then-candidate Emmanuel Macron's campaign e-mails and the online data dump. However, to prevent amplifying potentially falsified information and to avoid being a part of politicizing the operation, they refrained from reporting on the content of the data. Contrast that approach to U.S. media's reporting on the hacking and data dump of DNC and Clinton campaign e-mail accounts, which injected a foreign state's political agenda into an already hyper-politicized environment.

- Verify any information before it is published and contextualize in reporting both how it was obtained and the motivations behind the hack.

2. Create guidelines for using social media accounts as sources in stories. Looking ahead to future elections, media organizations can implement the following guidelines for using social media sources:

- Use two-step verification of social media accounts before publishing information. First, ensure that the social media platform has verified the account. And second, establish contact with the user on the phone. Written contact via direct message or e-mail is insufficient to establish the authenticity of a user account. Unverified social media accounts should require additional investigation to identify the account user.

- Cite verified social media posts more responsibly by quoting them rather than embedding them. Furthermore, when embedding a tweet, consider cutting out the part that shows replies, retweets, and favorites. This avoids providing a potentially inaccurate snapshot of an account's popularity or legitimization of the information due to the account's alleged popularity. For example, the IRA frequently used bots to make these accounts appear more popular than they otherwise would have been. Media organizations used information from falsified accounts operated by the Russian government and embedded their tweets in the articles, showing readers that the accounts had a popularity, reach, and significance they did not deserve.[89][90]

3. Build story literacy, particularly for complex, rapidly developing pieces of news. Throughout journalistic history, there have always been stories with many players, parts, and subtexts. But considering today's 24/7 media environment, the overwhelming volume of information an audience can consume, and the fact that many people do not follow a story from start to finish, reporters need to go to greater lengths to synthesize material.

87 The recommendations in this section are largely derived from the following report:

Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information," *Alliance for Securing Democracy, German Marshall Fund of the United States, March 23, 2018*, http://securingdemocracy.gmfus.org/publications/responsible-reporting-age-irresponsible-information. Heidi Tworek is a non-resident fellow at the German Marshall Fund of the United States.

88 United States District Court, Central District of California, Western Division, "Broidy Capital Management LLC, Elliott Broidy, and Robin Rosenzweig v. State of Qatar, Stonington Strategies LLC, Nicolas D. Muzin, and Does 1-10," March 26, 2018, https://www.documentcloud.org/documents/4451449-Broidysuit.html.

89 Josephine Lukito and Chris Wells, "Most Major Outlets Have Used Russian Tweets As Sources For Partisan Opinion: Study," *Columbia Journalism Review, March 8, 2018*, https://www.cjr.org/analysis/tweets-russia-news.php.

90 Donie O'Sullivan, "American Media Keeps Falling for Russian Trolls," *CNNTech, June 21, 2018*, http://money.cnn.com/2018/06/21/technology/american-media-russian-trolls/index.html.

Summarizing and repeating information as stories evolve can help an audience digest them. Some tools we suggest are:

- Using timelines and network diagrams to map out key players and events in multilayered stories.
- Create a dedicated vertical to a theme that encompasses many high-profile and breaking articles, such as Russian interference in democracies. This would put all relevant stories in one location for users to find information.
- Break down complicated stories by using Q&As and explainer cards.

4. Increase transparency in reporting practice and reporting procedure. In an era of heightened suspicion towards the press, greater transparency can help the public better understand how journalism works and why journalists report what they do. Media organizations could consider taking the following steps:

- Participate in The Trust Project, a new initiative that is developing transparency standards for news consumers to assess the quality and credibility of journalism. Journalists would explain why they wrote a particular story, sources they used, previous versions of the story, etc.
- Require freelancers to disclose their sources of funding and any possible conflicts of interest. This will help prevent manipulation of freelancers and could weed out fake freelancers.
- Write stories about journalistic procedure. In other words, explain to the public how journalists do their jobs. Entire TV series have been devoted to shedding light on a profession. Public interest stories on a reporter's approach to a particular story or source could generate interest in the news outlet while simultaneously increasing transparency.

5. Anticipate future problems in journalism today. Today's disinformation campaign may not look like tomorrow's threat. The technology that is used by millions of people around the world – and exploited by a handful of state and non-state actors – will continue to evolve rapidly. Leaked and weaponized information will change over time. Campaigns did not have to worry about their e-mails being dumped onto WikiLeaks over a decade ago. Now they do. Media organizations need to stay on top of emerging trends, tools, and threats to get ahead of future challenges rather than having to issue corrections that undermine their credibility after the fact.

- Assign responsibility for disinformation and emerging threats to a C-level executive within the news organization. The executive would be in charge of finding solutions to verify potentially falsified information.
- Create a regular schedule for revisiting and updating social media verification guidelines.
- Follow BuzzFeed's lead and assign a beat reporter to cover disinformation trends and technologies to keep its audience updated on the latest developments.

VIII. Recommendations for Civil Society

1. Extend the dialogue about foreign interference in democracies beyond Washington. In several European countries, governments and non-governmental organizations are leading outreach about Russian active measures beyond their capitals in order to build societal resilience. For example, the Swedish government distributed pamphlets to 4.7 million households explaining how to prepare for war or other national crises, including cyber-attacks on national infrastructure.[91] Estonia and other governments' intelligence agencies publish annual threat assessments for public consumption. The U.S. government can conduct similar PSA campaigns, but in the United States, non-governmental organizations will be better positioned than government to fulfill different types of resilience building functions. Civil society therefore needs to be more active outside the Beltway in raising awareness, depoliticizing the debate about addressing this threat, and getting buy-in for solutions.

91 "Sweden Sends Out Leaflets on How To Prepare for War," *BBC News, May 22, 2018*, https://www.bbc.com/news/world-europe-44208921.

- Think tanks traditionally provide analysis and recommendations to decision-makers in the government. They should also advocate and act. Domestic outreach programs that bring policy experts in the think tank community in contact with their fellow Americans can be mutually beneficial. Outreach across the United States can accomplish the following: Steer this conversation away from its politicized roots in the 2016 elections and toward the broader threat that malign foreign influence operations pose to our democratic institutions; Educate fellow citizens on the seriousness and urgency of solving the problem and on the ways their lives are affected by it; Identify trusted voices among local publics, officials, businesses, and civic leaders to participate in crafting solutions on the federal, state, and local levels.

- Non-governmental organizations should advance media literacy across the country to give Americans the tools they need to distinguish fact from fiction. Several European countries — Sweden, The Netherlands, Germany, and the Czech Republic, among others — have robust media literacy programs run by NGOs and, in Sweden's case, government agencies. These programs train educators, parents, and students in best practices for critical consumption of media, and develop materials for school curricula. There are American NGOs like the News Literacy Project already dedicated to working on media literacy. Other organizations, like many of Washington's think tanks, have networks throughout the country and in Europe to leverage, including in countries that have had success in promoting media literacy. NGOs should partner together to: Conduct trainings for the public, particularly for students, about disinformation campaigns and how to avoid being manipulated when consuming news.; Advocate to state and local governments to include media literacy in their public education curriculum; Devise curriculum to strengthen civic education, particularly on the question of why democracy matters and why it should be protected from external attempts to undermine it.

2. Expand efforts to monitor and counter disinformation campaigns. Projects like ASD's Hamilton 68 Dashboard, the Atlantic Council's DFR Lab, and StopFake have been groundbreaking in exposing disinformation campaigns across the transatlantic space in real time. They should continue to refine their tools and their analytical models, and they should also be more involved in directly countering falsehoods propagated by foreign actors and perpetuated by bots and trolls online. There also needs to be more of these sites and tools, and better coordination between them to avoid duplication of efforts and to amplify each other's successes. The Atlantic Council's Disinformation Portal, with which ASD partners, is a good initial step in this direction.

- NGOs need greater funding to keep up with this rapidly developing space. Government's primary role in the disinformation field should be to issue grants to support NGOs' work. Philanthropic and private foundations should also increase their support for civil society organizations monitoring and defending against foreign threats to democratic institutions.

3. Increase support for local and independent media. Today's media environment is dominated by the cable news networks, and, to a lesser extent, the major papers. Local and independent media are dying. That is bad for a number of reasons, including the fact that local media are often trusted to a greater degree than cable and online news outlets.[92]

- Philanthropic support is essential to supporting local journalism. In addition to direct support for news outlets, individuals and foundations should support initiatives like the Report for America project, which seeks to support a new generation of emerging journalists reporting on under-covered topics in under-covered communities. With more resources, local media can indeed be a bulwark against foreign interference and disinformation.

92 Knight Foundation, "American Views: Trust, Media and Democracy," *A Gallup/Knight Foundation Survey, January 16, 2018*, https://kf-site-production.s3.amazonaws.com/publications/pdfs/000/000/242/original/KnightFoundation_AmericansViews_Client_Report_010917_Final_Updated.pdf.

4. Pressure elected officials to take this threat seriously and address it immediately. Americans across the country have the power to make their voices heard and demand that government in Washington and in their states take action to defend against and deter foreign interference in our democracy. Concerned citizens should band together to form advocacy groups in order to raise awareness and put pressure on their elected representatives.

5. Remember that our democracy is only as strong as we make it. The polarization of American society, reflected in our politics, contributed to the conditions that the Russian government exploited. Americans have a responsibility to strengthen our democracy and address our problems at home that malign foreign actors use against us. We recommend that civil society organizations form partnerships with each other and, where appropriate, with the U.S. government to improve governance and the rule of law, fight corruption, and promote media literacy. Moreover, we need to instill a healthier respect for one another, regardless of our differences, by improving our civic discourse, practicing more responsible behavior on social media, and calling on our elected officials to take action to defend our democracy on a bipartisan basis.

Acknowledgements

The authors would like to thank President of the German Marshall Fund (GMF) Karen Donfried, GMF Executive Vice President Derek Chollet, and the GMF Board of Trustees for their support for the Alliance for Securing Democracy (ASD) and dedication to strengthening the transatlantic relationship.

We would like to thank the members of ASD's Advisory Council, who provided extensive feedback on the analysis and recommendations of this report and who so generously have devoted their time and expertise to our overall mission since ASD was founded in July 2017. We also thank ASD's principal donors – the Hewlett Foundation, Democracy Fund, Sandler Family Foundation, Seth Klarman, and Craig Newmark Philanthropies – and dozens of individual donors for their support and generosity.

We are indebted to the innumerable experts whom we consulted for input, drawing on their experience in government, the tech sector, media, and civil society. We also acknowledge the vast contributions to the literature these experts have made, and on whose reports and commentary we have relied; we list several of these influential reports in Appendix A.

European officials and colleagues in various non-governmental organizations have been gracious with sharing lessons learned from their nations' experiences confronting Russian and other foreign interference in their democracies, even when Americans should have listened to their warnings and advice well before the United States found itself under attack.

We could not have completed this report in a timely manner without the help and dedication of ASD's staff and many interns, who assisted us in all aspects of this endeavor.

Finally, we thank Americans across our country and across multiple sectors and organizations who have begun to organize and collaborate to tackle this urgent challenge to our democracy.

Appendix A: Influential Publications

The authors would like to acknowledge the substantial contribution of the following publications to the development of this report and to the furthering of research in the field of countering authoritarian influence in democracies:

Anne Appelbaum, Peter Pomerantsev et al., "'Make Germany Great Again:' Kremlin, Alt-Right and International Influences in the 2017 German Elections," *Institute for Strategic Dialogue*, December 6, 2017.

Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation," *Atlantic Council*, March 5, 2018.

"Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, January 6, 2017.

Belinda Li, "The Other Immigration Crisis," *Hudson Institute*, January 17, 2017.

Chris Meserole and Alina Polyakova, "Disinformation Wars," *Foreign Policy*, May 25, 2018.

Dipayan Ghosh and Ben Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," *New America*, January 23, 2018.

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

Erica Newland et al. "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users," *The Berkman Center for Internet & Society and The Center for Democracy & Technology*, September 2011.

European Commission, "Communication - Tackling Online Disinformation: A European Approach," April 26, 2018.

"Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation," *Stern Center for Business and Human Rights*, November 3, 2017.

Heather A. Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, October 13, 2016.

Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information," *Alliance for Securing Democracy, German Marshall Fund of the United States*, March 23, 2018.

Ian Vandewalker and Lawrence Norden, "Getting Foreign Funds Out of America's Elections," *Brennan Center for Justice*, April 6, 2018.

"Joint Communication to the European Parliament, the European Council and the Council: Increasing Resilience And Bolstering Capabilities to Address Hybrid Threats," *European Commission*, June 13, 2018.

Jonas Parello-Plesner, "The Chinese Communist Party's Foreign Interference Operations: How the U.S. and Other Democracies Should Respond," *Hudson Institute*, June 20, 2018.

Keir Giles, "Countering Russian Information Operations in the Age of Social Media," *Council on Foreign Relations*, November 21, 2017.

Lawrence Norden and Ian Vandewalker, "Securing Elections from Foreign Interference," *Brennan Center for Justice*, June 29, 2017.

"Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security" (United States Senate, Committee on Foreign Relations, January 10, 2018).

Robby Mook, Matt Rhoades, and Eric Rosenbach, "Cybersecurity Campaign Playbook," *Belfer Center for Science and International Affairs*, November 2017.

Robby Mook, Matt Rhoades, and Eric Rosenbach, "The State and Local Election Cybersecurity Playbook," *Belfer Center for Science and International Affairs*, February 2018.

Robert D. Blackwill and Philip H. Gordon, "Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge," *Council on Foreign Relations*, January 2018.

Robert K. Knake, "Sharing Classified Cyber Threat Information With the Private Sector," *Council on Foreign Relations*, May 15, 2018.

Tim Maurer and Erik Brattberg, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," *Carnegie Endowment for International Peace*, May 23, 2018.

U.S. Department of Justice, "United States of America v. Internet Research Agency LLC," February 16, 2018.

U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations," May 8, 2018.

Appendix B: ASD Advisory Council

Mike Chertoff

Mike Chertoff was U.S. Secretary of Homeland Security from 2005 to 2009. There, he worked to strengthen U.S. borders, provide intelligence analysis, and protect infrastructure. He increased the Department's focus on preparedness ahead of disasters, and implemented enhanced security at airports and borders. Following Hurricane Katrina, Chertoff helped to transform FEMA (Federal Emergency Management Agency) into an effective organization. He also served as a judge on the U.S. Court of Appeals Judge from 2003–05. He co-founded the Chertoff Group, a risk-management and security consulting company, and works as senior of counsel at the Washington, DC law firm Covington & Burling.

Toomas Ilves

Toomas Hendrik Ilves was elected president of the Republic of Estonia in 2006 and in 2011. During his presidency, Ilves was appointed to serve in several high positions in the field of information and communication technology in the European Union. He previously served as minister of foreign affairs and as the ambassador of the Republic of Estonia to the United States and Canada in Washington. Ilves was also a member of the Estonian Parliament, as well as a member of the European Parliament, where he was vice president of the Foreign Affairs Committee. He now co-chairs the World Economic Forum working group The Global Futures Council on Blockchain Technology and is a distinguished visiting fellow at the Hoover Institution at Stanford University.

David Kramer

David J. Kramer joined Florida International University's Steven J. Green School of International and Public Affairs as a senior fellow in the Vaclav Havel Program for Human Rights and Diplomacy in May 2017. Before moving to Miami, Kramer had worked in Washington, DC for 24 years, most recently as senior director for Human Rights and Democracy with The McCain Institute for International Leadership. Before that, he served for four years as president of Freedom House. Prior to that, he was a senior transatlantic fellow at The German Marshall Fund of the United States. Kramer served eight years in the U.S. Department of State during the George W. Bush administration, including as assistant secretary of state for Democracy, Human Rights, and Labor; deputy assistant secretary of state for European and Eurasian Affairs; professional staff member in the Secretary's Office of Policy Planning; and senior advisor to the undersecretary for Global Affairs. Kramer is a member of the board of directors of the Halifax International Security Forum and a member of the advisory council for the George W. Bush Presidential Center's Human Freedom Project.

Bill Kristol

William Kristol is the editor at large of the influential political journal, *The Weekly Standard*. Before starting that magazine in 1995, Kristol served in government, first as chief of staff to Secretary of Education William Bennett during the Reagan administration, and then as chief of staff to Vice President Dan Quayle in the George H. W. Bush administration. Kristol has also served on the board of the Project for the New American Century (1997–2005) and the Foreign Policy Initiative (2009–17). Before coming to Washington in 1985, Kristol taught government at the University of Pennsylvania and Harvard University.

Rick Ledgett

Rick Ledgett has four decades of experience in intelligence, cybersecurity, and cyber operations, including 29 years with the National Security Agency where he served as deputy director from January 2014 until his retirement in April 2017. In that capacity he was responsible for providing foreign intelligence and protecting the nation's most important national security-related networks. Rick is a senior visiting fellow at The MITRE Corporation, a director on the Board of M&T Bank, serves as a trustee on the Board of the Institute for Defense Analyses, and is a member of several corporate advisory boards.

Michael Morell

Michael Morell was acting director of the Central Intelligence Agency in 2011 and again from 2012 to 2013, and had previously served as deputy director and director for Intelligence at the Agency. In his over thirty years at the CIA, Morell played a central role in the United States' fight against terrorism, its initiatives to halt the proliferation of weapons of mass destruction, and its efforts to respond to trends that are altering the international landscape — including the Arab Spring, the rise of China, and the cyber threat. He was one of the leaders in the search for Osama bin Laden and participated in the deliberations that led to the raid that killed bin Laden in May 2011. He has been with Beacon Global Strategies as a senior counselor since November 2013.

Mike McFaul

Michael McFaul served for five years in the Obama administration, first as special assistant to the president and senior director for Russian and Eurasian Affairs at the National Security Council at the White House from 2009 to 2012, and then as U.S. ambassador to the Russian Federation from 2012–14. He is currently professor of political science, director, and senior fellow at the Freeman Spogli Institute for International Studies, and the Peter and Helen Bing senior fellow at the Hoover Institution. He joined the Stanford faculty in 1995. He is also an analyst for NBC News and a contributing columnist to *The Washington Post*.

Mike Rogers

Mike Rogers is a former member of Congress, officer in the Army, and FBI special agent. In the U.S. House he chaired the Intelligence Committee, becoming a leader on cybersecurity and national security policy, and overseeing the 17 intelligence agencies' $70 billion budget. Today Mike is a CNN national security commentator, and hosts and produces CNN's "Declassified." He serves as Chief Security Adviser to AT&T, sits on the board of IronNet Cybersecurity and MITRE Corporation, and advises Next Century Corporation and Trident Capital. He is Distinguished Fellow and Trustee at Center for the Study of the Presidency and Congress, and a Senior Fellow at the Belfer Center at Harvard University.

Kori Schake

Kori Schake has served in various policy roles including at the White House for the National Security Council, at the Department of Defense for the Office of the Secretary and Joint Chiefs of Staff, and at the State Department for the Policy Planning Staff. During the 2008 presidential election, she was senior policy advisor on the McCain–Palin campaign. She is now a research fellow at the Hoover Institution. She is the editor, with Jim Mattis, of the book *Warriors and Citizens: American Views of Our Military*. She is the Deputy Director-General at the International Institute for Strategic Studies, a contributing editor covering national security and international affairs at *The Atlantic*, a columnist for *Foreign Policy* magazine, and a contributor to *War on the Rocks*.

Julie Smith

Julianne "Julie" Smith served as the deputy national security advisor to the U.S. vice president from 2012 to 2013, acting national security advisor to the vice president in 2013, and principal director for European and NATO policy in the Office of the Secretary of Defense in the Pentagon. Smith is currently senior fellow and director of the Transatlantic Security Program at the Center for a New American Security.

Admiral Jim Stavridis (Ret.)

Admiral James Stavridis, U.S. Navy (Ret.) served as commander of European Command and as Supreme Allied Commander, Europe from 2009 to 2013. He commanded U.S. Southern Command in Miami from 2006–09 and commanded Enterprise Carrier Strike Group, conducting combat operations in the Arabian Gulf in support of both Operation Iraqi Freedom and Operation Enduring Freedom from 2002–04. He was a strategic and long-range planner on the staffs of the Chief of Naval Operations and the Chairman of the Joint Chiefs of Staff. He has also served as the executive assistant to the secretary of the navy and as senior

military assistant to the secretary of defense. He is now dean of the Fletcher School of Law and Diplomacy, Tufts University, and chairman of the U.S. Naval Institute board of directors.

Jake Sullivan

Jake Sullivan served in the Obama administration as national security advisor to Vice President Joe Biden and director of Policy Planning at the U.S. Department of State, as well as deputy chief of staff to Secretary of State Hillary Clinton. He was the senior policy advisor on Secretary Clinton's 2016 presidential campaign. He is now a senior fellow at the Carnegie Endowment for International Peace and Martin R. Flug visiting lecturer in law at Yale Law School.

Nicole Wong

Nicole Wong served as deputy U.S. chief technology officer in the Obama administration, where she focused on internet, privacy, and innovation policy. Prior to her time in government, Nicole was Google's vice president and deputy general counsel, and Twitter's legal director for products. She frequently speaks on issues related to law and technology. Nicole chairs the board of Friends of Global Voices, a nonprofit organization dedicated to supporting citizen and online media projects globally. She also sits on the boards of WITNESS, an organization supporting the use of video to advance human rights, and the Mozilla Foundation, which promotes open internet. Nicole currently serves as an advisor to the School of Information at the University of California, Berkeley, Harvard Business School Digital Initiative, the Democratic National Committee Cybersecurity advisory board, Refactor Capital, and the Albright Stonebridge Group.

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

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

www.gmfus.org

RESPONSES TO QUESTIONS SUBMITTED FOR THE RECORD

Questions for the Record from Representative Ann Wagner
Subcommittee on Europe, Eurasia, Energy and Environment
Undermining Democracy: Kremlin Tools of Malign Political Influence
May 21, 2019

Question:

I understand that some hope energy exports from Azerbaijan can lessen Europe's dependence on Russia for its energy needs. Ms. Rosenberger, is Russia concerned that the Southern Gas Corridor, which will connect Caspian Sea natural gas reserves with European markets, will diminish Russia's leverage in Europe when it is completed?

Answer:

Ms. Rosenberger did not submit a response in time for printing.

Question:

Latvia and Estonia have significant ethnic Russian minority populations, a legacy of the Soviet occupation. These minority communities remain relatively unintegrated—some 350,000 are non-citizen residents without voting rights—but so far have not advocated for annexation by Russia. Mr. Doran, how have Latvia and Estonia approached problems of integration, and are we seeing Russia seeking to expand feelings of disaffection among ethnic Russians in Baltic countries?

Answer:

Mr. Doran: This is an important question since it highlights a significant risk vector for Kremlin operations in the Baltic States.

First, it is essential to recall that the status of ethnic Russians living in all of the Baltic States—Estonia, Latvia, and Lithuania (to a lesser degree) is mainly a hold-over from the Soviet era. When the USSR disintegrated in 1991, ethnic Russians in the Baltic States found themselves living in a "new" country. Today in Estonia, for example, many still hold the status as "stateless persons." While they are not official citizens of any country, they hold "grey passports" which give them travel rights inside the Russian Federation and the EU's Schengen Zone. Moreover, these "stateless" people do have many—but not all—of the rights that full Estonian citizens enjoy.

Second, I would stress for the Committee that a prime area of concern should *not* be these ethnic populations as such. They are not a monolithic group, nor are they uniformly pro-Kremlin. Rather, it is the Kremlin's self-proclaimed right to intervene in foreign countries on behalf of Russian speakers or individuals of putative Russian ethnicity. This concept, often summarized as the "Medvedev Doctrine," is sweeping in its potential scope—and it is not theoretical.

As a pretext for Russia's illegal annexation of Crimea in 2014, the Kremlin and its propaganda outlets used this self-proclaimed right as a justification for its invasion of that territory. Specifically, the "imminent ultra-nationalist threat" that ethnic Russians and Russian-speakers

allegedly faced in Crimea. This was a manufactured pretext. No such threat existed. The point here: The Kremlin used the very presence of Russians living in Ukraine—and its asserted need to "protect" them with force—as an explanation for its invasion of a neighboring country.

Third, this has serious ramifications for the Baltic States. When it comes to future risk of Russian aggression, it is obviously difficult to predict with any degree of certainty if the Kremlin would invoke the same/similar pretext for military operations (overt or covert) against Estonia, Latvia—or even Lithuania. Nonetheless, we know that Kremlin leaders used this pretext before. This alone is significant. At a minimum, it should be prominent in the Committee's consideration of Russian active measures against U.S. allies in the region.

As for the specific approach that Latvia and Estonia have taken to the problems of integrating "stateless" persons into their societies, I would stress for the Committee's consideration that Russian propaganda outlets devote a great deal of effort to overstating these issues.

My organization (CEPA) has produced a significant catalog of analysis on how Russia uses disinformation to either target ethnic Russian populations in the Baltics with toxic narratives, or to use the plight of these individuals as a "wedge issue" aimed at peeling off Western political support for allied governments in Estonia and Latvia. Highly illustrative examples of Kremlin disinformation in this regard can be found here (Estonia), here (Estonia), here (Latvia) and here (Latvia).

Finally, there is some good news. The Baltics have become a popular emigration destination for Russian speakers and ethnic Russians, indicating that individuals are "voting with their feet" to find a better life and political freedom in these countries. Likewise, the Estonian and Latvian governments have simultaneously made outreach to domestic Russian communities a priority. Note how Estonian President Kersti Kaljulaid temporary relocated the official seat of her presidency to Narva last year—a symbolic, albeit important move to show awareness and respect toward the large ethnic Russian population in that city. And when it comes to the voting rights of "stateless" persons in Estonia in particular, the Committee will be pleased to learn that these individuals are now allowed to vote in local elections.

The bottom line here: some important progress has been made, and this is positive. However, the overall issues related to ethnic Russians in the Baltics will continue to be one that the Kremlin can exploit for "political warfare" while sowing the seeds of domestic strife or conflict. The Committee is right to keep its eye on this topic.

I wish to offer my sincere thanks for the opportunity to testify before the Committee. I am extremely grateful for your question.

CEPA Analysis referenced in the text above:

Urve Eslas, "Myth Busted: Estonia's 'Impossible' Citizenship," Center for European Policy Analysis, 30 October 2017. http://infowar.cepa.org/Briefs/Est/Myth-busted-Estonias-impossible-citizenship

Urve Eslas, "Eroding Trust in the Age of Spies," Center for European Policy Analysis, 10 October 2018. https://www.cepa.org/eroding-trust-in-the-age-of-spies

Anna Udre, "Battleground Wikipedia," Center for European Policy Analysis, 4 March 2019. https://www.cepa.org/battleground-wikipedia

Mārtiņš Kaprāns, "Isolating Russia's Three Master Narratives in Latvia," Center for European Policy Analysis, 21 December 2017. http://infowar.cepa.org/Briefs/Isolating-Russias-three-master-narratives-in-Latvia

○