Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

MEETING THE RUSSIAN HYBRID CHALLENGE

A COMPREHENSIVE STRATEGIC FRAMEWORK

Franklin D. Kramer
and Lauren M. Speranza

MEETING THE RUSSIAN HYBRID CHALLENGE

A COMPREHENSIVE STRATEGIC FRAMEWORK

Franklin D. Kramer
and Lauren M. Speranza

ISBN: 978-1-61977-415-5

May 2017

CONTENTS

EXECUTIVE SUMMARY

Hybrid challenges continue to threaten security across the Euro-Atlantic community. Though hybrid has multiple aspects, this paper particularly analyzes hybrid challenges facing the overlapping nations of NATO and the European Union (EU) that are a function of deliberate and persistent Russian activities. While hybrid conflict has been defined in many ways, this paper describes hybrid threats to include four key categories: low-level use of force; cyberattacks; economic and political coercion and subversion; and information war. This paper proposes a comprehensive strategic framework for Europe, Canada, and the United States to address these challenges at both the supranational and national levels and through public and private sector coordinated responses.

The paper is organized into two parts. The first sets forth the challenges, building on multiple analyses previously undertaken by governmental and nongovernmental organizations. The section outlines how these Russian hybrid actions attack the functioning of Western public and private institutions. While the West has undertaken various responses, including through NATO, the EU, and individual nations, these efforts have not adequately resolved the challenges. Accordingly, the second part, and the heart of the paper, lays out five categories of functional and structural recommendations designed to enhance the resilience of Western democratic governments and societies in the face of Russian hybrid threats. While the functional recommendations below are categorized in response to each particular threat, these challenges are often multifaceted and extend beyond one country. Consequently, the last recommendation is structural, proposing a coordinating entity to help guide the efforts of NATO, the EU, their nations, and the private sector to maximize the effectiveness of Western responses.

RECOMMENDATIONS

1) Low-Level Use of Force

Low-level hybrid use of force is a significant concern, particularly for the eastern nations of the EU and NATO. To address this challenge, allies and member states should coordinate their efforts on resilience according to the NATO-EU Joint Declaration at the 2016 NATO Warsaw Summit by working toward:[1]

- enhanced intelligence capabilities through the creation of an "Eastern Hub" (comparable to the one NATO is creating for the south) that can review Russian intentions, capabilities, and activities;
- expanded training and operational capabilities by:
  - coordinating the efforts of military special forces and the European Gendarmerie Force, and ensuring these forces work with national police and other domestic security agencies to physically protect critical infrastructure, develop contingency plans, and undertake exercises for resilience support and hybrid defense; and
  - establishing a network to increase information sharing and operational capabilities among NATO Force Integration Units and/or multinational battalions, the European Gendarmerie Force, the European Border and Coast Guard Agency, and its European Border Guard Teams (EBGTs);
- combined NATO-EU national assessments for key critical infrastructures, including working closely with the private sector;
- coordinated and harmonized force planning between the NATO Defence Planning Process and the EU Capability Development Plan, recognizing there is only one set of forces, and conflicting requirements need to be resolved;
- coordinated potential responses under Articles 4 and 5 of the North Atlantic Treaty[2] and Articles 42.7 and 222 of the Lisbon Treaty,[3] particularly if there is potential for transition from low-level use of force to conventional warfare; and
- use of legal tools: where international or national laws are broken, EU and NATO nations should use legal tools, such as indictments, forfeitures, and other sanctions, to limit and deter future Russian illegal actions.

2) Cyberattacks

To adapt to emerging threats in the cyber domain, and build on the NATO-EU Joint Declaration, the

1 "Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," NATO, 2016, http://www.nato.int/cps/en/natohq/official_texts_133163.htm.

2 See NATO, *The North Atlantic Treaty*, April 4, 1949, http://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf.

3 See European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Signed at Lisbon, 13 December 2007*, Official Journal of the European Union, December 17, 2007, http://ec.europa.eu/archives/lisbon_treaty/full_text/index_en.htm.

transatlantic community should develop a coordinated cyber strategy focused on operational capabilities, including:

- the establishment of an effective cyber operational structure in each country (with the United Kingdom's new National Cyber Security Centre providing a useful model);
- the creation of contingency plans that coordinate government and private sector action and take account of the potential for multinational and cascading effects;
- a working governance structure within each country among key cyber entities, including particularly the military, civil governmental authorities, Internet Service Providers, and electric grid operators, and, if appropriate, a comparable regional structure;
- active coordination by NATO and the EU on their cyber activities, so that nations have a consistent set of requirements and so appropriate protection, resilience, and recovery can be provided with respect to multinational and cascading cyber impacts;
- advance actions to reduce vulnerabilities and enhance protection, resilience, and recovery, especially in the critical sectors of telecommunications, electric grids, and finance;
- the assistance of "cyber framework nations"—specifically, the United States, Canada, Germany, and the United Kingdom—to countries with less-developed cyber capabilities, first focusing on the Baltics and Poland where multinational battalions have been deployed; and
- the use of cyber sanctions, particularly at the multinational level.

3) Economic and Political Coercion and Subversion

To respond to economic and political coercion and subversion, NATO, the EU, and national mechanisms should be established and/or expanded to:

- increase intelligence capabilities and sharing including through the use of a combined "hub" as a central clearinghouse;
- establish greater transparency on Russian actions by a) issuing public national intelligence reports and analyses, as is already done by several countries, and b) requiring reporting to national authorities and the EU on all economic actions by Russia of any consequential size or effect, including acquisitions of more than a certain percentage, significant loans, or other financial arrangements with domestic companies—particularly any of a country's critical infrastructures;

> "[The paper] lays out five categories of functional and structural recommendations designed to enhance... resilience...in the face of Russian hybrid threats.."

- enhance anti-corruption investigation and enforcement measures, which should focus on activities by Russia and Russian-controlled entities and be implemented at the EU-level, in the same way as the EU's security and anti-money laundering strategies;
- limit Russian political activities and financial investment by a) barring support of political parties by Russia and Russian-controlled entities, and b) expanding reviews of financial transactions by Russian entities that could lead to detrimental impacts on the national security, economy, and/or democratic functioning of a country; and
- increase emphasis on reducing key dependencies, including in the energy arena, where—to make Russia a normal market participant—European nations should actively promote alternative sources to Russia-provided energy.

4) Information Warfare

In response to Russia's substantial information warfare efforts, the transatlantic community should devise an information strategy that would:

- develop a comprehensive response to election interference, which would include:
  - a voluntary code of standards for online media-provided information in the context of elections, which could build on the existing *Code of Conduct on Countering Illegal Hate Speech Online* and further draw from national legal requirements regarding defamation,

privacy, and objectivity (such as in Germany and the United Kingdom);

- working with private sector online companies to block and/or limit the reach of Russian information efforts aimed at impacting elections that do not meet the criteria of the voluntary code;
- national governments having the capacity to fine, sanction, close the bank accounts of, restrict funding to, or suspend operating licenses of foreign or foreign-directed media in the event of demonstrated election interference (similar to what the UK's Office of Communications (Ofcom) did with RT, formerly Russia Today, when it was found to be in flagrant violation of UK objectivity regulations with certain coverage); and
- the use of multinational sanctions and other legal limitations in the event of demonstrated election interference.

- discredit the sources of Russian disinformation and further develop the capacity to highlight specific Russian disinformation through:
  - widely accessible measures, including, for instance, a public "dashboard," or other digital means, that identifies the falsity and lack of objectivity of Russian-generated media;
  - a fund to support civil society and other private sector efforts to respond to Russian disinformation; and
  - efforts to counter disinformation within EU and NATO nations and expanding resources for other NATO, EU, and national counter-disinformation efforts, including the capacity of the EU's European External Action Service East StratCom Task Force.
- work with the private sector to develop comprehensive available sources of information, giving the public the access and ability to develop a resilient understanding of today's extensive information flows.

5) The Euro-Atlantic Coordinating Council and a Multinational Coordinated Strategy

While meeting the Russian hybrid challenge can be undertaken through existing mechanisms, including informal cooperation between NATO and the EU, a fully effective transatlantic response would significantly benefit from new coordinating structures that go beyond the current limited cooperation and are still flexible enough to allow for both multinational and distributed specific actions. A key element of this response would include the establishment of a new transatlantic entity that would coordinate the efforts of NATO, the EU, and individual nations, as well as the private sector. The new entity would operate on a voluntary basis to provide coordinated diplomatic, economic, information, security, and military actions, including the necessary involvement of the private sector. More specifically:

- A "Euro-Atlantic Coordinating Council"—consisting of EU and NATO nations, as well as the EU and NATO as institutional bodies—could define and coordinate such an effort. Building on the financial sector's model of the Financial Stability Board and the Proliferation Security Initiative, which are each voluntary organizations, the Coordinating Council would operate as an oversight entity, while existing institutions, including NATO, the EU, and their nations, would undertake implementation.
- The Coordinating Council would have several working groups, each focused on a particular aspect of the hybrid challenge, including low-level use of force, cyberattacks, economic and political coercion and subversion, and information warfare.
- For greatest effectiveness in working with the Council, nations should adopt a version of the "Finland Model" of integrated governmental and private sector interactions to create responsive and resilient structures.
- In addition to government representatives, which would form the core of the Council, the Coordinating Council would have a structure to interact with relevant private sector entities, particularly for the protection of critical infrastructure such as telecommunications, electric grid companies, information platforms, and technology companies.
- The Council would help develop multinational coordinated actions, including countermeasures authorized under international law, that would create an effective counter-hybrid strategy building on the concept of solidarity, which is fundamental to both the EU and NATO treaties.

INTRODUCTION

Hybrid challenges continue to threaten security across the Euro-Atlantic community. Though hybrid has multiple aspects, this paper particularly analyzes hybrid challenges facing the overlapping nations of NATO and the European Union (EU) that are a function of deliberate and persistent Russian activities. While hybrid conflict has been defined in many ways, this paper describes hybrid threats to include four key categories: low-level use of force; cyberattacks; economic and political coercion and subversion; and information war.

Although these actions are not new, the past few years have shown a sharp increase in their intensity and scope. While the West has undertaken various responses, including through NATO, the EU, and individual nations, these efforts have not adequately resolved the challenges. The transatlantic community must recognize that an effective response requires an overarching, coordinated strategy to contain the multifaceted aspects of hybrid warfare. As a result, this paper proposes a comprehensive strategic framework for Europe, Canada, and the United States to address these challenges at both the supranational and national levels and through public and private sector coordinated actions.

I. HYBRID CHALLENGES

RUSSIA'S WORLDVIEW

Responding to Russia's hybrid challenge requires an understanding of the Russian worldview and the actions taken in support of that perspective.[4] Russia itself is an authoritarian regime with a decided anti-Western orientation and highly corrupt governing and economic institutions. One analysis underscored "Mr. Putin's insistence that he be allowed to run Russia solely the way he needs and wants," and how the "system . . . depends on cronyism, corruption and abuse of privilege."[5] Another stated, "What is distinctive about Russia is that under the reign of President Putin it has become an authoritarian regime."[6] A third quotes Putin's own statement: "I decide everything. Don't forget it."[7]

Corruption is a fundamental feature of Russia's governing and economic institutions. Freedom House has highlighted that "a growing lack of accountability enables bureaucrats to act with impunity" and that "the political system is essentially a kleptocracy, in which ruling elites plunder public wealth to enrich themselves."[8] The US Department of State had similar findings in its *Russia 2015 Human Rights Report*, citing the "bribery of officials, misuse of budgetary resources, theft of government property, kickbacks in the procurement process, extortion, and improper use of official position to secure personal profits."[9] The report found that corruption was prominent in a number of areas, including education, military conscription, healthcare, commerce, housing, social welfare, law enforcement, and the judicial system. In short, it is a "system based on massive predation."[10]

While authoritarianism and corruption pose difficulties on their own, Russia's anti-Western and zero-sum-focused international orientation further exacerbate the challenge of dealing with the Kremlin.[11] As one analysis explains, "In Moscow's eyes, the West gained the upper hand in the 1990s, both militarily through NATO's eastward expansion, and in propaganda terms by portraying Western democracy as the only attractive form of government. To counter the pre-eminence of the West, Moscow has shifted to guerrilla tactics in an attempt to undermine the West."[12]

As the foregoing suggests, Russian international objectives are clear: Russia seeks to reorder the existing international framework. As one European study on Russian foreign policy describes, "Russia seeks to gain superpower status and to reshape the rules of the international system so that Western domination ends and a multipolar world order emerges. This could help Russia expand its influence over the post-Soviet region, Central and Eastern

4 Russia, Moscow, the Kremlin, and the Russian government are used simultaneously to refer to Russia throughout the paper.

5 Fiona Hill and Clifford G. Gaddy, *Mr. Putin: Operative in the Kremlin*, Brookings, 2013, 269.

6 Vladislava Vojtíšková, Vít Novotný, Hubertus Schmid-Schmidsfelden, and Kristina Potapova, *The Bear in Sheep's Clothing: Russia's Government-Funded Organizations in the EU*, Martens Centre, 2016, https://www.martenscentre.eu/sites/default/files/publication-files/russia-gongos_0.pdf, 20.

7 Karen Dawisha, *Putin's Kleptocracy: Who Owns Russia?* (New York: Simon & Schuster, 2014), 349.

8 Freedom House, "Freedom in the World, Chapter: Russia," 2016, https://freedomhouse.org/report/freedom-world/2016/russia.

9 US Department of State, *Russia 2015 Human Rights Report*, 2015, https://www.state.gov/documents/organization/253105.pdf, 46.

10 Dawisha, *Putin's Kleptocracy*, 1.

11 Government of Finland, *Government Report on Finnish Foreign and Security Policy*, September 2016, http://valtioneuvosto.fi/documents/10616/1986338/VNKJ092016+en.pdf/b33c3703-29f4-4cce-a910-b05e32b676b9, 13.

12 "Russia's Propaganda Campaign against Germany," *Spiegel Online*, February 5, 2016, http://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html.

Coordination by Moscow increases the effectiveness of hybrid actors. Left: The National State Defense Management Center in Moscow, established in 2014, indicates a new level of coordination among Russian agencies and institutions. *Photo credit*: Kremlin.ru. Right: The self-proclaimed Donetsk People's Republic (DPR) separatist troops rehearsing for the 2015 Victory Day parade. *Photo credit*: Andrew Butko/Wikimedia Commons.

Europe, and even the Middle East."[13] Moreover, Russia would not "seek cooperation with Western countries on equal terms without challenging the current status quo."[14]

Hybrid activities are central to the means that Russia has employed to achieve its objectives. The Kremlin uses the full spectrum of hybrid actions, including cyberattacks, "little green men," and propaganda, in order to undermine the cohesion of NATO, the EU, and their member states.[15] Russian hybrid warfare also aims to sow divisions and separatism, promote pro-Russia policies, denigrate legitimate leaders, and establish what some have called a "moral equivalence"[16] between Russia and the West to support Russia's larger geostrategic goals. Russia's hybrid efforts are often linked to the article written by Chief of the Russian General Staff General Valery Gerasimov,[17] but regardless of the impetus, transatlantic policymakers have to recognize and plan for not only conventional military threats from Russia, but also the Kremlin's active subversion and destabilization efforts.[18]

13 Tomas Janeliunas,"Russia's Foreign Policy Scenarios: Evaluation by Lithuanian Experts," *Baltic Bulletin*, November 10, 2016, http://www.fpri.org/article/2016/11/russias-foreign-policy-scenarios-evaluation-lithuanian-experts/.

14 Ibid.

15 "Russia's Propaganda Campaign against Germany," *Spiegel* online, February 5, 2016, http://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html

16 "What We Know about Russian Meddling and Putin's Playbook," PBS News Hour, 2017, http://www.pbs.org/newshour/bb/know-russian-meddling-putins-playbook/.

17 General Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Voyenno-Promyshlennyy Kurier* online, February 26, 2013, http://vpk-news.ru/articles/14632.

18 Keir Giles, *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*, Chatham House, March 2016, https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf, 3.

Russia's hybrid efforts are based on a complex web of interconnected political, diplomatic, information, economic, and military actions, among other means.[19] While the objectives are similar, tactics vary depending on context. One study by the Martens Centre found that in certain European countries, the Kremlin emphasizes different soft power tools:

> In Western European countries, including the UK, France and Germany, it puts the emphasis mostly on its business ties, because with those countries it has very little in common in other areas . . . In countries with an Orthodox majority, such as Romania, Bulgaria, Serbia and Greece, Russian policy builds on the common religion and uses the Orthodox Church and connected organizations, such as the International Foundation for the Unity of Orthodox Christian Nations . . . In Slavic countries, including the Czech Republic, Slovakia, Poland and Bulgaria, it supports the old but still somewhat popular idea of pan-Slavism: Russia pushes the notion that 'we are all Slavs with the same origin and spirit' . . . In the Baltic countries the Russian government uses the Russian-speaking minority and compatriot organizations, which have mostly been founded since 2006, to exert influence. These NGOs [nongovernmental organizations] are predicated on the idea that Russian speakers form one unified civilization. They also falsify history and offer different versions of events, claiming for example, that Estonia 'voluntarily joined the USSR in 1940' . . . Finally, in Austria, Switzerland, Finland and Sweden, Russia places the emphasis on their neutrality.[20]

The foregoing discussion is based on conclusions reached by multiple European analyses, but these conclusions are also shared in the United States. For example, as described by the Office of the Director of National Intelligence:

> Moscow has been opportunistic in its efforts to strengthen Russian influence in Europe and Eurasia by developing affiliations with and deepening financial or political connections to like-minded political parties and NGOs. Moscow appears to use monetary support in combination with other tools of Russian statecraft, including propaganda in local media, direct lobbying by the Russian Government, economic pressure, and military intimidation. Russian trolls and other cyber actors post comments on the Internet, maintain blogs, challenge pro-Western journalists and media narratives, and spread pro-Russian information on social media. Russian sponsored media outlets RT and Sputnik have targeted various activist groups . . . and far-right and far-left elements of European society.[21]

In sum, Russia utilizes an all-domain hybrid effort to advance its geopolitical objectives, aiming to "manipulate the adversary's perception, to maneuver its decision-making process, and to influence its strategic behavior while minimizing, compared to the industrial warfare era, the scale of kinetic force use, and increasing the non-military measures of strategic influence. Informational pressure . . . on the adversary, its armed forces, state apparatus, citizens, and world public opinion . . . aimed at producing favorable conditions for strategic coercion."[22]

Recognizing this multiplicity of approaches and their interrelated connectivity is key to understanding Russian hybrid warfare and developing an effective response. The following section takes a deeper look into four main functional challenges within Russia's hybrid warfare campaign.

FUNCTIONAL CHALLENGES

Low-Level Use of Force

Russia has shown its ability to use low-level force as a means to achieve its geopolitical objectives throughout Europe. As with hybrid conflict generally, Russia has employed a full spectrum of activities, ranging from incitement of violence, kidnapping, and attempted assassination to infiltration and covert action combined with military efforts. The examples below illustrate both Russia's capabilities and its willingness to use them.

Incitement of violence is a significant concern for many countries. The Russian government has been accused of deploying operatives to foreign countries to deliberately protest or incite civil unrest or violence as part of its hybrid warfare campaign. Experts have

19 Dmitry Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy*, Institut Français des Relations Internationales, November 2015, http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf, 36.

20 Vojtíšková, Novotný, Schmid-Schmidsfelden, and Potapova, *The Bear in Sheep's Clothing*, 24-26.

21 Permanent Select Committee on Intelligence – Letter, Office of the Director of National Intelligence, 2016, https://www.scribd.com/document/325680160/Dni-LtrPermanent-Select-Committee-on-Intelligence-to-Chm-Rm-Re-Sec-502-of-Iaa-Fy-2016-23-Sep-16-2#from_embed.

22 Adamsky, *Cross-Domain Coercion*, 36.

argued that "the tactic is a ploy to demonstrate Russian strength while building on a narrative inside the country that the rest of the world is lining up against it."[23] One example of this occurred at the Euro 2016 soccer tournament:

> Senior government officials fear the violence unleashed by Russian hooligans at Euro 2016 was sanctioned by the Kremlin and are investigating links with Vladimir Putin's regime. It is understood that a significant number of those involved in savage and highly coordinated attacks on England fans and others in Marseille and Lille have been identified as being in the 'uniformed services' in Russia. Following the violence in Marseille, fake Twitter accounts were reportedly set up to spread the view that Russian fans had been provoked. A senior Russian parliamentarian tweeted, 'Well done lads, keep it up!'[24]

Higher on the scale of low-level use of force from incitement of violence is the capacity to breach borders, covertly or overtly, as part of a hybrid effort. In Estonia, for example, Russian forces crossed the border and kidnapped an Estonian border guard who subsequently was convicted by a Russian court and sentenced to a fifteen-year imprisonment for "spying, possession of weapons, and illegally crossing the border."[25] Estonian officials pushed back citing Russia's clear violation of international law, highlighting that Kohver, the guard, was abducted on Estonian territory during "an audacious cross-border raid by the Federal Security Service of the Russian Federation (FSB) involving radio-jamming equipment and smoke grenades."[26] Despite public calls from EU and other European officials for Kohver to be released, he was convicted and jailed in Russia, until returning to Estonia in a prisoner exchange.[27]

Kremlin-sanctioned low-level use of force has also targeted higher-level officials. In Montenegro, Russian security services were accused of carrying

"Covert action may also be utilized as a key operational tactic of Russian low-level use of force. The most prominent example of this is in Ukraine. . ."

out an assassination attempt on the Montenegrin prime minister.[28] Montenegro prosecutor Milivoje Katnic implicated Russia in what he called a "failed coup of Montenegro's government," adding that the assassination was an attempt to keep formerly Soviet-dominated Montenegro from pursuing NATO membership.[29] Montenegrin officials confirmed that Russian state authorities, in addition to nationalist forces, were behind the events,[30] and the United Kingdom's foreign minister publicly agreed.[31] The Kremlin rejected the accusations, dismissing them as Western attempts to stoke tensions with Russia.

Covert action may also be utilized as a key operational tactic of Russian low-level use of force. The most prominent example of this is in Ukraine, where the Kremlin used its own agents and disaffected elements on the ground to eventually carry out the annexation of Crimea. The annexation started as a covert military operation employing a combination of electronic warfare, propaganda, ambiguity, and surprise.[32] As the *Guardian* summarizes, capitalizing on disorder sparked by protests against government corruption in Crimea,

> Putin ordered surprise military drills on the border with Ukraine, and at Russia's Black Sea base on Ukraine's Crimean Peninsula. Almost simultaneous to the exercises, armed men in unmarked uniforms, most wearing masks,

23 Daniel Boffey, "Whitehall Fears Russian Football Hooligans Had Kremlin Links," *Guardian*, June 18, 2016, https://www.theguardian.com/football/2016/jun/18/whitehall-suspects-kremlin-links-to-russian-euro-2016-hooligans-vladimir-putin.

24 Ibid.

25 Shaun Walker, "Russia Jails Estonian Intelligence Officer Tallinn Says Was Abducted Over Border," *Guardian*, August 2015, https://www.theguardian.com/world/2015/aug/19/russia-jails-estonian-police-officer-allegedly-abducted-border-eston-kohver

26 Ibid.

27 "Russia and Estonia 'Exchange Spies' after Kohver Row," BBC, September 26, 2016, http://www.bbc.com/news/world-europe-34369853.

28 Ed Adamczyk, "Russia Involved in Attempted Coup, Montenegro Prosecutor Says," UPI, February 2017, http://www.upi.com/Top_News/World-News/2017/02/22/Russia-involved-in-attempted-coup-Montenegro-prosecutor-says/1581487767036/.

29 Ibid.

30 Ibid.

31 Kate McCann, "Boris Johnson Claims Russia Was Behind Plot to Assassinate Prime Minister of Montenegro as He Warns of Putin's 'Dirty Tricks,'" *Telegraph*, March 12, 2017, http://www.telegraph.co.uk/news/2017/03/12/boris-johnson-claims-russia-behind-plot-assassinate-prime-minister/.

32 Michael Kofman and Matthew Rojansky, *A Closer Look at Russia's 'Hybrid War*,' Wilson Center, April 2015, https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

seized airports and regional government buildings around Crimea. (Though some admitted being Russian, most, and Russia, denied any affiliation and characterized them as 'local self-defense groups.') With armed gunmen surrounding the regional parliament, Crimea, heretofore a part of Ukraine with slightly more independence than other regions, voted in a new government of pro-Russian figures and decided to hold a referendum on Crimea's future. Russia's parliament authorized deploying troops in Ukraine, should Putin see fit. On the ground, a de facto stealth invasion had already taken place, with Russian-plated vehicles blocking roads, the Russian fleet trapping Ukrainian warships, and pro-Russian forces in tense standoffs around every major Ukrainian base.[33]

Cyberattacks

In addition to using force in the context of hybrid conflict, Russia has the capability to utilize cyberattacks to disrupt operational networks, such as electric grids or finances, in both Europe and North America. This potential impact on *operational networks* is distinct from *information warfare* discussed separately later.

The risk from cyberattacks to critical infrastructure is substantial. According to then-Director of National Intelligence James Clapper, both the telecommunications sector and the electric grid face escalating cyber threats to their information technology, industrial control systems, and other operational technology systems on which they rely.[34] Likewise, Admiral Michael Rogers, dual-hatted as the director of the National Security Agency and commander of Cyber Command, has testified: "We have also observed that energy firms and public utilities in many nations including the United States have had their networks compromised by state cyber actors."[35]

Several recent analyses have identified vulnerabilities of Internet Service Providers (ISPs) to include distributed denial of service (DDOS) attacks, vulnerabilities in network devices, and insider threats.[36] Telecommunications systems have been attacked in key European countries, including Poland and Norway.[37] Ukraine's electric grid was also targeted in an attack that disabled multiple distribution utilities and impacted over two hundred thousand people for several hours.[38] Such activities have been increasing over the past decade. As one Atlantic Council study stated:

> Since 2007 and the Russian distributed denial-of-service attacks on the Estonian government and civilian entities, there has been a continued escalation of these types of attacks on nations in conflict situations, such as Georgia in 2008 and more recently Ukraine. Notably, NATO public websites and unclassified email were hit by DDOS attacks in March 2014, at the time of Russia's Crimea invasion. In December 2015, Turkish government websites and financial institutions were targeted in a two-week long DDOS attack resulting in the disruption of services and transactions. In an effort to stop the attack, Turkey blocked all foreign internet traffic. A European Parliament report has stated that cyber attacks 'have been directed to the military: grounding French naval planes, securing access to the UK Ministry of Defense's classified networks or attacking the Estonian Ministry of Defense (2013).'[39]

33 Alan Yuhas, "Ukraine Crisis: An Essential Guide to Everything That's Happened So Far," *Guardian*, April 13, 2017, https://www.theguardian.com/world/2014/apr/11/ukraine-russia-crimea-sanctions-us-eu-guide-explainer.

34 James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Committee," Office of the Director of National Intelligence, February 9, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

35 Admiral Michael S. Rogers, "Statement before the Subcommittee on Emerging Threats and Capabilities," House Armed Services Committee, March 16, 2016, http://docs.house.gov/meetings/AS/AS26/20160316/104553/HHRG-114-AS26-Wstate-RogersM-20160316.pdf.

36 Franklin D. Kramer, Robert J. Butler, and Catherine Lotrionte, *Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict*, Atlantic Council, December 2016, http://www.atlanticcouncil.org/images/publications/Cyber_and_Deterrence_web_0103.pdf, 4.

37 See *2016 Data Breach Investigations Report*, Rep. Verizon, June 6, 2016; Poland: Marcin Goettig, "Poland's No.2 Telecom Netia Says Suffered Cyber Attack," Reuters, July 8, 2016, http://www.reuters.com/article/us-poland-netia-cybercrimeidUSKCN0ZO22K; Norway: "Extent of Cyber Attacks Revealed," News in English, July 9, 2014, http://www.newsinenglish.no/2014/07/09/extent-of-cyber-attacks-revealed/.

38 Kramer, Butler, and Lotrionte, *Cyber and Deterrence*, 4. See SANS and E-ISACE, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 2016, http://www.nerc.com/pa/CI/ESISAC/Documents/EISAC_SANS_Ukraine_DUC_18Mar2016.pdf; and DHS-Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack against Ukrainian Critical Infrastructure, Alert (IR-ALERT-H-16-056-01)," February 25, 2016, https://ics-cert.us-cert.gov/alerts/. See also Admiral Michael S. Rogers, "Statement before the Subcommittee on Emerging Threats and Capabilities," House Armed Services Committee; and Kaspersky Lab, *Threat Intelligence Report for the Telecommunications Industry,* 2016, https://securelist.com/files/2016/08/Kaspersky_Telecom_Threats_2016.pdf, 4.

39 Franklin D. Kramer, Robert J. Butler, Catherine Lotrionte, *Cyber, Extended Deterrence, and NATO*, Atlantic Council, 2016, http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf, 2.

In a recent report, the US government similarly determined that "in foreign countries, RIS [Russian] actors conducted damaging and/or disruptive cyber attacks, including attacks on critical infrastructure networks."[40] Those vulnerabilities present an inviting target and can have not only peacetime effects, but also consequences for deterrence and conflict, as militaries rely heavily on telecommunications and the electric grid for intelligence, operations, logistics, and communications. In a high-end conflict, the almost certain likelihood is that multiple cyberattacks would be repeated. In a network-centric world, vulnerabilities in the cyber domain can have rapid follow-on effects of highly negative consequence. For example, if an adversary were to carry out simultaneous attacks on electric, communications, and financial sectors, these would produce "cascading failures" and "compound problems for infrastructure restoration."[41]

Cyberattacks can, of course, focus on information as well as critical infrastructure. For example, Russian cyberattacks targeted the German Bundestag, gaining access to fourteen servers, including the main one, which contained "all access data to the German parliament."[42] German authorities were able to attribute the attack to a Russian military intelligence agency. Officials also cited "a number of attacks following the same pattern in recent years, targeting German defense companies and other NATO countries."[43]

Economic and Political Coercion and Subversion

Economic and political coercion and subversion are a third key element of Russia's hybrid strategy. A Chatham House analysis emphasized Russia's ability to "purchase or co-opt business and political elites to create loyal or at least compliant networks."[44] The study describes how the nontransparent and corrupt Russian business culture fosters an environment where bribes and business opportunities can be employed to produce "agents of influence" or "Trojan horses" in foreign governments or organizations, allowing Russia to wield influence in target countries across Europe.[45]

Similarly, a study from the Center for Strategic and International Studies highlighted how Russia has deliberately provided funding and support to disruptive political movements in Europe, which seek to "undermine the Euro-Atlantic orientation of those countries and foster greater support for Russian policies."[46] While cultivating relationships with these types of nationalist parties and autocratic leaders, the Kremlin "strategically exploit[s] vulnerabilities in Central and Eastern Europe's democracies, such as weak governance, underdeveloped civil society space, and underfunded independent media, while cultivating relationships with rising autocratic leaders and nationalist populist parties."[47] This has allowed Russia to develop a vast network of quid pro quo relationships to directly influence political decision-making and penetrate economies across the region.

With these efforts, Russia aims to exploit weak, open systems to hijack foreign countries' governing and economic institutions and organizations, using corruption to further expand its own spheres of influence.[48] These concerns increase when Russia is more integrated into a country's economy. According to one study: "[T]hose countries in which Russia's economic footprint was on average more than 12 percent of its GDP were generally more vulnerable to Russian economic influence and capture."[49]

As an example, energy is an arena where there has been particularly high vulnerability. The *Open Letter to the Obama Administration from Central and Eastern European Leaders* pointed out: "The threat to energy supplies can exert an immediate influence on our nations' political sovereignty, also as allies contributing to common decisions in NATO. That is why it must also become a transatlantic priority."[50]

As the above suggests, these issues are not limited to Central and Eastern Europe. As an Atlantic Council study highlights, in Western states, where there are

40 US Department of Homeland Security and US Federal Bureau of Investigation, *Grizzly Steppe – Russian Malicious Cyber Activity*, Joint Analysis Report, US CERT, 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf, 1.

41 Kramer, Butler, and Lotrionte, *Cyber and Deterrence*, 3-6.

42 "Russia's Propaganda Campaign against Germany," *Spiegel* Online.

43 Ibid.

44 Giles, *Russia's 'New' Tools for Confronting the West*, 40.

45 Ibid.

46 Heather Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook*, Center for Strategic and International Studies, 2016, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf, vi.

47 Alina Polyakova, Marlene Laruelle, Stefan Meister, and Neil Barnett, *The Kremlin's Trojan Horses*, Atlantic Council, 2016, http://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_1213_second_edition.pdf, 4.

48 See, for example, Conley, Mina, Stefanov, and Vladimirov, *The Kremlin Playbook*, x.

49 Ibid., xiv.

50 "An Open Letter to the Obama Administration from Central and Eastern Europe," Radio Free Europe/Radio Liberty, July 16, 2009, http://www.rferl.org/a/An_Open_Letter_To_The_Obama_Administration_From_Central_And_Eastern_Europe/1778449.html.

Both infrastructure and cyber present critical vulnerabilities to Russian hybrid attacks. Left: Power lines from Kiev Hydroelectric Station, taken on April 14, 2013. The 2016 attack on Ukraine's Electric Grid knocked out at least 30 of the country's 135 power substations for about six hours. *Photo credit*: YellowForester/Wikimedia Commons. Right: The Locked Shields 2017 exercise was organized by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, in April 2017. It is the largest and most advanced cyber defense exercise in the world. *Photo credit*: NATO

no comparable concentrations of Russian-speaking minorities with historical or cultural connections to Russia, the Kremlin has shown its ability to use more subtle destabilization tactics centered on: (1) "building political alliances with ideologically friendly political group[s] and individuals, and (2) establishing pro-Russian organizations in civil society, which help to legitimate and diffuse the regime's point of view."[51] The analysis explains:

> Since the 2008 economic crisis, which provoked mistrust in the Western economic model, the Kremlin saw an opportunity to step up its influence operations in Europe's three great powers—France, Germany, and the UK. Russia has developed well-documented relationships with anti-EU, far-right political parties and leaders. The influence strategy is tailored to each country's cultural and historical context. In some cases, such as the National Front in France, the Kremlin's financial support for such parties is explicit . . . in the UK, it is more opaque as the UK remains more resistant to the Kremlin's efforts. While the on-and-off leader of the UK Independence Party, Nigel Farage, is unabashedly pro-Russian, other links occur through multiple degrees of separation and chains of operators across sectors . . . And in Germany, network building occurs through organizational cooperation and cultivation of long-term economic links, which open German domestic politics to Russian penetration.[52]

The Estonian Internal Security Service has described the challenge presented by corruption as follows:

51 Polyakova, Laruelle, Meister, and Barnett, *The Kremlin's Trojan Horses*, 4.

52 Ibid., 5-6.

> A corrupt individual can also easily fall into the clutches of powers wishing to damage Estonian national security. Estonian companies operating in strategic economic and industrial sectors and their management are at the same time the objects of increased attention by unfriendly foreign states. They can be used as the means for affecting the Estonian economy and society as a whole. In any case, a corrupt person is easier prey for a hostile power due to greed or vulnerability to blackmail resulting from past actions, without realizing how he or she could be exploited. When laws can be bought and developments directed for one's own benefit, this can be damaging to the country's economic security and jeopardize the workings of the democratic system of government.[53]

The impact of corruption can be substantial, and understanding its reach can be difficult. For instance, corruption in senior levels of government may not be as obvious as lower-level corruption—for example, bribing for permits and licenses—that the public would encounter on a daily basis. But as Estonia's Internal Security Service cautions, "if senior officials set a negative example by their ethical values and actions, these are also spread in the organization or sector; the most dangerous corruption scenario is the takeover of power in the state."[54]

Other countries' intelligence services have seen the same pattern. The Czech intelligence service (BIS) describes: "Major economic interests are of interest also to foreign intelligence services, which aim to gradually win the loyalty of individuals with useful information or decision-making powers. Foreign intelligence services exploit the desires of some individuals to feel important, to secure financial gain or their lack of self-reflection."[55] As in previous years, the Czech report goes on to describe illegal lobbying and concomitant actions by Russian entities, especially toward the legislative process and public administration.[56]

This use of business activity for subversive political ends is an intrinsic feature of Russia's economic and governance systems. As one commentary summarized: "In the end, nobody knows where business ends in Russia and politics begins, and here is the strength but also the very serious danger of the hybrid business model."[57]

Information Warfare

Information warfare is a fourth branch of Russian hybrid warfare. While information warfare is not a new threat, the past few years have shown a sharp increase in Russian information warfare activities. NATO's former Supreme Allied Commander Europe General Philip Breedlove has described Russia's efforts as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[58] Several analyses have confirmed the scope of the effort. For example, a RAND report stated: "Russian propaganda is produced in incredibly large volumes and is broadcast or otherwise distributed via a large number of channels. This propaganda includes text, video, audio, and still imagery propagated via the Internet, social media, satellite television, and traditional radio and television broadcasting."[59]

The overall philosophy is based on the Russian notion of "reflexive control." As the Institute for the Study of War describes: "Reflexive control causes a stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary's perceptions of the situation decisively."[60] A Chatham House study adds to this, explaining the "pollution of the information framework for decision-making is a key element of th[is] long-established Soviet and Russian principle."[61]

The Kremlin uses a variety of techniques in its information warfare efforts, including denying facts, changing quotes, exaggerating, over-generalizing, discrediting, exploiting balance, employing narrative laundering, creating context, drowning facts with

53 Estonian Internal Security Service, *Annual Report*, 2015, https://www.kapo.ee/sites/default/files/public/.../Annual%20Review%202015.pdf, 35.

54 Ibid.

55 Czech Annual Report of the Security Information Service, 2015, https://www.bis.cz/vyrocni-zpravaEN890a.html?ArticleID=1104, 2.1

56 Ibid.

57 Mark Galeotti and Anna Arutunyan, "Commentary: Hybrid Business – The Risks in the Kremlin's Weaponization of the Economy," Radio Free Europe/Radio Liberty, July 20, 2016, http://www.rferl.org/a/russia-commentary-hybrid-business-weaponization-economy/27869714.html, 12.

58 Peter Pomerantsev, "How Russia Is Revolutionizing Information Warfare," Defense One, 2014, http://www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635/.

59 Christopher Paul and Miriam Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model*, RAND, 2016, http://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf, 2.

60 Maria Snegovaya, *Putin's Information Warfare in Ukraine*, Institute for the Study of War, 2015, http://understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf, 7.

61 Giles, *Russia's 'New' Tools for Confronting the West*, 41.

emotion, presenting opinions as facts, and using false facts or visuals, misleading titles, loaded metaphors, and conspiracy theories.[62] Different tactics are tailored for different countries. For instance, in Eastern Europe, Russian TV is used to target Russian-speaking populations, while in the Visegrad countries (Poland, Czech Republic, Slovakia, and Hungary), hundreds of disinformation websites are promoted. In Nordic countries, on the other hand, Russian "web-brigades" are more commonly used as trolls to spark tensions with controversial posts online.[63]

An Atlantic Council study summarizes the Russian effort as follows:

> Through its state-sponsored global media network, which broadcasts in Russian and a growing number of European languages, the Kremlin has sought to spread disinformation by conflating fact and fiction, presenting lies as facts, and exploiting Western journalistic values of presenting a plurality of views. Through its network of political alliances across the post-Soviet space, Russia seeks to infiltrate politics, influence policy, and inculcate an alternative, pro-Russian view of the international order. Whereas the ultimate goal in the near abroad is to control the government or ensure the failure of a pro-Western leadership, in Europe, the goal is to weaken NATO and the EU.[64]

Media

The Kremlin invests hundreds of millions of dollars in media operations across about one hundred countries. This includes its RT outlet, which combines entertainment programs and manipulated Russian news content, as well as Sputnik, a Russian state-funded news agency often accused of acting as "a mouthpiece for the Kremlin."[65] Other Russian news agencies and outlets are also used to disseminate the Kremlin's messaging, alongside local media, which serve as force multipliers in these efforts.[66]

Russia's media efforts are both concerted and multifaceted. One study found:

> All news reports are created by professionals from Russian news agencies and disseminated further by paid Russia[n] supporters, and unwittingly by those who end up believing this version of the news. The biggest advantage of this way of spreading the message lies in that they are not produced generically, but are especially crafted for a specific audience, and presented in their native tongue, ensuring that the target audience is reached in a straight-forward manner, without the need of translation.[67]

Cyber activities

Cyber activities more broadly are critical to Russia's information warfare. A RAND study explains that "in addition to acknowledged Russian sources like RT, there are dozens of proxy news sites presenting Russian propaganda, but with their affiliation with Russia disguised or downplayed."[68] Russia also takes advantage of social media as "the most effective tool for influencing the minds of huge communities, even whole nations."[69] To do this, the Kremlin employs social media trolls to orchestrate targeted online attacks using fake accounts, false information, hate speech, and provocative language. According to Radio Free Europe/Radio Liberty reports, there are "thousands of fake accounts on Twitter, Facebook, LiveJournal, and vKontakte maintained by Russian propagandists."[70] The accounts are run by hundreds of young employees, organized in so-called "troll factories," who write blogs, posts, or comments for news and other websites that support the Kremlin.

As a Chatham House study notes, these troll campaigns are not "static, but instead constantly develop new approaches not yet reflected in mainstream reporting or popular awareness."[71] This increases their effectiveness and ability to respond to countermeasures. In some examples, "ringleader accounts designed to look like real people push organized harassment—including threats of violence—designed to discredit or silence people who wield influence in targeted realms, such as foreign policy or the Syrian civil war. Once the organized hecklers select a target, a variety of volunteers will join in, sometimes

62 See "Information Warfare Initiative: Techniques," Center for European Policy Analysis, 2016, http://infowar.cepa.org/Techniques.

63 Georgi Gotev, "Commission Official: Russian Propaganda Has Deeply Penetrated EU Countries," Euractiv, 2016, http://www.euractiv.com/section/global-europe/news/thurs-commission-official-russian-propaganda-has-deeply-penetrated-eu-countries/.

64 Polyakova, Laruelle, Meister, and Barnett, *The Kremlin's Trojan Horses*, 3-4.

65 "Russian News Agency Sputnik Sets Up Scottish Studio," BBC, 2016, http://www.bbc.com/news/uk-scotland-scotland-politics-37036900.

66 Tomáš Čižik, *Information Warfare: Europe's New Security Threat*, Center for European and North Atlantic Affairs, 2016, http://cenaa.org/en/wp-content/uploads/2016/03/POLICY-PAPERS-Čiž%C3%ADk.pdf, 3.

67 Ibid.

68 Paul and Matthews, *The Russian 'Firehose of Falsehood,'* 2.

69 Giles, *Russia's 'New' Tools for Confronting the West*, 41.

70 Paul and Matthews, *The Russian 'Firehose of Falsehood,'* 2.

71 Giles, *Russia's 'New' Tools for Confronting the West*, 44-46.

as a result of the target's gender, religion, or ethnic background."[72] These campaigns are "augmented by the ubiquitous activities of trolls (online profiles run by humans) and bots (run by automated processes), which exploit specific features of the relationship between traditional and social media in order to plant, disseminate and lend credibility to disinformation."[73]

Soft power

Information warfare is not only conducted through cyber activities and other media channels. Russia also maintains influence through organizations and civil society, which the Kremlin manipulates to deliver its messages and shape its preferred narrative. As several studies have indicated, Russian and Russia-funded government-organized nongovernmental organizations (GONGOs), NGOs, and other organizations are part of a broader network designed to support Russian interests, propagate Kremlin-backed anti-Western narratives, undermine transatlantic values and institutions, and legitimize the Russian government's actions by cultivating—or rather coercing—public support.[74] One study described how outside Russian borders—for instance, in the Baltic countries—the Kremlin uses "the Russian-speaking minority and compatriot organizations to exert influence," control the narrative, and shape public opinion.[75]

Elections

Russia's information warfare can significantly affect the functioning of democracy. A primary objective of the efforts just described is to sow distrust in democracy and the transatlantic institutions that stand behind it. As one study stated, "In the Czech media sphere, Kremlin propaganda efforts are not as focused on challenging individual facts, but rather 'framing the debate' in a way that is sympathetic with Moscow's goals."[76] Recently, the Kremlin has amped up its efforts by interfering with public opinion and democratic elections.

The EU has alleged that Russian propaganda was used to interfere in important referendums in the Netherlands and Britain in 2016, including with the historic Brexit vote.[77] The key elections in Germany and France have increased the growing concern among European officials about Russian interference. In an interview with Reuters, German intelligence agency chief Hans-Georg Maassen lamented: "Last year we saw that public opinion in Germany was influenced by the Russians. This could also take place next year, and we're alarmed." He explained: "We feel that this is part of a . . . hybrid threat, where public opinion and decision-making are being influenced."[78] Russia has also been accused of interfering with the recent French presidential elections. The campaign manager for Emmanuel Macron, the new president, accused RT and Sputnik of being "the first source of false information shared" about Macron. He also divulged that "during the same period, with the same rhythm," the campaign has been a victim of hacks on its servers, as was undertaken just before the French presidential vote.[79]

Russia's ability to combine disinformation efforts with cyberattacks has led to the emergence of hack-and-release tactics that involve obtaining information and using it to influence public officials or opinion. This involves a broadening of the practice of *kompromat*,[80] directed not only to individuals but also to groups and institutions. According to one analysis,

> The way it works is simple: Kremlin insiders or other powerful individuals buy, steal or manufacture incriminating information about an opponent, an enemy, or any other person who poses a threat to powerful interests. Then, they publish it, destroying the target's reputation in order to settle public scores or manipulate public events. Rather than using the information seized for intelligence purposes, the hackers select damaging excerpts from the cache of stolen data, and then leak them at a pivotal moment in [an] election.[81]

72 Andrew Weisburd, Clint Watts, and Jim Berger, "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," War on the Rocks, November 6, 2016, https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

73 Giles, *Russia's 'New' Tools for Confronting the West*, 44-46.

74 See Vojtíšková, Novotný, Schmid-Schmidsfelden, and Potapova, *The Bear in Sheep's Clothing*, 11; and Polyakova, Laruelle, Meister, and Barnett, *The Kremlin's Trojan Horses*.

75 Vojtíšková, Novotný, Schmid-Schmidsfelden, and Potapova, *The Bear in Sheep's Clothing*, 21.

76 Tony Wesolowsky, "Kremlin Propaganda in Czech Republic Plays Long Game to Sow Distrust in EU," Radio Free Europe/Radio Liberty, June 16, 2016, http://www.rferl.org/a/czech-kremlin-propaganda-plays-long-game-sow-eu-distrust/27802234.html.

77 Ibid.

78 "German Intelligence Services 'Alarmed' about Potential Russian Interference in Elections," Deutsche Welle, November 16, 2016, http://www.dw.com/en/german-intelligence-services-alarmed-about-potential-russian-interference-in-elections/a-36413582.

79 Andy Greenberg, "Hackers Hit Macron With Huge email Leak Ahead of French Election," *Wired*, May 5, 2017, https://www.wired.com/2017/05/macron-email-hack-french-election/.

80 In Russia, *kompromat* (literally "compromising material") is compromising information about a politician or other public figure used to create negative publicity or blackmail, ensuring loyalty.

81 Amanda Taub, "DNC Hack Raises a Frightening Question:

US officials and analysts have asserted that this kind of Russian operation was behind the recent hack of the Democratic National Committee (DNC), and a broader attempt to influence the 2016 US presidential elections. In a joint statement in October, the US Intelligence Community explained it was "confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations" and that the "thefts and disclosures [we]re intended to interfere with the US election process."[82] The statement also explained, "Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there."[83]

The Office of the Director of National Intelligence's January 2017 report on Russian activities in the 2016 US presidential election also stated:

> Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.[84]

II. CRITICAL STEPS

Responding to Russia's hybrid challenge requires a comprehensive strategic approach that addresses the multifaceted aspects of hybrid warfare. The objective of any such strategy would be to contain, by limiting and counteracting, Russian hybrid efforts. Fundamental elements of the strategy should be effective defensive efforts, a capacity for resilience in the face of Russian actions, and, as appropriate, cost-imposing measures. A strategy to meet hybrid challenges is not, of course, the entirety of a Western strategy for Russia. An overall strategic approach would include deterrence at the conventional and nuclear levels, diplomacy to determine whether areas of potential cooperation exist, and engagement in the rules-based international order to the extent that Russia will abide by international norms. A counter-hybrid strategy is just a part—though a very important part—of the greater strategic whole. In its implementation, five main efforts are required. As noted above, the following recommendations begin with functional proposals and then conclude with a recommendation to create a coordinating entity to help guide the efforts of NATO, the EU, their nations, and the private sector to maximize the effectiveness of Western responses.

1) Low-Level Use of Force

Low-level use of force is a significant concern for the eastern nations of the EU and NATO, particularly the Baltic states. Moreover, as low-level use of force can morph intentionally or by miscalculation into full-scale conflict, all NATO and EU countries have a substantial interest in deterring or containing such activities. Both institutional and functional actions are needed to deter low-level use of force or to respond if and as required.

Key efforts to address low-level use of force should include:

Enhanced Intelligence by Creating an Eastern Hub: NATO has recently established a "hub" focused on the south, with the aim of increasing the Alliance's ability to coordinate and boost understanding of the threats emanating from Europe's south and NATO's ability to address them.[85] In a press conference, NATO's Secretary General Jens Stoltenberg announced that NATO expects the hub to be staffed by around one hundred people responsible for "assessing potential threats and engaging with partner nations and organizations."[86] Allies could adapt this model to address the Russian hybrid threat by creating a comparable hub focused on the East, but ideally including participation from

What's Next?" *New York Times,* July 29, 2016, https://www.nytimes.com/2016/07/30/world/europe/dnc-hack-russia.html.

82 "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security," The US Intelligence Community, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, 1.

83 Ibid.

84 Office of the Director of National Intelligence, *Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution*, January 6, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf, ii.

85 Jens Stoltenberg, "Pre-ministerial Press Conference," NATO, February 14, 2017, http://www.nato.int/cps/en/natohq/opinions_141005.htm

86 "Press Conference by NATO Secretary General Jens Stoltenberg Following the Meeting of the North Atlantic Council at the Level of Defense Ministers on Deterrence and Defense," NATO, February 15, 2017, http://www.nato.int/cps/en/natohq/opinions_141109.htm.

the EU. This should include EU nations—such as Sweden and Finland, who would bring valuable contributions—as well as EU institutional capabilities, such as the EU's Intelligence Analysis Center (INTCEN), which provides in-depth analysis, early warning, and situational awareness for EU decision makers and member states.[87] Another asset is the EU's Hybrid Fusion Cell,[88] which acts as "a focal point for indicators and warnings of hybrid attack that are noted by the EU institutions."[89] These capabilities, along with support from NATO's new Assistant Secretary General for Intelligence and Security (ASG-I&S),[90] should be used to support the proposed Eastern Hub. Assessment of Russian intentions, capabilities, and activities would provide the requisite initial agenda for this hub.[91] If NATO creates its planned joint hybrid analysis center[92] under the ASG-I&S, this entity may also serve a similar function to the hub.

Expanded Training and Operations: Two key aspects of responding to low-level use of force will be a) the ability of the domestic security forces, such as police and border guards, to work with the military, and b) for a nation facing such a conflict to have sufficient personnel to respond, which may require a surge capacity from allies. To achieve these capabilities:

- NATO and the EU should coordinate efforts of military special forces and the European Gendarmerie Force to physically protect critical infrastructure in the event of low-level conflict. Those groups can work with national police and militaries to develop contingency plans and undertake exercises for resilience support and hybrid defense. While the European Gendarmerie Force was established to operate outside European Union borders, as the hybrid challenge has now manifested within Europe, the force should become available for Europe's own protection. This would still maintain the spirit of its mandate, which is to "strengthen international crisis management capacities and to contribute to the development of the Common Security and Defense Policy in accordance with Article 42.3 of the Treaty on the European Union."[93]
- For countries with existing NATO Force Integration Units (NFIUs) and/or multinational battalions, a network should be established to increase information sharing and operational capabilities between those entities and the European Gendarmerie Force, as well as FRONTEX, the European Border and Coast Guard Agency, and its European Border Guard Teams (EBGTs).[94] The EBGTs are made up of personnel from member states and are "experts in different areas of border management including land and sea border surveillance, dog handling, identification of false documents, and second-line activities such as establishing nationalities of irregular migrants detected at the border."[95] These individuals would be valuable assets for NATO's new Enhanced Forward Presence[96] on the ground in Eastern Europe and the NFIUs responsible for their integration.

87 "EU Intelligence Analysis Center (INTCEN) Fact Sheet," AskTheEU.org, 2016, https://www.asktheeu.org/en/request/637/response/2416/attach/5/EU%20INTCEN%20Factsheet%20PUBLIC%20120618%201.pdf, 1.

88 Council of the European Union, *Food-for-Thought Paper, Countering Hybrid Threats*, available on Statewatch, May 13, 2015, http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf, 7; and Council of the European Union, *Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats 'EU Playbook*,' available on Statewatch, July 7, 2017, http://statewatch.org/news/2016/jul/eu-com-countering-hybrid-threats-playbook-swd-227-16.pdf.

89 European Commission, *EU Joint Framework for Countering Hybrid Threats*, April 6, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en.

90 NATO's new assistant secretary general for intelligence and security is responsible for providing intelligence support to the North Atlantic Council and the Military Committee, advising the secretary general on intelligence and security matters, setting up a new Joint Division, and thus merging NATO's civilian and military intelligence strands.

91 If NATO does not establish such a hub, an alternative would be for this capability to overlap or reside within the new European Centre of Excellence for Countering Hybrid Threats, hosted by the government of Finland, established in April 2017.

92 "NATO Representative Shea: Alliance Has Learned Much from Ukraine's Experiences in Countering Russian Propaganda, Interfax-Ukraine," Interfax, April 4, 2017, ("We have also created a new NATO intelligence division, which will produce a hybrid fusion center."), http://en.interfax.com.ua/news/interview/413634.html.

93 The European Gendarmerie Force is a multinational initiative made up of seven member states—France, Italy, the Netherlands, Poland, Portugal, Romania, and Spain—established by treaty. It allows member states that together establish multinational forces to also make them available to the common security and defense policy. See "The European Gendarmerie Force," European Gendarmerie Force, http://www.eurogendfor.org/organisation/what-is-eurogendfor.

94 European Border Guard Teams (EBGTs) refers to the new Frontex regulation, which came into force in December 2011 and specifies that Frontex will create EBGTs for deployment in Frontex *joint operations and rapid border interventions*. The EBGT is composed of border guards from the EU member states.

95 See "European Border Guard Teams," Frontex, http://frontex.europa.eu/operations/european-border-guard-teams/. "Member States will contribute border guards to this pool based on the specific expert profiles developed by Frontex."

96 As agreed at the 2016 NATO Warsaw Summit, NATO's Enhanced Forward Presence includes the deployment of four multinational battalions to Poland and the Baltic states to deter Russian aggression in the region.

Coordination of military, police, and domestic security forces will be valuable in defending against hybrid action. Left: The UK-led Enhanced Forward Presence battle group deployed to Estonia on April 21, 2017, working with Estonian, French, and Danish partners. *Photo credit*: UK Ministry of Defence. Right: The Carabinieri paratroopers "Tuscania" marching in the Army Parade in Rome on June 2, 2006. *Photo credit*: Jollyroger/Wikimedia Commons.

Combined NATO-EU National Assessments for Critical Infrastructures: Existing efforts, including NATO's seven baseline requirements for national resilience[97] and the European Programme for Critical Infrastructure Protection (EPCIP),[98] should be harmonized and implemented in a seamless fashion. NATO's resilience standards provide helpful benchmarks against which allies can measure their level of preparedness, and the EU's EPCIP has highlighted the importance of contingency planning. Working together, rather than separately, would greatly improve results, especially as each organization's efforts are directed toward the same critical infrastructures.

A crucial aspect will be to integrate relevant private sector entities into assessment and protection efforts. NATO should use its existing Advisory Support Teams (ASTs) structure, which is made up of small units able to undertake assessments and provide support

97 NATO's baseline standards for resilience, as anchored in Article 3, include assured continuity of government and critical government services; resilient energy supplies; the ability to deal effectively with uncontrolled movement of people, and to de-conflict these movements from NATO's military deployments; resilient food and water resources; the ability to deal with mass casualties; resilient civil communications systems; and resilient transport systems. See "Resilience and Article 3," NATO, 2016, http://www.nato.int/cps/en/natohq/topics_132722.htm.

98 The EPCIP seeks to improve the protection of critical infrastructures in the EU by creating an EU framework for that purpose, which includes "a procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures; measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN); the use of CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies; support for Member States concerning National Critical Infrastructures (NCI); contingency planning; an external dimension; and accompanying financial measures." See Commission of the European Communities, *Communication from the Commission on a European Program for Critical Infrastructure Protection*, December 12, 2006, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN, 3-4.

to nations, in this instance to focus on resilience.[99] Comparable personnel should be provided from EU staffs to work with the ASTs. The teams should focus joint efforts on the Baltic countries, as well as Poland, Romania, and Bulgaria, which are frontline states in terms of the need to respond to critical infrastructure vulnerability. The new European Center of Excellence for Countering Hybrid Threats, hosted by the government of Finland with several participating NATO and EU members, could potentially provide a useful venue for developing assessments, doctrine, and training—particularly on how to integrate public with private sector efforts.[100]

> "The new European Center of Excellence for Countering Hybrid Threats [in Finland] . . . could potentially provide a useful venue for developing assessments, doctrine, and training."

Coordinated Force Planning: NATO and the EU have taken some steps to harmonize their respective force planning processes, stating they intend to "pursue coherence of output between the NATO Defense Planning Process (NDPP) and the EU Capability Development Plan through staff-to-staff contacts and invitations for EU staff to attend NDPP and Planning and Review Process (PARP) screening meetings upon invitations by the individual countries concerned."[101] This is a worthwhile step, but it discounts the reality, as recognized by all concerned, that "nations only have one single set of forces."[102] Because the overlapping nations of NATO and the EU can contribute only so many resources, a much stronger coordination mechanism is necessary. To be sure, the EU and NATO staffs may differ on prioritization, but this is precisely the type of difference that requires resolution. There are multiple ways to create a resolution mechanism; one is the Coordinating Council approach discussed later.

Coordination of Potential Responses under Articles 4 and 5 of the North Atlantic Treaty and Articles 42.7 and 222 of the Lisbon Treaty: As noted, low-level use of force can morph into conventional warfare. It would be very important to have coordinated responses by NATO and the EU in the event of the potential for such a transition. Of course, there would be high-level political dialogue at such times, but effective working-level interactions between the institutions should take place simultaneously. Again, the Coordinating Council described later could oversee such efforts.

Use of Legal Tools: In some cases of hybrid action, where international or national laws are broken, EU and NATO nations should use legal tools, such as indictments, forfeitures, and sanctions, to limit and deter future Russian illegal actions. The US demonstrated the use of these legal tools with its recent indictment of four Russian individuals, including two members of the FSB, for theft of information from Yahoo,[103] and its previous indictment of five Chinese military hackers for "computer hacking, economic espionage, and other offenses directed at 6 American companies."[104] These cases represent significant steps toward developing proportionate, concrete penalties for purposefully low-level hybrid actions. Using Russia's illegal abduction of Estonia's border guard officer as an example, Estonian authorities should be able to indict the Russian operatives they believe to be behind the attack. This model can be applied to other instances of hybrid conflict such as cyberattacks, for example, against France's TV5,[105] and may also be appropriate for certain Russian violations of anti-corruption laws, each discussed below.

99 See the discussion of "resilience support teams" in Franklin D. Kramer and Bantz J. Craddock, *Effective Defense of the Baltics*, Atlantic Council, May 2016, http://www.atlanticcouncil.org/images/publications/Effective_Defense_of_the_Baltics_0516_web.pdf, 12.

100 "NATO Welcomes Opening of European Centre for Countering Hybrid Threats," NATO, April 11, 2017, http://www.nato.int/cps/en/natohq/news_143143.htm.

101 "Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," NATO, December 6, 2016, http://www.nato.int/cps/en/natohq/official_texts_138829.htm.

102 Ibid.

103 "US Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," US Department of Justice, March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

104 "US Charges Five Chinese Military Hackers for Cyber Espionage against US Corporations and a Labor Organization for Commercial Advantage," US Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

105 Pierre Meilhan and Greg Botelho, "French TV Network Hit by 'Powerful Cyber Attack,'" CNN, April 8, 2015, http://www.cnn.com/2015/04/08/europe/french-tv-network-cyberattack/index.html.

2) Cyberattacks

Cyberattacks affecting operational networks have been demonstrated against multiple entities, including the electric grid (as in Ukraine), the telecommunications system (in both Norway and Poland), and television stations (as in France).[106] Such vulnerabilities add to the risk of conflict in hybrid scenarios and raise the potential for escalation to a high-end conflict. Building on the NATO-EU Joint Declaration, which called for expanded coordination on cybersecurity,[107] and with nations following the model of the UK National Cyber Security Centre,[108] the transatlantic community should develop a coordinated strategy to address these threats.

First, each nation needs an **effective cyber operational approach**. While each country will adapt to its particular circumstances, the recent cyber strategy and organizational structure adopted by the UK provides a useful benchmark against which nations can plan and measure their own efforts. In addition to its new National Cyber Security Centre, the UK has included in its efforts: 1) "government taking a more active cyber defense approach—supporting industry's use of automated defense techniques to block, disrupt and neutralize malicious activity before it reaches the user"; 2) "deterrence [by] strengthening . . . law enforcement capabilities to raise the cost and . . . reduce the reward of cyber criminality . . . ensuring [the UK] can track, apprehend and prosecute those who commit cyber crimes, [and] invest[ing] in offensive cyber capabilities, because the ability to detect, trace and retaliate in kind is likely to be the best deterrent"; and 3) "develop[ing] the capabilities [the UK] need[s] in [its] economy and society to keep pace with the threat in the future."[109] Similar approaches should be adopted by other transatlantic nations.

Second, **contingency plans to deal with cyberattacks** must be established. It is important to differentiate cyberattacks that could be undertaken by a nation-state or a terrorist organization from the multiple day-to-day intrusions undertaken by criminals and even from espionage. Though the techniques of exploitation overlap, the focuses for deterring and defending attacks are different from those of crime and espionage. A useful way to begin the development of the required capabilities would be to consider what would be necessary for a high-end contingency. In such a contingency, military and civil authorities would need to work closely with ISPs and electric grid operators. An effective planning process supported by regular exercises would be particularly important to establish so that, in the event, all parties know what is required of them.[110] In this regard, it will be particularly important for NATO and the EU to coordinate their efforts.

Third, a **working governance structure** should be established among the country's cyber authorities, including the military, its civil governmental authorities, and its ISPs and electric grid operators. As many have pointed out, the telecom and grid structures are in the hands of the private sector in many countries, and establishing an effective interactive mechanism with the government to create protection and resilience in the face of a cyberattack will be critical. Since, for many European countries, critical infrastructures are multinational or have multinational effects, it could be important for there to be a comparable regional structure in appropriate circumstances.

Fourth, **NATO and the EU need to have a consistent set of requirements for cybersecurity** and actively coordinate their cyber activities through working governance arrangements so that appropriate protection, resilience, and recovery is provided with respect to multinational and cascading cyber impacts.

Fifth, it is important to undertake **actions in advance of a cyberattack** to establish the greatest likelihood of effective protection, resilience, and recovery. As numerous analyses have determined, to generate desired results, defenders cannot wait for the actual attack. As noted above, the UK cyber strategy provides for active defense *before* malicious activities reach the user. Thus, as a similar analysis states: "Among other important steps prior to conflict, intrusions must be blocked as much as possible; malware needs to be removed; and capabilities for maintaining data integrity, confidentiality, and availability need to be built and exercised. Critical to this effort is the use of a variety of adaptive resilience techniques, ranging from

106 See footnotes 36, 37, and 102.

107 "Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," NATO.

108 Government of the United Kingdom, *National Cyber Security Strategy: 2016-2021*, 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 20.

109 Philip Hammond, "Chancellor Speech: Launching the National Cyber Security Strategy," Government of the United Kingdom, October 1, 2016, https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy.

110 This section is drawn from Kramer, Butler, and Lotrionte, *Cyber and Deterrence*. Contingency planning as well as other points set forth in this section are discussed at greater length in that report.

diversity and redundancy to moving target defenses and deception."[111]

Sixth, not all nations of NATO or the EU have substantial cyber capabilities, despite general progress in this regard. Accordingly, nations with high-end capabilities—in particular, the United States, Canada, Germany, and the United Kingdom—should act as "**cyber framework nations**" to support other nations' capabilities. While the precise nature of the support would vary from nation to nation, by way of example, this could involve the "establishment, transfer, training, and support of cyber capabilities [to] establish an effective intrusion protection system, provide forensic support, and develop resilience capabilities to be utilized in the event of an attack by an adversary."[112] A first effort should be focused on the Baltic nations and Poland, where NATO multi-national battalions have deployed.

Finally, as noted above, sanctions—and especially multinational sanctions—should be utilized in response to state-sponsored cyberattacks, whether undertaken directly, through proxies, or otherwise supported. Sanctions could not only be directed at immediate actors and supporting entities, but could also include equivalent and proportional responses that would be appropriate to the specific incident and would deter future attacks. Given the multiple and continuing cyberattacks being faced by Western governments and private sector entities, it would be sensible to undertake planning for the type of sanctions that might be called for, so that actions would not be necessarily slower and somewhat ad hoc.

3) Economic and Political Coercion and Subversion

As discussed earlier: "Malign Russian influence in Central and Eastern Europe primarily follows two tracks: one aimed at manipulating a country by dominating strategic sectors of its economy to abuse capitalism and exploit the weaknesses in its economic governance systems; and another that seeks to corrode democracy from within by deepening political divides and cultivating relationships with aspiring autocrats, political parties (notably nationalists, populists, and Euroskeptic groups), and Russian sympathizers."[113]

There are five broad approaches to respond to such Russian actions. In general, they require increased intelligence, greater transparency, enhancement of anticorruption activities, limitations on Russian financial and political activities, and reduction of key dependencies, particularly in the energy arena.

> "[N]ations with high-end capabilities . . . should act as 'cyber framework nations' to support other nations' capabilities."

Before turning to the specifics, it is notable that Europe has already taken significant actions comparable to those proposed below both in the energy arena through its Energy Security Strategy and in the financial arena through its actions on money laundering. The Energy Security Strategy, for example, was specifically undertaken in "response to concerns surrounding the delivery of Russian gas via Ukraine."[114] This demonstrates the EU has recognized that Russian economic activities can have consequential security implications and require significant responses that, in appropriate circumstances, should be mandatory. As noted, the EU has recently taken comparable action in connection with money laundering by adopting a directive giving tax authorities access to corporate and economic information for the purpose of preventing money laundering. By allowing access to details on the "beneficial ownership of intermediary entities and other relevant customer due diligence information" throughout monitoring efforts, the directive will help prevent tax evasion and fraud.[115]

In keeping with these approaches to energy security and money laundering, the following recommendations are proposed responses to address the Russian economic and political subversive activities already described.

First, **increased intelligence** is necessary, as no effective response can be generated without a solid understanding of the context. As previously described, several national intelligence services have published useful reports of Russian activities in their countries. Greater sharing and a centralized data bank would

111 Kramer, Butler, and Lotrionte, *Cyber and Deterrence*, 2.

112 Ibid, 19.

113 Conley, Mina, Stefanov, and Vladimirov, *The Kremlin Playbook*, x.; "An Open Letter to the Obama Administration," Radio Free Europe/Radio Liberty.

114 "Imports and Secure Supplies," European Commission, 2016, https://ec.europa.eu/energy/en/topics/imports-and-secure-supplies.

115 "Taxation: Council Adopts Directive on Access to Beneficial Ownership Information," Council of the European Union, December 12, 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-beneficial-ownership-information/. The directive will apply as of January 1, 2018.

enhance the ability of nations to understand Russian subversion efforts. The proposals above include the suggestion of an Eastern Hub for integrating and assessing Russian activities relevant to low-level use of force. Such a hub could also be used for intelligence on economic issues and as a central clearinghouse for individual nations, NATO, and the EU. Alternatively, a separate effort could be created (for example, at the recently established European Center of Excellence for Countering Hybrid Threats in Finland). This effort could, of course, integrate intelligence from existing entities such as the EU's INTCEN and NATO's ASG-I&S. Overall, the key point is that Russian actions involve multiple countries, and therefore their review should include a multinational effort.

Second, **greater transparency** on Russian actions should include two aspects. As a starting point, the intelligence information collected should regularly be made public in an appropriate fashion. As already noted, the Czech and Estonian intelligence services issue annual reports with useful descriptions of Russian activities. All countries should undertake similar reporting, and the proposed hub, or some similar group, could bring together the reports in a centralized fashion on an annual basis. Alternatively, this could be done at the EU or NATO level. In addition, all economic actions by Russia of any consequential size should be reported to national authorities and the EU. For example, Russian acquisition of more than a certain percentage of—or significant loans or other financial arrangements with—public companies should require such reporting, especially if related to a country's critical infrastructures, including telecommunications, electric grid and other energy, banking, and finance. As underscored by a Transparency International report, it is critical to have "publicly accessible registries of beneficial ownership information in order to break the vicious cycle of impunity that hidden ownership allows. The identification of who controls a company and its profits will increase financial transparency and help to stop the corrupt."[116]

Third, **enhanced anti-corruption measures focused on Russia** should be implemented at the EU level and in conjunction with nations. Europe already has a substantial existing anti-corruption framework under the auspices of the Council of Europe. The framework includes legal instruments such as the Criminal Law Convention on Corruption[117] and the Civil Law Convention on Corruption,[118] as well as implementation mechanisms including the Group of States against Corruption, which undertakes "monitoring [and] compliance with Council of Europe anti-corruption standards."[119] The European Union itself issued an anti-corruption report in 2014,[120] although recently it declined to issue a follow-up report.[121] However, as the discussion earlier demonstrates, none of these efforts have kept Russia from its efforts to "purchase or co-opt business and political elites to create loyal or at least compliant networks."[122] Accordingly, a more focused anti-corruption effort specifically targeted to Russian actions should be implemented. As noted earlier, the EU has adopted strong anti-money laundering measures to meet, in part, terrorist actions.[123] Anti-corruption measures should comparably be developed that focus on Russian activities—the key being investigation and implementation of anti-corruption laws. The EU should provide funding and personnel necessary to undertake effective enforcement.

Fourth, **limitations on Russian financial and political activities** should be established. As a first step, there should be a bar on support to political parties by Russia and Russian-controlled entities. An important second step would be to enhance existing European mechanisms that review foreign investments or other financial transactions by focusing specifically on actions by Russian entities that could lead to detrimental impacts on the national security, economy, and/or the democratic functioning of a country.

There are already limitations on foreign investment in key transatlantic countries including France, Germany, Italy, and the United States. As described in a Congressional Research Service analysis:

> **France.** The French Minister of Economy issued a decree in 2014 that amended the list of foreign investment activities that are

116 Transparency International, *Ending Secrecy to End Impunity: Tracing the Beneficial Owner*, February 2014, http://www.transparency.org/whatwedo/publication/policy_brief_02_2014_ending_secrecy_to_end_impunity_tracing_the_beneficial, 1.

117 "Chart of Signatures and Ratifications of Treaty 173," Council of Europe, January 5, 2017, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/173/signatures?p_auth=WyH2OA7L.

118 "Details of Treaty No. 174," Council of Europe, 2017, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/174.

119 "What Is GRECO?" Council of Europe, 2017, http://www.coe.int/en/web/greco/about-greco/what-is-greco.

120 European Commission, *Anti-Corruption Report*, February 3, 2014, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/corruption/anti-corruption-report_en.

121 Nikolaj Nielsen, "EU Commission Drops Anti-Corruption Report," EU Observer, February 2, 2017, https://euobserver.com/institutional/136775.

122 Giles, *Russia's 'New' Tools for Confronting the West*, 40.

123 "Press Release: Commission Strengthens Transparency Rules to Tackle Terrorism Financing, Tax Avoidance, and Money Laundering," European Commission, July 2016, http://europa.eu/rapid/press-release_IP-16-2380_en.htm.

subject for review to include activities that are considered essential to safeguard national interests in public order, public security and national defense. The list includes the sustainability, integrity and safety of (1) energy supply (electricity, gas, hydrocarbons or other sources of energy); (2) water supply; (3) transport networks and services; (4) electronic communications networks and services; (5) operation of a building or installations of vital importance; and (6) protection of public health.

Germany. In 2009, Germany amended its legislation to prohibit investments by investors from outside the EU and the European Free Trade Association that threaten to impair public security or public order.

Italy. In 2012, Italy established a new mechanism for government reviews of transactions regarding assets of companies operating in the defense or national security sectors, and strategic activities in the energy, transport and communications industries.[124]

Similarly, the UK recently announced that it was going to give greater scrutiny to foreign acquisitions of critical infrastructure transactions—though, in that case, in connection with proposed Chinese investment in a nuclear plant.[125] The concept of greater scrutiny is similarly the rationale behind US activities by the Committee on Foreign Investment in the United States.[126]

The key element for an enhanced European mechanism, as each of the national mechanisms suggests, is that criteria focused on particular issues can be created, relevant to the context of economic and political subversion. A new European mechanism at the EU level could determine which would be key factors and then implement an appropriate approach to review them as, for example, has been done in the money laundering realm.[127]

Fifth, there should be **increased emphasis on reducing key dependencies**, particularly in the energy arena. The EU Energy Security Strategy is an entirely worthwhile effort; the issue is whether more needs to be done to implement its objectives. In the energy arena, a reasonable goal should be to make Russia simply a market participant, not an oligopolistic entity with excess power over any country. To accomplish that, one approach would be to much more actively promote alternative sources, such as Lithuania has recently done concerning gas,[128] so that Russia is not a majority provider of any energy resource. This would necessarily require significant changes in the market including the development of requisite infrastructures, but the security benefits would be highly valuable.

4) Information War

As discussed earlier, the challenge of the information war derives from substantial Russian propaganda efforts, including through Russian news agencies directly acknowledged by the Russian government and unacknowledged actions such as fake sites, Internet trolls, and hack-and-release tactics. Both public and private authorities have taken actions in response to these threats, but the results have not been sufficient to undercut the effectiveness of Russian efforts. Accordingly, the transatlantic community needs an expanded strategy.

While the current efforts of NATO, the EU, and individual nations are all worthwhile, it would be highly valuable to focus enhanced efforts on limiting Russian interference in elections, discrediting the main sources of Russian disinformation, and enhancing the resilience of the citizenry by assuring available balanced media and information flows.

First, **develop a comprehensive response to election interference**, which could include:

124 James K. Jackson, *The Committee on Foreign Investment in the United States (CFIUS)*, Congressional Research Service, April 6, 2016, https://fas.org/sgp/crs/natsec/RL33388.pdf, 31.

125 "Government Confirms Hinkley Point C Project Following New Agreement in Principle with EDF," United Kingdom Department for Business, Energy, and Industrial Strategy, September 15, 2016, https://www.gov.uk/government/news/government-confirms-hinkley-point-c-project-following-new-agreement-in-principle-with-edf.

126 Among other factors considered under CFIUS are: "(3) the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security . . . (6) the potential national security-related effects on United States critical infrastructure, including major energy assets; (7) the potential national security-related effects on United States critical technologies; (8) whether the covered transaction is a foreign government-controlled transaction." See Section 721 of the Defense Production Act of 1950, codified at 50 U.S.C. App. 2170.

127 The process could review "(1) the threat, which involves an assessment of the intent and capabilities of the acquirer, (2) the vulnerability, which involves an assessment of the aspects of the . . . business that could impact national security, and (3) the potential national security consequences if the vulnerabilities were to be exploited." See "EU Commission Drops Anti-Corruption Report," US Department of the Treasury, April 1, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl0401.aspx.

128 "Lithuania to Manage without Gazprom's Gas Auctions," The Baltic Course, September 20, 2016, http://www.baltic-course.com/eng/energy/?doc=124192.

Substitution of non-Russian sources will enhance European energy security. Left: The liquefied natural gas (LNG) terminal in Klaipeda, Lithuania. *Photo credit*: ©KN. Right: LNG Tanker in Kenai, Alaska. *Photo credit*: ConocoPhillips Company.

- a voluntary code of standards for online media-provided information in the context of elections, which could build on the existing *Code of Conduct on Countering Illegal Hate Speech Online* and further draw from national legal requirements regarding defamation, privacy, and objectivity (such as in Germany and the United Kingdom);
- working with private sector online companies to block and/or limit the reach of Russian information efforts aimed at impacting elections that do not meet the criteria of the voluntary code;
- national governments having the capacity to fine, sanction, close the bank accounts of, restrict funding to, or suspend operating licenses of foreign or foreign-directed media in the event of demonstrated election interference (similar to what the UK's Ofcom did with RT when it was found to be in flagrant violation of UK objectivity regulations with certain coverage); and
- the use of multinational sanctions and other legal limitations in the event of demonstrated election interference.

As discussed above, Russian interference in European and American elections has become a real threat for the transatlantic community. While key officials on both sides of the Atlantic have publicly acknowledged this challenge and its potential to seriously undermine democracy, transatlantic values, and institutions, the West has yet to develop a comprehensive response. Nations have taken important individual steps, for instance, as the United States did when the Barack Obama administration issued sanctions against nine Russian individuals and entities behind the Democratic National Committee hack in late 2016.[129] However, unilateral action can go only so far in deterring these Russian activities, and a unified transatlantic front

129 Natasha Bertrand, "Obama Issues New Sanctions against Russia, Ejects 35 Russian Diplomats over Election-Related Hacking," Business Insider, December 29, 2016, http://www.businessinsider.com/obama-new-sanctions-against-russia-over-hacking-2016-12.

would be significantly more effective. International law fully authorizes responses to intrusions on sovereignty and the electoral process is a key element of the sovereignty of any democratic nation.[130] Moving forward, allies and partners should work together and agree to multilateral action in response to Russian interference in foreign elections, including an online code of conduct, working with the private sector to block pernicious Russian disinformation efforts and the use of sanctions, and countermeasures to respond to such Russian actions.

While it would require thoughtful analysis, a voluntary code of standards for media-provided information in the context of elections could be established by building on the existing *Code of Conduct on Countering Illegal Hate Speech Online* and drawing on legal requirements present in national laws regarding defamation, privacy, and objectivity. For context, in the existing code, the European Commission and EU member states partnered with key information platform companies, including Facebook, Microsoft, Twitter, and YouTube, to establish an innovative, and potentially highly effective, public-private working arrangement to limit the spread of incitement to violence and hate speech online. The parties have agreed to institute guidelines prohibiting hateful conduct on their platforms, and "to have in place clear and effective processes to review notifications regarding illegal hate speech on their services so they can remove or disable access to such content" in an appropriate and timely manner.[131] The information is funneled through national contact points identified by the companies and member states, which further equips member states' law enforcement agencies to recognize and handle illegal hate speech online in the future. The companies provide regular training to their staff, and also work with the Commission and member states to establish partnerships with civil society organizations, who serve as a broader network of expert "reporters" helping to provide valid notices of pernicious online content.[132] This model could be adapted to limit the reach of not just hate speech, but also—in the context of elections—false news, cyber trolls, fake sites being used as fronts for Russian activities, and related threats. The EU could also work to implement this broader media code of election conduct with key online private sector companies, civil society organizations, and journalists who could help monitor for violations.

To identify the key components that could form such a media code of conduct at the EU level, the efforts of national governments in this realm could be reviewed and evaluated to determine their merit at the regional or supranational level. For example, Germany, which has adopted some of the strictest laws[133] aimed at preventing hate speech and harmful online content, formed a new task force among the government, companies, industry associations, and activists that agreed to stricter monitoring rules concerning rising hate speech against refugees.[134] German officials have called for private sector online media companies, such as Facebook, to boost their removal rates to 70 percent within twenty-four hours.[135] At the time of this writing, Germany is also considering legal requirements including significant fines for online platform companies to ensure prompt elimination of hate speech once advised of its existence.[136] In the UK, Ofcom, the regulator and competition authority for UK communications industries, uses its own code of standards to detect biased or manipulated content and take appropriate action to ensure impartial news and information within the country.[137] Lithuania has also taken steps to combat disinformation through its *Law on Provision of Information to the Public*, which helps mandate and ensure that public media information is provided accurately and in an unbiased

130 Sean Watts, "International Law and Proposed US Responses to the DNC Hack," Just Security, October 14, 2016, https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/; Catherine Lotrionte, "Countering State-Sponsored Cyber Economic Espionage under International Law," *North Carolina Journal of International Law*, Vol. 40, No. 2 (Winter 2015), 502 ("For example, manipulating another state's election results through cyber means in order to dictate the winning party would be a coercive act impeding on that state's right to freely decide its own political system"), https://www.law.unc.edu/journals/ncilj/issues/volume40/issue-2-winter-2015/countering-statesponsored-cyber-economic-espionage-under-international-law/.

131 See European Commission, *Code of Conduct on Countering Illegal Hate Speech Online*, 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf, 2.

132 Ibid.

133 Anthony Faiola, "Germany Springs to Action over Hate Speech against Migrants," *Washington Post*, January 6, 2016, https://www.washingtonpost.com/world/europe/germany-springs-to-action-over-hate-speech-against-migrants/2016/01/06/6031218e-b315-11e5-8abc-d09392edc612_story.html?utm_term=.20113442d0a8.

134 Ibid.

135 "Facebook nennt erstmals Zahl entfernter Hasskommentare," Zeit Online, 2016, http://www.zeit.de/digital/2016-09/hasskommentare-facebook-heiko-maas-richard-allan.

136 The German Parliament is set to receive a new bill, which includes levying fines of up to €50 million for not promptly removing defamatory content. See Cara McGoogan, "Germany Threatens to Fine Social Media Companies €50m for Hate Speech and Fake News," *Telegraph*, March 14, 2017, http://www.telegraph.co.uk/technology/2017/03/14/germany-threatens-fine-social-media-companies-50m-hate-speech/.

137 The *Ofcom Broadcasting Code* can be found at https://www.ofcom.org.uk/__data/assets/pdf_file/0005/100103/broadcast-code-april-2017.pdf.

fashion.[138] Upon evaluation, these national efforts could serve as the basis and inform the requirements for the EU-level media code of conduct proposed earlier. These requirements and standards should be clear, specific, and transparent and focused on the context of elections.

In the context of demonstrated election interference, national governments should have the capacity to fine, sanction, close the bank accounts of, or restrict funding to foreign or foreign-directed media. Several nations have already undertaken some valuable efforts in this regard. In one case, for example, the UK's Ofcom, described above, found that RT had breached regulations and code with its coverage of the Ukraine crisis and Syrian conflict, and has accordingly sanctioned the Russian outlet.[139] In light of the Ofcom findings, UK bank NatWest closed the accounts of the UK branch of RT, restricting its financial security and ability to operate in the country.[140] Likewise, Latvia shut down Sputnik's local website in March 2016, criticizing the credibility of its coverage of the Ukraine conflict and denouncing it as a "propaganda tool."[141]

To be sure, there is an important line between protecting publics from false information and limiting free speech. Any measures of this nature empowering governments to control certain flows of information should be based on very clear and specific guidelines and circumstances and implemented only after significant violations. The focus of governmental entities should be on foreign entities and not on citizens of their country. Under international law, governments do have the authority to protect the sovereignty of the country, and this includes the free exercise of elections. Nonetheless, even in the context of elections, governments should work to restrict information from only foreign sources that affect the sovereignty of the country through its pernicious nature, such as inciting violence or hatred, or blatant falsehood reaching the levels comparable to defamation. In the same vein, severe penalties such as sanctions or license suspensions should be reserved only for repeat offenders or in appropriate severe cases. Requirements for objectivity should be agreed upon and penalties should be implemented proportionately to deter violations in the future.

To effectively enforce the proposed code of conduct regarding elections, the transatlantic community should use multinational sanctions and other legal limitations in the event of demonstrated election interference. As important as it was to respond on a multinational basis to Russian actions in Ukraine, it is even more important to ensure that Western democratic elections are free from improper influence. To be sure, nations have and should continue to utilize their own laws in this regard. However, a multinational response to actions in one nation is much more powerful as a response and as a deterrent to future actions.

Second, the transatlantic community should **discredit the sources of Russian disinformation and further develop the capacity to highlight specific Russian disinformation** through:

- widely accessible measures, including, for instance, by establishing a public "dashboard," or other digital means, that identifies the falsity and lack of objectivity of Russian-generated media;
- establishing a fund to support civil society and other private sector efforts to respond to Russian disinformation with a focus on educating journalists, as well as the broader public; and
- enhancing the capacity for countering disinformation within EU and NATO nations and expanding resources for the EU's European External Action Service (EEAS) East StratCom Task Force and other NATO, EU, and national counter-disinformation efforts.

Due to the vast nature of Russian information warfare, it is important to emphasize and discredit the *sources* of disinformation, rather than the pieces of disinformation themselves.[142] Accordingly, a significant campaign should be undertaken to analyze and disrepute, when appropriate, outlets like RT and Sputnik, including through the use of comparative evaluations. A critical

138 Law on Provision of Information to the Public (1996 as amended 2000), *Republic of Lithuania*, December 21, 2000, http://workspace.unpan.org/sites/internet/Documents/UNPAN039762.pdf.

139 "Russia Today's Bank Accounts Closed in UK," Euractiv, October 17, 2016, http://www.euractiv.com/section/global-europe/news/kremlin-funded-rt-television-says-uk-bank-closing-its-accounts/.

140 Ibid.

141 "Latvia Shuts Down Russia's Propaganda Website, Sputnik," Euractiv, March 30, 2016, http://www.euractiv.com/section/global-europe/news/latvia-shuts-down-russias-propaganda-website-sputnik/.

142 One-on-one rebuttals can have the net result of reinforcing the disinformation since, among other things, it is repeated in the rebuttal. See generally, Brendan Nyhan, and Jason Reifler, *Misinformation and Fact-checking*, New America Foundation, February 2012, http://www.dartmouth.edu/~nyhan/Misinformation_and_Fact-checking.pdf ("Attempts to correct false claims can backfire via two related mechanisms. First, repeating a false claim with a negation (e.g., 'John is not a criminal') leads people to more easily remember the core of the sentence ('John is a criminal'). Second, people may use the familiarity of a claim as a heuristic for its accuracy. If the correction makes a claim seem more familiar, the claim may be more likely to be seen as true.").

component here would be to highlight these sources' connections to the Russian regime. These efforts should be conducted openly and presented to the public in accessible, reliable formats. Additionally, governments should undertake efforts to expose front companies and trolling campaigns, emphasizing their ties to Russian governmental activities.

To achieve this, there would be value in having a mechanism that provides prompt evaluations to the public in an easily digestible form. One of the simplest models would be a dashboard, or other digital means, that would flag and focus on particular Russian outlets and/or narrative strands to highlight lack of objectivity including biased, half-truth, and false information. Recent efforts in the digital arena have shown that the technology is available for such efforts, and existing private sector capabilities are outlined below.[143] While this type of dashboard effort could be more far-reaching than a centralized government approach, it could nonetheless use government sources and tools, such as the EEAS East StratCom Task Force, the EU Hybrid Fusion Cell, the NATO press center in Brussels, and the NATO StratCom Center of Excellence in Riga, Latvia, and could be placed on numerous sites—both governmental and nongovernmental. Additionally, the data drawn from the dashboard could be compiled into an annual report, such as those Transparency International releases on corruption, but in this instance focused on Russian disinformation.

Russian disinformation is generally highly distributed and fast-moving, and government efforts tend to be localized and slower than those of the private sector and individuals. Accordingly, supporting private efforts that respond promptly are highly worthwhile. Private journalists, civil society, and various social media all have a role to play. Frequently, these entities lack resources, but some steps have already been taken in this area. For example, at the regional and civil society levels, the Baltic Centre for Media Excellence is designed to provide training to journalists and news outlets in Estonia, Latvia, Lithuania, and other countries of the Eastern Partnership on issues of independence, linguistics, and technological diversity.[144] Likewise, several think tanks and civil society organizations, including the European Endowment for Democracy, the Center for European Policy Analysis, and the Legatum Institute, have launched various projects to highlight and analyze Russian disinformation.[145] However, creating a fund at the EU or NATO (or in combination) level that is focused on supporting such private sector and civil society efforts would have multiplier effects and could be very worthwhile in responding to Russian propaganda. The fund could include two aims: 1) supporting efforts to educate journalists and 2) supporting government efforts to educate and communicate with their publics.

Finally, the resources devoted by governments to address information warfare should be increased. One of the fundamental problems for the success of the Western narrative is that, at the EU and NATO levels, while budgetary resources are provided for countering disinformation and strategic communication efforts, they are often widely spread across a multitude of institutions, departments, projects, teams, and campaigns.[146] In practice, this means communications efforts are often carried out with different levels of attention, in isolation from each other, and in some cases, as a side project for teams focusing on other policy issues. It would be worthwhile to enhance and concentrate some of these efforts, particularly through the EEAS East StratCom Task Force, by increasing resources for its and other governmental information efforts. While, in February 2017, the European Parliament passed a noteworthy resolution calling to turn the East StratCom Task Force into a fully fledged unit of the EEAS with an adequate budget and staff, the EEAS strategic communications division and the comparable NATO unit still remain under-resourced.[147]

Third, **work with the private sector to develop comprehensive available sources of information so that the public has access to and can develop a resilient understanding of today's extensive information flows**.

One of the issues facing any consumer of media is the prospect of being inside an "information bubble," where information supporting only one view is reviewed. Russia's flood of information via media,

143 Amanda Hess, "How to Escape Your Political Bubble for a Clearer View," *New York Times*, March 3, 2017, https://www.nytimes.com/2017/03/03/arts/the-battle-over-your-political-bubble.html.

144 See "About," Baltic Media Center of Excellence, 2016, https://baltic.media/about.

145 Edward Lucas and Peter Pomeranzev, *Winning the Information War*, Legatum Institute, August 2016, https://lif.blob.core.windows.net/lif/docs/default-source/publications/winning-the-information-war-full-report-pdf.pdf?sfvrsn=2.

146 See European Parliamentary Service, "NATO Strategic Communications – An Evolving Battle of Narratives," July 2016, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586600/EPRS_BRI(2016)586600_EN.pdf; and European Union Institute for Security Studies, *Strategic Communications: East and South*, July 2016, http://www.iss.europa.eu/uploads/media/Report_30_Stratcoms.pdf.

147 See "Draft Report on the EU Strategic Communication to Counteract Propaganda against It by Third Parties," European Parliament, 2016, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2016/2030(INI).

trolls, and the like is designed to create such a bubble. An effective response to this would be supporting the "resilient citizen" who can evaluate the nature of what is being provided. While public-supported media can play a role in this, technology, via the private sector, is particularly well-suited to doing so.

In fact, computer scientists and tech giants are beginning to use algorithms and online data to find misinformation more quickly than traditional fact-checkers.[148] For example, Facebook recently decided to add a "fact-check" button for its users in the United States[149] and Germany in light of growing concerns that disinformation on social media is influencing elections around the world.[150] The tool allows users to flag potentially misleading stories, uses an external organization—such as Snopes, PolitiFact, or the Associated Press—to verify content, and then marks false stories as "disputed," attaching an explanation, warning users before sharing, and preventing its promotion in its algorithms.[151] These capabilities help equip society to recognize disinformation. Similarly, the new iPhone app Read Across the Aisle uses a dynamic red-blue meter on various articles to help readers identify a particular site's or outlet's ideological slant.[152] BuzzFeed is also piloting a new feature called Outside Your Bubble, which collects opinions or biased statements from the Internet, removes them from their context, and reframes them as cogent bullet points on a neutral platform.[153] FlipFeed, a Twitter plug-in, can also replace a person's normal Twitter feed with one from a random, anonymous Twitter user with a different political slant, in an effort to help people understand alternative views.

More traditional media are also making helpful strides in this realm. For instance, Washington journalist Will Sommer publishes a weekly digest, *Right Richter*, which "aggregates right-wing perspectives for left-leaning audiences."[154] Slate also publishes *Today in Conservative Media*, a daily roundup of conservative news stories, providing a similar service.[155]

This is not to suggest the sole use of any of these particular efforts, but to illustrate that technology can be used to help provide balanced content and to support the "resilient citizen."[156]

5) The Euro-Atlantic Coordinating Council and a Multinational Coordinated Strategy

As discussed above, hybrid conflict can involve not only the low-level use of force, but also concomitant political, economic, and information activities. No single organization in Europe or North America currently has the structure or capacity to establish a coordinated strategy to meet such challenges. The result is a multiplicity of efforts lacking a unified approach, which has reduced overall effectiveness. Consequently, as a key element of the strategy, the transatlantic community should establish a new entity that can coordinate the efforts of NATO, the EU, individual nations, and the private sector, and provide an overarching approach for creating resilience through coordinated diplomatic, economic, information, security, and military actions. A fundamental value of such coordination would be to demonstrate that the transatlantic community views hybrid attacks on any single nation as a challenge to the whole community that should be dealt with in a common and supportive fashion.

The need for a coordinated approach has been well-recognized by NATO, the EU, and their member states. At the Warsaw Summit in July 2016, NATO Secretary General Jens Stoltenberg, European Commission President Jean-Claude Juncker, and European Council President Donald Tusk signed a joint declaration calling for "new ways of working together" to "boost [the] ability to counter hybrid threats, including by bolstering resilience and working together on analysis, prevention, and early detection through timely information sharing and, to the extent possible, intelligence sharing between staffs."[157] The

148 Mark Scott, "In Europe's Election Season, Tech Vies to Fight Fake News," *New York Times,* May 1, 2017, https://www.nytimes.com/2017/05/01/business/europe-election-fake-news.html?s&_r=0.

149 Mike Isaac, "How Facebook's Fact-Checking Partnership Will Work," *New York Times*, December 15, 2016, https://www.nytimes.com/2016/12/15/technology/facebook-fact-checking-fake-news.html.

150 Cara McGoogan, "Facebook Combatting Fake News in Germany ahead of Elections," *Telegraph*, January 16, 2017, http://www.telegraph.co.uk/technology/2017/01/16/facebook-combating-fake-news-germany-ahead-election/.

151 Ibid.

152 Amanda Hess, "How to Escape Your Political Bubble for a Clearer View."

153 Ben Smith, "Helping You See Outside Your Bubble," BuzzFeed, February 17, 2017, https://www.buzzfeed.com/bensmith/helping-you-see-outside-your-bubble?utm_term=.bpvjeLL1J#.noyBoJJ8R.

154 Amanda Hess, "How to Escape Your Political Bubble for a Clearer View."

155 Ibid.; See also Laura Wagner, "Today in Conservative Media: Other Media," Slate, January 13, 2017, http://www.slate.com/blogs/the_slatest/2017/01/13/mainstream_media_was_the_big_story_in_conservative_media_today.html.

156 Reid Standish, "Why Is Finland Able to Fend Off Putin's Information War?" *Foreign Policy*, March 1, 2017, http://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

157 "Joint declaration by the President of the European Council,

Structured coordination among NATO, European Union, and nations will enhance resilience to hybrid attacks. Left: NATO's new headquarters in Brussels. *Photo credit*: NATO. Right: The European External Action Service Headquarters (EEAS) in Brussels, Belgium. *Photo credit*: European External Action Service/Flickr.

declaration also called for increased cooperation on strategic communication and response and the "development of coordinated procedures" through respective playbooks to facilitate implementation.[158] More recently, in December 2016, NATO and the EU proposed to "enhance staff-to-staff sharing of time critical information," "[e]ncourage cooperation between the NATO Strategic Communications Centre of Excellence and the EEAS Stratcom division," and "[e]ncourage participation by the EU and NATO, as well as EU Members States and NATO Allies, in the work of the 'European Center for Countering Hybrid Threats'."[159]

These actions are useful steps, but they do not constitute a fully comprehensive strategic approach for the transatlantic community. They lack a structure that can devise and support an effective plan, and they do not provide an interface between the public and private sectors. If a historical analogy is useful, it is the difference between NATO's effectiveness before the integrated military organization was established and its effectiveness and military capabilities afterward. In the same way, NATO and the EU need a structure that can develop and support a comprehensive coordinated strategy to meet the wide-ranging threat presented by Russia's hybrid actions. Moreover, as much of the effort in responding to hybrid challenges occurs at the national level, the structure should include the individual nations of NATO and the EU. Additionally, the structure should have an appropriate set of arrangements for engaging with the private sector, which owns and operates critical infrastructure that will be necessary to effectively respond to hybrid challenges. Establishing the Coordinating Council

the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization," NATO.

158 Ibid.

159 "Statement on the implementation of the Joint Declaration," NATO. See also "NATO-EU Relations," NATO, 2017, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170213_1702-factsheet-nato-eu-en.pdf.

would provide the necessary structure requisite to coordinating such a comprehensive approach, just as establishing the integrated military structure did in response to the threat from the Soviet Union.

The Euro-Atlantic Coordinating Council would be explicitly designed to overcome the difficulties the EU and NATO have had in working together. Despite the overlap in membership—currently twenty-two of the twenty-eight NATO nations are members of the EU—multiple factors, including bureaucratic resistance, the consequences of the Turkey-Cyprus dispute, the concept that NATO is only a military organization, and a desire by many Europeans not to have the EU somehow dominated by the United States—have all contributed to the difficulty. It is true that NATO and the EU have undertaken useful steps to work together, as noted above, but these measures are far from a comprehensive response to Russia's hybrid challenges. Moreover, they do not directly include national structures, which are critical to confronting the hybrid threat. Further, while the EU has itself released a "joint framework" on countering hybrid threats, the framework does not include key countries including the United States, Canada, Iceland, Norway, and Turkey, and soon the United Kingdom; is largely a set of proposals to "support," "explore," and "monitor; and lacks a structure to include key private sector entities."[160]

The Coordinating Council could be structured as a voluntary organization along the lines of the Financial Stability Board, which itself is such a voluntary organization and consists of the "Plenary, Steering Committee, Standing Committees, Working Groups, Regional Consultative Groups, Chair, and the Secretariat."[161] While there would be no virtue in seeking to copy precisely the Stability Board structure, the model provides a useful outline. In addition to a Plenary Group, where the Coordinating Council organization would meet as a whole, working groups could focus on each aspect of the Russian hybrid challenge: low-level conflict, cyberattacks, economic and political coercion and subversion, and information warfare. A small secretariat drawn from NATO and EU staff could be established to maintain continuity between and among groups and in the interim between plenary sessions. Other structures could await establishment if or until needed.

Because the proposed Coordinating Council would essentially act as a self-selected coalition of the willing, it would be up to nations to decide whether to participate at Council meetings and whether to take recommended actions at the national level. Somewhat similarly, it would be up to the EU, NATO, or nations to determine which of their multiple institutions and/or agencies would participate; there would be no bar to nations and/or the EU or NATO sending multiple representatives. Recognizing that the EU and NATO address hybrid threats in different ways, this would help account for competencies being spread across various institutional bodies, and cases in which institutional staffs need to interact directly with each other rather than with nations.

To be most effective, nations should adopt a version of the "Finland Model" of integrated governmental and private sector interactions to create responsive and resilient structures. The model is set forth in Finland's *Security Strategy for Society*, which states:

> The securing of functions vital to society as a whole is related to intersectoral activities [and] . . . cooperation between the state, municipalities, the business community, and organizations. . . . The measures and resource-finding of . . . ministries, regional and local administrations, the business community, and organizations are connected to the development of strategic tasks. . . . In the development and use of capabilities, the ministries must always take into account the different administrative levels and the role of the business community and organizations.[162]

A key aspect of the Finland Model is the coordination of governmental and private sector actions. This is particularly necessary for critical infrastructures, which are mostly in private hands, but are obvious targets in hybrid conflict. The private sector has the expertise in running such infrastructure, but it does not have the protective capabilities that governments can provide. Moreover, governments are more apt to focus on resilience requirements in responding to hybrid challenges, which the private sector, with an understandable focus on profitability, would not take into account in the same way. Accordingly, both at the national and the Coordinating Council levels, there will be a need to establish structures to include the key private sector entities in the areas on which there is a focus. To start, it would be useful to have each of the working groups suggested above create a proposal

160 See "Joint Framework on Countering Hybrid Threats," Eurlex, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018.

161 See "Organizational Structure and Governance," Financial Stability Board, 2017, http://www.fsb.org/about/organisation-and-governance/.

162 Finnish Ministry of Defense, "Security Strategy for Society," 2011, http://www.yhteiskunnanturvallisuus.fi/en/materials, 6, 16.

for private sector engagement in its particular arena. One key factor here is the necessity of prioritization. An attempt to work with every element of the private sector is a recipe for failure as the effort would be spread too wide. A better approach would be to engage those companies critical to ensuring success in a particular arena.

One of the most valuable aspects of the Coordinating Council would be its ability to coordinate responses among the transatlantic nations and incorporate the essence of the concept of solidarity that underlies both the NATO and EU founding treaties. Currently, many of the responses to Russian actions are undertaken at the national level by a single nation—for example, the US-issued sanctions against Russian individuals and organizations involved in the 2016 hacking of the Democratic National Committee.[163] However, the US is not the only transatlantic nation affected by Russian interference in electoral processes. As noted above, officials in France, Germany, and the Netherlands have also been affected by or expressed concern over improper Russian influence over their elections.[164] The US responses to the DNC intrusions would have had a much greater effect if they had been adopted across the transatlantic community by nations facing shared threats. In the future, NATO and EU nations should work together to extend and implement unified responses, and the Coordinating Council could provide the platform to do so. Overall, this would result in a much more powerful deterrent for improper Russian actions.

International law has established that countermeasures are permitted to respond to unlawful actions by offending nations, even when no armed attack, as defined by the UN Charter or the North Atlantic Treaty, has occurred. Rather, countermeasures are nonviolent acts (not involving the use of force) that can be used in response to the commission of an earlier illegal act.[165] Many of the Russian actions described earlier, such as low-level use of force, cyber intrusions, and threats to electoral democracy, meet the threshold for authorizing countermeasures. The recommendations proposed herein include some specifics that should be implemented at the national level, but a multinational approach would make them even more effective. As one analysis has recommended:

> [A]n expanded 'fusion' effort [could] bring to bear intelligence, cyber, financial, law enforcement and other capabilities to disrupt the actions of state and state-associated entities undertaking adversarial cyber-action against the availability and integrity of democratic institutions and key critical infrastructures, such as the electric grid and telecommunications, of the US, allies, and other partners. The model would build off the fusion teams utilized in counter-terror activities, and leverage previous law enforcement-led activities that have resulted in the disruption of criminal cyber-networks and enablers like botnets. Importantly, these efforts would focus on developing and implementing sustained campaigns for countering adversarial cyber action, and include the participation of allies and other partners.[166]

Depending on the scale of the hybrid action in question, it may also be appropriate for NATO and EU nations to take internationally authorized countermeasures, including actions affecting diplomatic privileges or financial assets and, as noted, the use of multilateral sanctions.[167] NATO and EU governments should use these tools where appropriate to begin establishing clear consequences and strong deterrents for hybrid conflict. The Coordinating Council could develop appropriate responses to be implemented that would build on the solidarity among the transatlantic nations and generate multinational efforts for the greatest deterrent effect.

CONCLUSION

Russia's hybrid challenge raises major concerns for transatlantic nations. A comprehensive coordinated strategy is needed that will engage both the nations of NATO and the European Union, as well as the institutions themselves. The structural and functional recommendations outlined here could form the building blocks of such a strategy and provide the framework for deterring Russian hybrid action in the future.

163 "Issuance of Amended Executive Order 13694; Cyber-Related Sanctions Designations," US Department of the Treasury, December 29, 2016, https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20161229.aspx.

164 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?_r=0.

165 See United Nations, *Legislative Series: Book 25, Chapter 2: Countermeasures,* http://legal.un.org/legislativeseries/documents/Book25/Book25_part3_ch2.pdf.

166 Franklin D. Kramer, Robert J. Butler, and Catherine Lotrionte, "How to Stop Russia's Hacking," *US News and World Report*, August 12, 2016, https://www.usnews.com/opinion/articles/2016-08-12/how-the-us-can-fight-back-against-russias-cyberattacks.

167 Sanctions, under international law, are technically not countermeasures but rather what are referred to as retorsions—although the practical impact is the same.

ABOUT THE AUTHORS

Franklin D. Kramer is a distinguished fellow and board member at the Atlantic Council and a former assistant secretary of defense.

Lauren M. Speranza is assistant director of the Transatlantic Security Initiative at the Atlantic Council's Brent Scowcroft Center on International Security.

Atlantic Council Board of Directors

CHAIRMAN
*Jon M. Huntsman, Jr.

CHAIRMAN EMERITUS, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*George Lund
*Virginia A. Mulberger
*W. DeVier Pierson
*John J. Studzinski

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
*Peter Ackerman
Timothy D. Adams
Bertrand-Marc Allen
John R. Allen
*Michael Andersson
Michael S. Ansari
Richard L. Armitage
David D. Aufhauser
Elizabeth F. Bagley
*Rafic A. Bizri
Dennis C. Blair
*Thomas L. Blair
Philip M. Breedlove
Reuben E. Brigety II
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Sandra Charles
Melanie Chen
George Chopivsky
Wesley K. Clark
David W. Craig
*Ralph D. Crosby, Jr.
Nelson W. Cunningham
Ivo H. Daalder
Ankit N. Desai
*Paula J. Dobriansky
Christopher J. Dodd
Conrado Dornier
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
Julie Finley
Lawrence P. Fisher, II
*Alan H. Fleischmann
*Ronald M. Freeman
Laurie S. Fulton
Courtney Geduldig
*Robert S. Gelbard
Thomas H. Glocer
Sherri W. Goodman
Mikael Hagström
Ian Hague
Amir A. Handjani
John D. Harris, II
Frank Haun
Michael V. Hayden
Annette Heuser
Ed Holland
*Karl V. Hopkins
Robert D. Hormats
Miroslav Hornak
*Mary L. Howell
Wolfgang F. Ischinger
Reuben Jeffery, III
Joia M. Johnson
*James L. Jones, Jr.
Lawrence S. Kanarek
Stephen R. Kappes
*Maria Pica Karp
*Zalmay M. Khalilzad
Robert M. Kimmitt
Henry A. Kissinger
Franklin D. Kramer
Richard L. Lawson
*Jan M. Lodal
*Jane Holl Lute
William J. Lynn
Izzat Majeed
Wendy W. Makins
Zaza Mamulaishvili
Mian M. Mansha
Gerardo Mato
William E. Mayer
T. Allan McArtor
John M. McHugh
Eric D.K. Melby
Franklin C. Miller
James N. Miller
Judith A. Miller
*Alexander V. Mirtchev
Susan Molinari
Michael J. Morell
Richard Morningstar
Georgette Mosbacher
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Sean C. O'Keefe
Ahmet M. Oren
Sally A. Painter
*Ana I. Palacio
Carlos Pascual
Alan Pellegrini
David H. Petraeus
Thomas R. Pickering
Daniel B. Poneman
Daniel M. Price
Arnold L. Punaro
Robert Rangel
Thomas J. Ridge
Charles O. Rossotti
Robert O. Rowland
Harry Sachinis
Brent Scowcroft
Rajiv Shah
Stephen Shapiro
Kris Singh
James G. Stavridis
Richard J.A. Steele
Paula Stern
Robert J. Stevens
Robert L. Stout, Jr.
John S. Tanner
*Ellen O. Tauscher
Nathan D. Tibbits
Frances M. Townsend
Clyde C. Tuggle
Paul Twomey
Melanne Verveer
Enzo Viscusi
Charles F. Wald
Michael F. Walsh
Maciej Witucki
Neal S. Wolin
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
George P. Shultz
John W. Warner
William H. Webster

*Executive Committee Members
List as of May 16, 2017

Atlantic Council

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

Atlantic Council

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

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