February 2020

Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

ANDREW RADIN, ALYSSA DEMUS, KRYSTYNA MARCINEK

Understanding Russian Subversion

Patterns, Threats, and Responses

Russia is suspected of having undertaken a wide range of subversive activities against the United States and its partners and allies since 2014—examples include military support for the separatist republics in eastern Ukraine, an attempted coup in Montenegro, and influence campaigns in the 2016 U.S. and 2017 French elections. Responding to Russian subversion is difficult, in part because the threat is, by its very nature, not clearly known. In this Perspective, we review past RAND Corporation and other relevant work and synthesize overall insights about why and how Russia undertakes subversion. This review and synthesis offer insights about the likely threat of Russian subversion to the United States and its partners and allies.

Russia likely finds subversion—which we define as efforts intended to influence the domestic politics of other countries—attractive because it could help achieve multiple Russian foreign policy interests at relatively low cost. The threat of Russian subversion to different countries varies based on the intensity of Russia's interests and the resources available to undertake subversion. In western Europe and the

RAND CORPORATION

United States, Russian subversive tools appear to be limited to information, cyber, and political ones. In neighboring former communist countries, Russia uses a wider range of military and economic tools. To better deter Russian subversion, we suggest concentrating defensive efforts on the most vulnerable regions and institutions and ensuring that punishments in response to subversion are clearly linked to specific Russian actions. We also propose focusing on addressing covert or denied Russian activities, both because they are particularly harmful and because targeting overt Russian activities could delegitimize Western outreach to populations that are on the fence about their support for Western institutions.

The first section of this Perspective defines subversion and explains why we focus on this category. In the second, we build from existing RAND work to characterize Russia's interests in undertaking subversion. The third section traces how contemporary Russian subversive activities find their origins in the Soviet period and Russia's recent history. The fourth section characterizes the elements of state power that Russia can use for subversion, including political, military, informational, and economic. The fifth provides a framework for deterring Russian subversion through denial and punishment. The sixth concludes and offers policy implications.

What Is Subversion?

By *subversion*, we mean activities intended to influence a target country's domestic politics. We believe this term offers a useful and concrete way to understand the threat of Russian activities. Other works use such terms as *hybrid warfare*, *active measures*, *hostile measures*, the *gray zone*, *political warfare*, or *sharp power* (Cardenal et al., 2017; Cohen and Radin, 2019; Robinson et al., 2018). There is substantial debate about these terms—for example, critics have argued that *hybrid warfare* does not accurately characterize Russian thinking on this issue.[1] Nevertheless, all these terms refer to the same basic problem: A wide range of somewhat coordinated Russian activities seeks to influence and undermine countries' politics and institutions in undesirable ways, including Russian support of separatism in Ukraine; computer network operations; backing pro-Russian nongovernmental organizations; and publicly acknowledged information campaigns executed by RT, Sputnik, or other attributed media. Russian subversion often exploits political or social divides within Western societies. Russian subversion activities may also leverage concepts and tools that were established to protect democratic societies (e.g., freedom of speech and freedom of assembly) to undermine these institutions.

To be sure, there are differences in the intensity, threat, and legitimacy of particular Russian subversive activities. In general, overt and attributed activities, such as diplomacy or public messages, may be seen as relatively more legitimate, especially since there are parallel efforts by Western countries and institutions. Russia also engages in covert activities, in which Russia seeks to hide its role, and denied activities, in which Russia takes less effort to hide its role but does not publicly acknowledge its actions, as in the case of Russia's support for separatism in eastern Ukraine. We see denied and covert subversive activities as especially threatening. For example, people may be more receptive to a tweet from someone who seems to be a normal citizen rather than from RT or the official account of the Russian foreign ministry. The Kremlin's financial and human resources give it a unique ability to mimic and influence legitimate social groups in ways that are often not discovered until long after they are perpetrated, if they are recognized at all. Clear attribution of denied or covert activities to Russia can limit the effectiveness of these actions.

Why Russia Might Undertake Subversion

Subversion is one possible activity that Russia, like any other country, may use to pursue its foreign policy interests. Subversion appears to be disruptive but is relatively low cost. It allows states to achieve foreign policy goals when diplomacy and overt soft power are insufficient and when large-scale violence may be unlikely to succeed or is otherwise undesirable. A discussion of Russia's foreign policy interests is a useful starting point for understanding Russian subversion because these interests guide Russia's decisions about when or when not to choose subversion instead of other foreign policy options.

In their study on Russian hostile measures of influence, Cohen and Radin identified core, interrelated Russian foreign policy objectives (Cohen and Radin, 2019). First and foremost, Russia seeks to defend its territory and regime. Russia seeks recognition as a great power, which involves maintaining influence in its immediate region. Stopping European Union (EU) and North Atlantic Treaty Organization (NATO) enlargement is perceived as essential to Russian security, preservation of its sphere of influence, and status as a great power. Like any other country, Russia also seeks to ensure its economic prosperity. The latter goals also contribute to the first and primary goal, the preservation of the country and regime. Each of these interests may lead Russia to adopt subversion as a desirable foreign policy tool.

Defense of the Country and the Regime

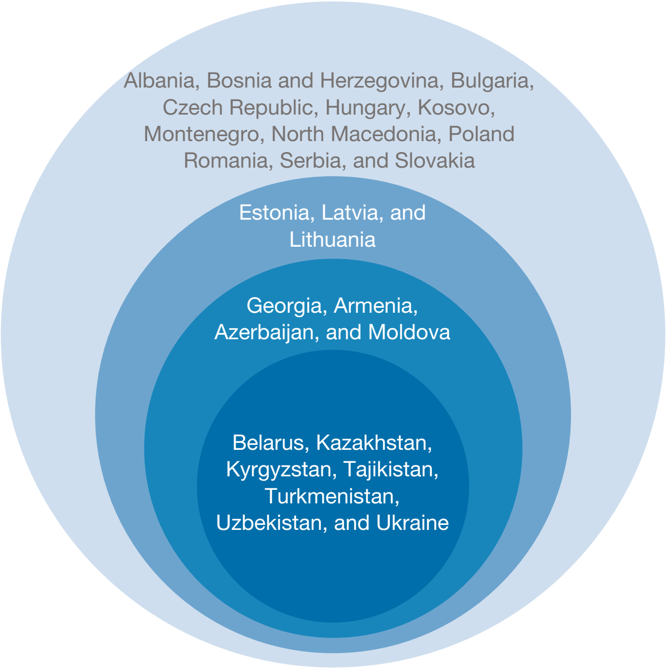
Russian officials and analysts, dating back to the Soviet Union, have often seen a connection between external military threats and internal opponents of the ruling regime. In the post–Cold War era, Russian analysts have observed that the United States has engaged in democracy promotion through its support for "color revolutions" in former Soviet states and for the Arab Spring. These analysts have drawn a connection between these efforts and possible U.S. intentions to engage in a color revolution, or regime change, in Russia, especially following the 2011–2012 prodemocracy protests in Russia and the events in 2014 in Ukraine (Kennan ["X"], 1947; Korsunskaya, 2014; Radin and Reach, 2017, pp. 8–21; Radin et al., 2019).

For the Kremlin, subversion may play a triple role in responding to what it perceives as Western efforts at regime change. First, subversion of Moscow's adversaries may distract or deter them from interfering in the domestic politics of Russia or of those in its sphere of influence. Second, foreign subversion may have an intended or unintended positive influence on popular support for the Russian regime, especially if subversion achieves popular Russian foreign policy goals. Note, for example, the increase in Putin's popularity during the Ukrainian crisis in 2014, although Russia's activities in Ukraine may have been simultaneously limited by perceived brotherhood between Russians and Ukrainians (Greene and Robertson, 2015; Oliker et al., 2009, pp. xiv–xvii, 43–44). Third, subversion may weaken Western institutions that are perceived as a threat to the regime. In the case of the 2016 U.S. election, for example, a U.S. Intelligence Community assessment concluded that "the Kremlin sought to advance its longstanding desire to undermine the U.S.-led liberal democratic order, the promotion of which Putin and other senior Russian leaders view as a threat to Russia and Putin's regime" (Office of the Director of National Intelligence, 2017, p. 1). This assessment reflects what has become a common trope in the U.S. foreign policy discourse: that Russian activities, both subversive and otherwise, threaten the "international order" (Mattis, 2018; see also Radin and Reach, 2017; RAND Corporation, undated).

Recognition as a Great Power with a Global Presence and a Seat at the Table in Resolving Major Disputes

Recognition as a great power includes Russia's role as a member of the United Nations, its participation in peace negotiations, and its desire for greater recognition from other countries (Radin and Reach, 2017, pp. 15–17). Subversion may help to pursue that goal in several ways that are related to the assessment that Russia seeks to undermine the U.S.-led liberal democratic order. Subversive tools may be a low-cost means of demonstrating Russia's ability to cause harm. From this perspective, Moscow may use subversion to demonstrate that Russia cannot be ignored. Second, Russia's meddling in both eastern Europe and in the United States or western Europe may seek to demonstrate the weakness of the West and, consequently, to undermine the hopes U.S. partners and allies place in the United States. If the West becomes a less appealing partner, some countries may begin to perceive Russia as a more attractive alternative to the West. This approach could backfire; the targets of Russian subversion often become less supportive of Russia.

Russia's Desired Sphere of Influence


Albania, Bosnia and Herzegovina, Bulgaria, Czech Republic, Hungary, Kosovo, Montenegro, North Macedonia, Poland Romania, Serbia, and Slovakia
Estonia, Latvia, and Lithuania
Georgia, Armenia, Azerbaijan, and Moldova
Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, and Ukraine

SOURCE: Adapted from Radin and Reach, 2017, p. 11

Maintaining Russia's Sphere of Influence, Stopping EU and NATO Enlargement, and Assuring Russia's Economic Prosperity

Russia's desire to maintain a sphere of influence is based on its understanding of itself as a great power, uninterrupted from its time as an empire. Maintaining a sphere of influence may also be a means of guaranteeing both a security buffer zone and a base for economic prosperity. The circles in the figure on p. 4, replicated from Radin and Reach's 2017 work on Russian views of the international order, illustrate one approach to understanding Russia's vision of desired influence, based on accounts of Russian identity and identification with particular countries.

The rings in the figure highlight how Russia has the greatest desire for control within Belarus, Ukraine, and Central Asia (darkest blue circle); somewhat diminished interest in the Caucasus and Moldova; followed by the Baltics, which many Russian analysts exclude from the concept of the *near abroad*, another term for Russia's desired region of influence; with the outer sphere including the former Warsaw Pact countries and Western Balkans (lightest blue circle). Russia's use of subversive activities within the countries in these rings can help ensure that regimes in these countries adopt friendly policies toward Russia, including guaranteeing that the countries consult Russia when making important decisions; are responsive to Russian desires; or, in the case of the inner rings, participate in Russian-led organizations and do not join Western institutions (Radin and Reach, 2017, pp. 9–14).

Subversion efforts targeting countries outside these rings, such as the United States or western Europe, may also stop EU and NATO enlargement, especially if the efforts can create divisions among the Western allies about the need for enlargement. However, while Russia opposes EU and NATO enlargement, it does not necessarily seek to eliminate or dismantle the EU or NATO. Russia may also hope to weaken the EU and NATO to be able to negotiate bilaterally with European countries, rather than with the EU and NATO. But the destruction of the EU and NATO could also destabilize Europe, introducing unpredictable and significant risks to the Russian economy and its security.[2]

Rather than using subversion to tear down Western institutions, it seems plausible that Russia may use subversion to shape domestic political outcomes in other countries in less extreme ways.

Rather than using subversion to tear down Western institutions, it seems plausible that Russia may use subversion to shape domestic political outcomes in other countries in less extreme ways. Russia may seek to engineer the election of leaders that are supportive of Russia's political or economic interests even if they are not explicitly pro-Russian in their orientation. This may include support for antiestablishment parties or candidates, such as the Alternative für Deutschland [Alternative for Germany] (AfD) party in Germany or Marine Le Pen in France.

Le Pen, for example, agreed with Russia's line of argument on Ukraine and Crimea and opposed the sanctions regime (Pasha-Robinson, 2017).

That said, it may be difficult, or impossible, to identify the particular motivations behind a campaign and link them to the pursuit of specific interests. Indeed, it is possible that there may be multiple or disputed intentions among the Russian actors to pursue them. Cohen and Radin, for example, argue that Russian hostile measures may follow a "soft strategy," according to which Russia does not necessarily have a linear, step-by-step path in mind between subversive actions and desired outcomes (Cohen and Radin, 2019, pp. 13–14). Instead, Russia may undertake actions with the hope that they may eventually bring about its goals. This soft strategy does not necessarily make Russian subversion more or less effective, but may make it more difficult to identify or evaluate.

Origins of Contemporary Russian Subversion

Contemporary Russian subversion is not new—it builds from foreign policy and activities of the Soviet Union and before, as well as Russia's domestic and foreign policy since 1990. Over time, the regional scope and ambition of Soviet and Russian subversion has varied, but where it is most ambitious, it has focused on pursuing control in eastern Europe, exerting a degree of influence in other parts of the world, and shaping Western policy to reduce the threat at home.

The Soviet regime, like the Tsarist one before it, used subversion internally and externally for many purposes but with mixed success. In particular, the Soviets used subversion as an instrument to maintain support for Soviet policy in the broader Communist world and to enforce compliance with Soviet policies when states in the Eastern bloc deviated from sanctioned policy.[3] Following the Soviet and Yugoslav split in 1948, the Kremlin employed several forms of subversive activities to counter Yugoslav dictator Josip Tito's efforts to exercise independence and undermine his position. These included Soviet infiltration of Yugoslav security services and military institutions, as well as Soviet and satellite-state production and dissemination of anti-Tito propaganda (Central Intelligence Agency [CIA], 1949; National Security Agency, 1998; U.S. Department of State, 1951). In Hungary and Czechoslovakia, subversion accompanied Soviet efforts to address instability early in each country's revolution, in 1956 and 1968, respectively (CIA, 1968a, pp. 2–3; CIA, 1968b). Yet, in all three cases, these efforts failed to achieve the Kremlin's aims. In Hungary and Czechoslovakia, Soviet attempts to quell political unrest via subversion also failed, and the Kremlin was forced to use conventional means to regain control in both states. Likewise, Moscow was ultimately unable to unseat Tito through subversive means.

In the developing world, the Soviets used subversion to promulgate Communist ideology and influence, shape states' political events, and curb Western influence.[4] Prior to the 1970s, Soviet subversive activities in Africa involved "training cadres, infiltrating the trade union movement . . . encouraging the growth of radial nationalist parties and factions," and attempting to establish "Communist adherents in positions of influence" (Director of Central Intelligence, 1962, p. 1). The Soviets provided military aid and advisors but relied on Cuban forces to intervene in internal African conflicts in the 1970s and 1980s because this approach provided Moscow with plausible deniability (Director of Central Intelligence, 1979, p. 20). However, the Soviets could not necessarily achieve their most ambitious objectives through subversion (Central Intelligence Agency, 1982). For example, even though much of the African intelligentsia supported communist ideology, they did not necessarily align with Soviet ideology or policy (Director of Central Intelligence, 1962).

Soviet subversion efforts targeting the United States appeared intended to tarnish perceptions of the West domestically and globally, drive a wedge between the United States and its allies, frustrate U.S. interests, and "influence American public opinion in favor of . . . Soviet foreign policy priorities and to exert pressure on U.S. government officials to effect changes that are favorable to Moscow" (U.S. Congress, 1980; see also Federal Bureau of Investigation, 1987, p. 34644). In the early 1980s, the Soviets capitalized on percolating U.S. public discontent over revelations that the U.S. government had conducted biological warfare research at a facility in Maryland and on fears surrounding the newly discovered acquired immunodeficiency syndrome (AIDS) virus. The Komitet Gosudarstvennoy Bezopasnosti [Soviet Secret Service] (KGB) attempted to link the two by spreading a rumor that the virus was the product of "Pentagon experiments to develop new and dangerous biological weapons" (Boghardt, 2009, pp. 3–4). The Soviets also used front organizations, such as the Communist Party of the United States of America, to conduct active campaigns intended to undermine support for U.S. efforts, such as the Strategic Defense Initiative (Federal Bureau of Investigation, 1987, p. 34644). However, Russia's efforts to foster support for communist ideology among U.S. audiences did not appear to take root. Disinformation efforts, such as the AIDS rumor, may have been more successful. A survey in 1992 found that 15 percent of Americans probably or definitely considered the statement that "the AIDS virus was created deliberately in a government laboratory" to be true (Boghardt, 2009, p. 19). That said, without evidence of whether survey respondents were exposed to or influenced by the Soviet rumor, it is difficult to link these outcomes to Soviet efforts.

After the fall of the Soviet Union, Russia continued to use subversion, but its geographic and political ambition refocused on domestic politics and the former Soviet Union. Andrew Wilson, for example, traces the use of subversion in the post-Soviet world to "the black arts of political manipulation and double-speak inherited from the Bolshevik era" (Wilson, 2005, p. xv). To name a few examples, he describes the occurrence of electoral fraud, use of state funds for partisan political purposes, the politicization of the judiciary, media manipulation, the creation of fake organizations to mimic opposing political parties, and dissemination of compromising materials on opponents (*kompromat*). Wilson notes how these techniques became a Russian export in the late 1990s and early 2000s, quoting a Ukrainian commentator that Russian manipulators were not "just making money, but serving as Russian agents of influence, 'distributors' of Russian interests" (Wilson, 2005, p. xiii).

Over the course of the 2010s, especially in response to the 2011 domestic Russian protests, Russian subversion seems to have become more technologically advanced and internet-oriented. Initially, the Kremlin used Russian troll farms for domestic purposes, such as maligning political opposition and activists in the eyes of domestic audiences. With the Ukraine crisis in 2014, and the 2016 U.S.

elections, Russia seems to have broadened the ambition of its subversive activities to the wider world (Chen, 2015; Helmus et al., 2018, p. 15).

Western analysts have, in part, attributed Russia's increased use of nonmilitary tactics, some covert and denied, to ideas expressed in a 2013 article authored by Russian Chief of the General Staff, General Valery Gerasimov.[5] The article indicates that Russia's increased adoption of subversion and other nonmilitary tactics seems to have been based in large part on the observation of parallel, threatening Western activities.[6] Gerasimov, for example, drew on the events of the Arab Spring: "The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness" (Gerasimov, 2013; Galeotti, 2014). His writing implicitly advocates for the development of Russian forces that can respond in kind to these increasing nonmilitary threats (Galeotti, 2014).

Since its publication, Gerasimov's article has been interpreted as evidence of the existence of a "Gerasimov doctrine" guiding Russian use of subversion. However, in practice, Russia's approach appears to be far less disciplined or organized. In fact, Mark Galeotti, a leading analyst of Russia's intelligence activities who popularized the term *Gerasimov doctrine*, apologized for developing the term in a 2018 article. Galeotti clarifies that the Gerasimov doctrine "doesn't exist" as a concrete approach and explains that, instead, Russia's "campaign is dangerous precisely because it has no single organizing principle, let alone controlling agency" (Galeotti, 2018). Instead, he argues that Russia's activities are "largely opportunistic, fragmented, even sometimes contradictory" (Galeotti, 2018). The degree to which there is a singular strategic intent or effective coordination of Russian subversion hence remains somewhat unclear. Instead, we will focus on what Russia *can* do by considering the different elements of state power at Russia's disposal.

Subversion by Different Russian Entities

The table on p. 9 categorizes the organizations that undertake Russian subversion. The rows list the main elements of Russian state power, ordered according to which elements are most powerful within Russia's immediate neighborhood (military), working downward toward capabilities that play a larger role around the world.[7] The columns of the table point to the different categories of actors involved in Russian subversion, from organizations that are part of the Russian government; to organization that are not part of the state but act on Russia's behalf, with different degrees of attribution; to independent groups that share an interest with Russia and may work, knowingly or not, in collaboration on a particular issue.

In many cases, covert or denied subversive activities and overt ones are used in tandem. In Syria, where Moscow has not denied its military presence, overt Russian activities represent the main lines of effort, although some of Russia's activities have aspects of deniability, such as the use of private contractors (Ayres, 2019).

Military

Since 2014, Russia has repeatedly used its military for subversion. In Crimea, Russia used airborne and special

How Do Russian Organizations Engage in Subversion?

	State	Attributed and Unattributed Proxies	Foreign Partners of Russia	Major Challenges to Target
Military	GRU-Spetsnaz; VDV	Private military companies (Wagner Group)	Separatists	• Relatively highly capable light forces • Difficult to distinguish from armed civilians at the beginning; a law enforcement response might be insufficient, while a military response bears political costs and may contribute to Russian propaganda
Political	Possibly executed by intelligence agencies (GRU, FSB, SVR)	State-linked patriotic groups (e.g., Night Wolves biker gang)	Ataka in Bulgaria, Front National in France, AfD in Germany	• Political influence in target countries • Attribution to Russian government • Grounded in preexisting political divisions
Economic	State-owned enterprises (e.g., Gazprom, Rosneft)	Private, state-linked companies (e.g., Lukoil)	Trade partners with Russia	• Extensive European trade links with Russia • Difficulty distinguishing legitimate activity
Information	RT, Rossiya Segodnya, Sputnik, security services	Internet Research Agency (and other troll farms)	Users who amplify Russian media or unknowingly participate—“useful idiots”	• Deceptive or false content • Difficult to regulate • Attribution • Global reach
Cyber	GRU, FSB, SVR	Co-opted independent hackers: APT28, APT29	Patriotic hacking groups: CyberBerkut	• Highly capable • Attribution • Global reach

SOURCES: Robinson et al., 2018; Helmus et al., 2018; Larrabee et al., 2017; Radin et al., 2019.

NOTES: APT = advanced persistent threat; Ataka = Attack Party (Bulgaria); FSB = Federalnaya sluzhba bezopasnosti [Federal Security Service] (Russia); GRU = Glavnoye razvedyvatelnoye upravleniye [Main Intelligence Directorate] (Russia); GRU-Spetsnaz = Special Forces of the GRU; VDV = Vozdushno-desantnye voyska [Russian Airborne Troops]; SVR = Sluzhba vneshney razvedki [Foreign Intelligence Service]. While we use the term GRU because it is known as such, the organization is now formally “Glávnoe upravlénie Generál’nogo shtába Vooruzhjonnyh Sil Rossíjskoj Federácii” [Main Directorate of the General Staff of the Armed Forces of the Russian Federation] and abbreviated GU.

operations forces, colloquially referred to as “little green men” or “polite people” to seize territory in February 2014, although it admitted its involvement only later (Kofman et al., 2017, pp. 6–31). In eastern Ukraine, Russia initially deployed intelligence operatives to support the development of a separatist movement, and, when the separatists were on the brink of defeat in August 2014, deployed conventional military forces to support them (Radin, 2017, pp. 7–8; Robinson et al., 2018, pp. 72–74). Russia has also relied on nongovernmental Russian proxies, such as the Wagner private military company in Ukraine and Syria (Radin et al., 2019, p. 209; “SBU Releases . . . ,” 2018).

While Russia’s military presence in eastern Ukraine has been well documented, Russia continues to deny this presence, likely because of domestic politics and the perceived brotherhood between Russia and Ukraine

Russian military subversion will be quite difficult in NATO countries and is most likely to occur in the non-Baltic former Soviet republics.

mentioned earlier. Acknowledging its military incursion into Ukraine would also likely undermine some of the main lines of Russian messaging, such as defending noninterference in states' internal affairs and critiquing military operations without United Nations Security Council approval. In March 2014, Russia claimed that ousted Ukrainian president Viktor Yanukovich had asked for Russian help, but that line of reasoning had particularly little credibility after August 2014 under newly elected president Petro Poroshenko (Charbonneau, 2014).

The politically sensitive subversive military operations in Ukraine, and possible future military actions, draw on a range of Russian light infantry forces, including the VDV, GRU-Spetsnaz, and Special Operations Forces Command. The forces appear to have been a significant priority in Russia's larger modernization efforts, which began in 2008 following the military's disappointing performance in Georgia. According to Radin et al., such rapidly deployable forces contribute to two of Russia's main tasks for its military: regional dominance within the former Soviet Union and expeditionary operations (Radin et al., 2019, pp. 45–46, 139–153).

Russia's ability to undertake significant operations in NATO countries, however, is likely to be more challenging, as the case of the Baltic states demonstrates. In response to the possibility of military subversion, the military commanders of the Baltic states have indicated their intent to "shoot" the "little green men" on their territory—to rapidly deploy security forces to defeat any covert or denied Russian military presence (Radin, 2017, p. 25; Schmitt and Myers, 2015; Stuttaford, 2015). Such a Russian force would need to be sufficiently small to prevent clear attribution of Russian armed aggression, which would justify a strong response from NATO allies under Article 5 of the North Atlantic Treaty. Given the performance of even the ill-prepared Ukrainian military against Russian-backed separatists in Ukraine, the more-capable Baltic forces would likely have a good chance against Russian-backed paramilitaries. Russia would be forced to either accept the defeat of its proxies or intervene with conventional forces and risk a full-scale war with NATO.[8] It seems that optimal conditions for an effective military subversion require geographical proximity, weak border control, weak counterintelligence, lack of strong allies, easy access to firearms, sociopolitical divisions, and the element of surprise. This analysis indicates that Russian military subversion will be quite difficult in NATO countries and is most likely to occur in the non-Baltic former Soviet republics.

Political

The Russian government and its proxies have sought to develop links with parties and leaders throughout Europe and beyond. Russia's ability to build connections abroad draws on a wide network of people and organizations, including oligarchs, such as Konstantin Malofeev, who allegedly backed separatists movements in Ukraine; the Night Wolves, a biker gang with close links to Putin; and the Russian Orthodox Church (Robinson et al., 2018, pp. 58–60).

Russia may support two broad groups of political actors: those who have an explicitly pro-Russian agenda and those who do not but who do have interests that align with Russia's. The former group is primarily, but not exclusively, found within the former communist countries. Cohen and Radin, for example, highlighted the opportunity from Russia's historical and cultural ties within Central and Southeast Europe. Such countries as Bulgaria and Serbia—where Slavic languages are widely spoken and where the Orthodox Church is the main religious denomination—also have political parties that explicitly support Russia (Cohen and Radin, 2019, pp. 68–70).

However, historical ties are far from determinative—in the case of Poland, for example, elements of shared history have resulted in predominantly negative views of Russia. Estonia and Latvia, which have substantial minorities of Russian speakers (meaning migrants from the Soviet Union and their descendants), also have political parties that are largely supported by Russian speakers. These parties had not been able to join government coalitions until 2016, when the Centre Party joined the Estonian government, which may have contributed to a sense of marginalization among the Russian-speaking population. Despite their historic links to Russia, these parties do not advocate a pro-Russian agenda and have policies toward the EU and NATO similar to those of parties associated with the ethnic majorities (Cohen and Radin, 2019, pp. 32–33; Helmus et al., 2018, pp. 62–64).

Given the difficulty of building support for explicitly pro-Russian parties, even in countries with deep historic ties, Russia often backs parties that share some common interests but are not explicitly pro-Russian. This approach is especially prevalent outside eastern Europe but may also occur in the former Soviet Union.[9] Russia has backed parties on both the far left and far right—as is alleged in Greece, for example—showing a general preference for nationalist, Euro-skeptic parties that might weaken or, at a minimum, decrease the ambition of the EU and NATO (Cohen and Radin, 2019, pp. 84–87). In western Europe, Russia has also reportedly supported parties that support some Russian foreign policy positions, such as Marine Le Pen's Front National and Germany's AfD (Cohen and Radin, 2019, pp. 114–122).[10] However, the importance of Russian support remains unclear in determining the success of these parties.

Economic

Russia is a major economic power. Russia's economic influence especially comes from its major presence in the energy market—state-owned Gazprom and Rosneft and state-backed Lukoil are major Russian international energy companies. Europe and the United States have emphasized the need to diversify away from Russian supplies, citing in part the threat of Russian leverage. Nevertheless, Russia's role as an energy supplier is, in principle, not subversive as we have defined it. It is neither denied or covert. Indeed, many actors see Russia as a legitimate and reliable supplier, as shown by the efforts of Germany and other countries

Russia generally has more leverage in regions that remain particularly dependent on Russian energy and where Russian infrastructure investments are large compared with the local economy, as in Southeast Europe.

to maintain trade with Russia through the construction of Nord Stream 2 (Pezard et al., 2017, p. 61; Wilkes, 2018).

However, there are instances of Russia using energy supplies or infrastructure subversively. For example, in 2006, when the Lithuanian government decided to sell the Mazeikiai refinery to the Polish company PKN ORLEN, instead of to Russian bidders (Lukoil and TNK-BP; TNK-BP has since been acquired by the Russian energy company Rosneft), Russia cut off pipeline oil supplies to the facility. The Russian pipeline operator attributed the issue to a leakage caused by an accident. But Lithuanian authorities claim that the report of an accident was an attempt to sabotage the deal and maintain control over the Lithuanian oil market (Dempsey, 2006; PKN ORLEN, 2006). In Bulgaria, analysts assert that Russia engaged in corruption to expand its control over the energy market and to deter diversification, including through support of antifracking protests (Cohen and Radin, 2018, pp. 90–91). While there are some allegations that Russian economic investments may be for intelligence-gathering or other political purposes, there are also strong indications that Russia's primary goal is sustaining its economic interests in the region. A commonly cited example of Russia's informal influence on German policy is that Gerhard Schröder, a former German Chancellor, was appointed chairman of the board of the joint German-Russian Nord Stream pipeline and the chairman of the board of Rosneft (Cohen and Radin, 2019, pp. 126–127; Rosneft, 2018).

These examples show how Russia's interests and ability to use its economic presence as a subversive tool vary in different regions. Russia generally has more leverage in regions that remain particularly dependent on Russian energy and where Russian infrastructure investments are large compared with the local economy, as in Southeast Europe. Russia has less leverage in regions in such countries as Germany, in which energy exports from Russia make up a significant portion of Russia's overall portfolio, and there are other alternative suppliers (Larrabee et al., 2017, pp. 33–50).

Information

The Russian government also attempts to use the control of information as a means of influencing audience perceptions and behaviors, adversary decisionmaking, and political outcomes in ways that serve its interests. Russian military doctrine and strategic-level documents emphasize the significance of information control and exposure both as a tool and a threat (Ministry of Foreign Affairs of the Russian Federation, 2000; Ministry of Foreign Affairs of the Russian Federation, 2016; Russian Armed Services, 2014).

Indeed, many Russian writers see the control of information as central to the achievement of political objectives.[11] The closely related concepts of *informational struggle* and *reflexive control* describe ways to persuade one's adversary to make specific choices that are favorable to the initiator's own interests. These concepts suggest altering the target's perceptions of reality or otherwise influencing their decisionmaking process.[12] Linda Robinson and her coauthors have assessed that Russia has invested considerable resources in developing its information-driven subversion tools, particularly in "developing a diverse and sophisticated set of information channels aimed at promoting Russia's goals abroad" (Robinson et al., 2018, p. 69).

Christopher Paul and Miriam Matthews have characterized Russian propaganda as the "firehouse of falsehood," noting the high volume of communication and "shameless willingness to disseminate partial truths or outright fictions" (Paul and Matthews, 2016). In particular, Todd Helmus and his coauthors observed in a 2018 report that Russian information activities significantly intensified after the annexation of Crimea in 2014, including "a dizzying swirl of disinformation about Russia's actions and intentions in Crimea and Ukraine" (Helmus et al., 2018, p. 16). One line of this effort involved the use of a robust network of social media groups to disseminate antigovernment rhetoric in Ukraine, such as calling for a "Third Maidan," likely in an effort to undermine the authorities in Kyiv (Helmus et al., 2018, p. 16).[13] Investigative journalists discovered that the network that claimed to operate in Ukraine was actually based in a suburb of Moscow and was likely associated with the Russian security services (Samokhvalova, 2016).

More recently, Moscow has used information-driven subversion tools against targets in its far abroad, primarily to influence the outcomes of political campaigns in western Europe and the United States. Although now exposed as a likely Kremlin affiliate, the St. Petersburg Internet Research Agency secretly masqueraded as U.S.-based social and political organizations around the 2016 presidential election. As Helmus and coauthors have noted, the messages promulgated in the ads and pages the Internet Research Agency created were an attempt to exploit and deepen existing U.S. social cleavages related to race, political ideology, and class (Helmus et al., 2018, p. 20). The ads' metadata reveal that the organization used existing Facebook advertising algorithms to deliberately target specific audiences within the United States. Russian agents were able to pair messages with the segments of the population they were more likely to resonate with or incite (Helmus et al., 2018, p. 20). Moscow also employs human-operated troll accounts, honeypots (fake accounts meant to attract users' attention), and automated bots as force multipliers to extend the reach and visibility of its messaging (Helmus et al., 2018, p. 23).[14]

Russia employs a range of actors to develop and execute (produce and disseminate) its information-driven subversion efforts. Some, such as the Russian intelligence services (KGB, GRU, SVR), are part of the state. These actors may work in concert with overt state-owned media organizations, such as RT and Sputnik, to support denied or covert activities. Other nonstate organizations, such as troll farms (e.g., the Internet Research Agency), are likely connected to the Kremlin through personal, political, or financial ties, although the state does not acknowledge these ties (*United States of America v. Internet Research Agency LLC*, 2018). In other cases, Moscow fosters relationships with individuals or organizations that are unaware they are interacting with Russian actors. These useful idiots, as they are sometimes called, unwittingly participate in Russian subversion efforts, while others unknowingly amplify Russian messages by retweeting, reposting, or "liking" subversive messages without knowing their true origin.

Measuring the success of information-driven Russian subversion efforts is inherently difficult. In today's information-saturated environment the Kremlin's target audiences are exposed to countless messages from various stimuli. Isolating the effect of any one of these messages outside a controlled environment is nearly impossible without a baseline of attitudes and behaviors and clear specification of Russia's desired objectives. What is more, in the context of political campaigns, Russian-linked messaging may mirror that of a legitimate candidate. This makes it more difficult to disaggregate the effects of the Russian effort from those of the legitimate political campaign.

Attribution is an additional challenge because the online information environment affords users anonymity and accessibility (Bodine-Baron et al., 2018). Overattribution is also a risk—other state or nonstate actors could leverage a Western tendency to attribute information operations to Russia. The accessibility of the online environment allows Russian actors to directly research Western audiences without needing to foster relationships with journalists as the Soviets did. At the same time, audiences can access a wide range of media sources and, therefore, are less dependent on any one media channel, meaning that the Kremlin faces competition for audience attention.

Finally, the global scope of information technologies allows Moscow to reach audiences in its near and far abroad (Helmus et al., 2018, p. 17). However, influence via information requires an intimate and nuanced understanding of the target audience, which may favor Moscow more with audiences in the near abroad than with those farther from Russia geographically and/or culturally.

Cyber Means

Cyberattacks are a specific type of information-related subversion activity that offers a flexible tool for covertly achieving a range of objectives. While in Western military thinking cyber means are often conceived of as a distinct field, Russian doctrine tends to treat this area as one element among many within the broader concept of information warfare (Darczewska, 2014, pp. 11–13). Cyberattacks are commonly used for classic espionage operations but may also be used to contribute to diverse efforts to shape foreign narratives. The 2016 attack on the Democratic National Committee (DNC), for example, gathered information to contribute to a larger information campaign. Another striking case is the false attribution of Russian hacking of the computers and phones of the wives of U.S. military personnel to the Islamic State's "Cyber Caliphate." The apparent intent of this campaign was to divert U.S. attention away from Russia toward the Islamic State (Satter, 2018).

Cyberattacks are commonly used for classic espionage operations but may also be used to contribute to diverse efforts to shape foreign narratives.

The first widely known cyberattack attributed to Russia was a series of distributed denial of service attacks on multiple entities in Estonia in April and May 2007, which, at its height, resulted in brief shutdowns of websites belonging to the parliament and other government entities, political parties, banks, and news and telecommunications companies.[15] The attack itself was not attributed to any specific recognizable group, and the early phase of the attack appeared relatively amateurish. But the timing of the end of the campaign points to some degree of coordination (Connell and Vogler, 2017, p. 13.; Robinson et al., 2018, pp. 91–96).

Since 2015, a large number of attacks attributed to Russian actors have been identified and credited to two groups: APT28 (also known as Fancy Bear, Sofacy Group, and Pawn Storm, among others) and APT29 (Cozy Bear, Dukes). According to the Estonian Foreign Intelligence Service, APT28 is affiliated with the GRU, while APT29 is associated with the FSB and the SVR (Estonian Foreign Intelligence Service, 2018, pp. 53–55). Both were suspected to be engaged in the attack on the DNC in 2016, and each is separately accused of executing multiple attacks against other government institutions both in the United States and Europe (Robinson et al., 2018, pp. 69–71). In late 2015, an attack on the Ukrainian power grid that led to an energy outage affecting approximately 225,000 customers was attributed to a Russian group (Voltz, 2016). The GRU was also believed to be behind the June 2017 "NotPetya" attack, which targeted a widely used Ukrainian tax software site and substantially disrupted Ukraine's financial infrastructure (Nakashima, 2018).

The difficulty of attribution is commonly cited as a key challenge of cyberattacks. Cyber analysts rarely have clear, smoking-gun evidence. Instead, they usually attribute attacks based on a combination of indicators, such as technical findings (e.g., code artifacts), political motives, pattern-of-life analysis, the length and scope of operations, and all-source intelligence (Davis et al., 2017, pp. 9–16; F-Secure, 2017, p. 9). Cybersecurity firms also sometimes disagree about attribution (Davis et al., 2017, pp. 20–21). Still, as the previous examples indicate, there is sometimes a high degree of confidence that particular Russian actors are behind particular attacks, even where there is false flagging, as in the Cyber Caliphate case. There may be greater uncertainty in the linkage between some pro-Russian hacker groups and the government. There appears to be only speculation about whether the pro-Russian hacktivist group CyberBerkut, for example, works in occasional coordination with APT28 or is indeed an arm of APT28 (Bartholomew and Guerrero-Saade, 2016; ThreatConnect, 2016; see also Estonian Foreign Intelligence Service, 2018, p. 52).

Coordination and Command and Control

Russia may achieve the greatest results when it is able to combine multiple tools in one campaign, but Russia's command and control of subversion does appear to have limits (Robinson et al., 2018, pp. 83–85). In Ukraine in 2014, Russia used diplomatic persuasion to try to convince Kyiv not to align with the West, amplifying the message via a large-scale information campaign. Concurrently, intelligence organizations created false social media accounts, armed separatists, and directly engaged in kinetic activities. In the economic sphere, Gazprom doubled gas prices in Ukraine and cut off the supply when Kyiv contested the higher price (Helmus et al., 2018, pp. 15–17; Kofman et al., 2017; Larrabee et al., 2017). In the case of the 2016 election campaign in the United States, the U.S. intelligence community notes that the influence operation was multifaceted, including intelligence organizations; social media trolls; attributed Russian media organizations, such as RT; and non-Russian organizations, such as WikiLeaks (Office of the Director of National Intelligence, 2017, p. 2).

There is some evidence of control from the top, such as through the Russian presidential administration. Vladislav Surkov, a former Deputy Prime Minister and now special advisor to the President of the Russian Federation, appears to be responsible, among his other duties, for overseeing the campaign in Ukraine. According to emails leaked by the Ukrainian hacker group CyberHunta in October 2016, Surkov received a list of candidates for the supposedly independent government of the Donetsk People's Republic three days before the government was announced (Digital Forensics Research Lab, 2016; Kramer, 2016). However, it remains unclear how broad Surkov's authority is and to what degree his activities might be coordinated with the Russian Ministry of Defence or intelligence agencies. According to Mark Galeotti, no institution is singly responsible for command and control of Russian subversion. Galeotti has noted that, while there is some higher-level coordination, such as from the presidential administration, many efforts originate from bottom-up initiatives based on varied interpretations of the government's (and Putin's) broad goals (Galeotti, 2017).

Evidence from other incidents also betrays a lack of hierarchical command and control. In the DNC hack, for example, APT28 and APT29 separately attempted to steal the same credentials, without any apparent cooperation or even knowledge of each other's activities (Robinson et al., 2018, p. 70; Alperovitch, 2016). Smaller operations, involving fewer actors and lines of effort, do not necessarily have better coordination, especially because there may be competition among the participating government institutions (Galeotti, 2016). While decentralization and a lack of a highly defined command-and-control system may make Russian subversion less effective, it also may make subversion more difficult to detect and counter.

A Framework for Deterring Russian Subversion

To consider past and future responses to deter Russian subversion, we divided possible responses into two commonly used categories, deterrence by denial and deterrence by punishment (Snyder, 1960, pp. 163–178). For both categories, we next describe what deterrence activities consist of and provide some possible criteria for evaluating whether these deterrence activities are effective or advisable. These criteria draw from existing analyses of the challenge of Russian subversion, as well as criticism of existing U.S. deterrent activities discussed later.[16] Carefully evaluating proposed deterrence options is essential because the costs and risks of an activity to improve deterrence could exceed the potential benefit of the activity for reducing Russian subversion. While there may be insufficient information to make a full evaluation of these factors, it is advisable to conduct at least a rough assessment.

Deterrence by denial involves actions that make Russian subversion less likely to succeed or more expensive or challenging to undertake. In the case of ongoing Russian subversion activities, deterrence by denial is synonymous with defense (e.g., Synder, 1961; Bodine Baron et al., 2018).[17] In practice, deterrence by denial refers to policies designed to reduce the vulnerability of the United States, its allies, and partners to the full range of Russian subversive activities. Examples include improving cyberdefense, reducing dependence on Russian energy, strengthening border security in countries neighboring Russia, and providing media literacy training to reduce peoples' susceptibility to Russian information campaigns (Helmus et al., 2018, Ch. 6). A key advantage of deterrence by denial is that it is less likely to challenge the Russian interests described above and, therefore, presents a lower risk of provoking undesired Russian responses. However, investing in defensive activities probably cannot eliminate all vulnerabilities to Russian subversion. It may be cheaper and easier for Russia to find new avenues of subversion than for the West to address vulnerabilities.

Programs to improve defense, and thus deterrence by denial, should be evaluated on at least five factors:

- *Risk reduction.* Different proposed programs or policies may be expected to have a varied effect on vulnerabilities to Russian subversion in the short and long terms.
- *Achieving other socially desirable objectives.* For example, initiatives that introduce new media literacy training into education programs may address a broader concern about social media beyond concerns related to Russian subversion. Similarly, reducing European dependence on Russian gas may also increase European consumption of American-produced liquid natural gas.
- *The cost of the proposed program.* Calculating the cost of defensive programs is difficult, especially because costs are not limited to the financing of the specific program, but also include second-order economic effects. For example, border security costs may include both the costs of hiring new personnel or buying new equipment and a second-order cost of reduced trade.
- *The alignment between the proposed program and Western norms and values.* For example, efforts to block all information on social media coming from Russia would likely reduce Russian influence (through that channel). Such a policy, however, would be incompatible with Western democratic values that prioritize the free flow of information.
- *Shaping Russian decisionmaking.* It may be possible to predict whether activities intended to reduce Russian subversion are likely to produce an escalatory Russian response. For example, a large military

deployment may improve defense against Russian special forces operations but, depending on the deployment, may also lead to a security dilemma in which Russia responds to what it perceives as a threat to its own interests. Of course, a high-confidence assessment of Russian reactions may not be feasible, but it may be possible to gauge likely Russian reactions based on past behavior (e.g., Frederick et al., 2017).

Existing analysis of Russian subversion has proposed ways to improve defensive activities (e.g., Fly, Rosenberger, and Salvo, 2018; Fried and Polyakova, 2018). However, with some exceptions, including a 2018 RAND report that specifically evaluates possible responses to Russian social media activities, there are few existing analyses of the effectiveness or wisdom of existing defensive activities based on these (or similar) criteria (Bodine-Baron et al., 2018).

In the context of Russian subversion, *deterrence by punishment* consists of actions, or threats, to impose direct costs to Russia that would outweigh the potential gains achieved by subversion. Examples include the economic sanctions that the United States and others have imposed on Russia in the wake of Russia's annexation of Crimea, the diplomatic sanctions that followed the poisoning of former Russian spy Sergei Skripal in the United Kingdom, and the indictment of Russian operatives ("Spy Poisoning . . . ," 2018; *United States of America v. Internet Research Agency LLC*, 2018; U.S. Department of State, undated). Several factors contribute to the effectiveness and desirability of particular punishments:

- *The speed and certainty of the attribution of Russian subversion*. Is there clear evidence that Russia was responsible, and can this evidence be presented to the public? Absent rapid and clear attribution, formulating, justifying, and communicating punishments may be difficult.
- *The severity of the punishment*. Would the costs the punishment imposes on Russia or its leadership sufficiently outweigh the potential gains from Russian subversion efforts?
- *The clarity in outlining the conditions of the punishment*. Have the United States, its allies, and its partners clearly linked undesired subversive activities with specific punishments? Are these punishments likely to be levied if, and only if, Russia pursues specific undesired subversive activities? Is the punishment likely to be removed if Russia changes its behavior?
- *Russian perceptions of punishments*. Do Russian officials believe that the punishment is actually linked to their behavior? What are likely Russian reactions to the punishment? Is there indication of whether Russian officials believe a punishment to be a sign of a larger intent to cause harm to Russia or undermine its government? On the other hand, could the absence of any punishment encourage greater subversive activities in the future?
- *The costs associated with punishments*. What are the direct costs of the punishment for the United States or other interested parties? How might the punishments, if levied, affect the Russian population, as compared with elites? Is it possible to estimate the potential indirect costs for the United States or European countries?

As in the case of Western defensive activities, neither a definitive list of punishments nor an evaluation of these punishments exists. Our preliminary analysis, however, suggests that existing punishments fall into two categories: They either affect Russia too little to change its decision-making or are not linked closely enough to Russian subversive activities. These problems do not mean that existing punishments of Russia should be abandoned; even imperfect punishments may have a deterrent effect. Instead, these issues underscore the need to develop more effective punishments that are more clearly tied to Russian behavior.

Identifiable punishments falling into the first category are clearly linked to specific Russian activities but do not appear to impose high enough costs relative to Russia's other interests to be effective deterrents. Effective punishment may be especially difficult in cases of Russian subversion in countries that, like Ukraine, fall in the innermost rings of Russia's sphere of influence (see figure). For example, after Russia's seizure of Crimea in early March 2014, the United States introduced sanctions in response to the violation of the "sovereignty and territorial integrity of Ukraine" (Obama, 2014a).[18] After Russia took further action to annex Crimea, the United States expanded its sanctions (Executive Order 13661, 2014). President Barack Obama's statement in March 2014 expressly tied U.S. sanctions to the specific Russian actions:

> We've seen an illegal referendum in Crimea; an illegitimate move by the Russians to annex Crimea; and dangerous risks of escalation . . . . [B]ecause of these choices, the United States is today moving, as we said we would, to impose additional costs on Russia." (Obama, 2014b)

In July and September, the United States and EU also sanctioned Russian individuals and entities by freezing Russian assets in the United States, prohibiting Western travel, blocking access to Western capital, preventing the export of energy technology, and blocking imports to Crimea (ReedSmith, 2014). However, many of the individuals or companies sanctioned are based in Russia or Crimea and either do little business with the United States or depend far more on their status in Russia. While forgoing access to Western capital and technology is damaging to Russian companies, Russian interests in Ukraine likely exceed such concerns. These sanctions are thus likely to have little effect on Russia's decision to continue its policy in Crimea and Ukraine.

Our preliminary analysis, however, suggests that existing punishments fall into two categories: They either affect Russia too little to change its decisionmaking or are not linked closely enough to Russian subversive activities.

Similarly, the 2018 U.S. indictments of individuals associated with the Internet Research Agency and the GRU was clearly tied to their criminal activities during the 2016 U.S. presidential election. The indictments may have made it more difficult for these individuals to travel and may have had some small effect on the perceived legitimacy of working for the GRU. However, it is highly unlikely that those indicted will ever face trial in the United States. The indictments overall had little prospect of seriously affecting the lives of individuals and organizations operating in Russia under the direction of the Kremlin.

A second category of punishments has great consequences for Russia and could motivate a change in policy, but these are less clearly linked to changes in Russian behavior. For instance, the 2017 Countering America's Adversaries Through Sanctions Act (CAATSA) provides broad powers to sanction a variety of Russian entities, many of which are important contributors to the Russian economy.[19] For example, Oleg Deripaska and the companies he controls have been identified as potential targets of U.S. sanctions. His company, Rusal, is a major global producer of aluminum, and sanctions of Rusal could significantly affect Russian aluminum exports (Zhdannikov, Lough, and Wroughton, 2018). However, CAATSA and related laws on U.S. sanctions are highly complex and difficult to interpret, and there is ambiguity in how existing sanctions will be implemented or under what conditions they will be lifted.[20] In particular, CAATSA specifically justifies sanctions against Russia on the basis of its activities in Ukraine and Russian subversion against the United States (e.g., Borak, 2018; U.S. Department of State, undated). The Russian leadership may wonder whether these sanctions would be likely to be lifted if Russia were to reduce its information operations against the United States while not reversing the annexation of Crimea—the latter policy could be very difficult for Russia to change. Ongoing discussions of additional sanctions could further reduce the deterrent effect of sanctions on Russian decisionmaking because Russia may believe that it will be subject to additional sanctions regardless of its behavior (Zengerle, 2018).

Overall, a key ongoing challenge for U.S. policy is to develop sufficiently effective responses to Russian subversion and to ensure that these responses are indeed linked to Russia not taking subversive actions in the future.

Conclusion

Russia has engaged in a wide range of subversive efforts to influence U.S., allied, and partner domestic politics. Contrary to descriptions of a coherent Gerasimov doctrine, Russian subversion lacks a single organizing principle. Instead, Russian foreign policy interests motivate different forms of subversion; Russian subversive capabilities vary greatly across countries and activities; Russian subversion often lacks strong centralized command and control; and the effectiveness of Russian subversive efforts remains largely unknown. Despite these challenges, our earlier observations point to some recommendations for how to better deter and respond to Russian subversion in the future.

Improving Deterrence by Denial

We recommend improving deterrence by denial by focusing U.S. programs to build resilience in the most vulnerable countries and institutions. Efforts to deter by denial must be tailored to account for the varying intensity and types of threats each state faces. To identify where U.S. efforts can be most useful, it is necessary to evaluate existing vulnerabilities, trace past U.S. efforts, and consider where U.S. assistance may be the most effective. For example, in non-NATO former Soviet states, such as Ukraine, Russia is able to wield the broadest range of its subversive capabilities, including the use of military and political proxies. Several reports from RAND and other institutions have already investigated the vulnerabilities of European countries, but more work remains to be done (Cohen and Radin, 2019; Conley et al., 2016; Larrabee et al., 2017; Pezard et al., 2017). While there are limits of the effectiveness of U.S. foreign assistance, U.S. efforts to improve Ukrainian defense institutions, strengthen cybersecurity, and address Russian election meddling are useful investments in this context (U.S. Department of State, 2018). Russia is able to use fewer tools for subversion in former communist countries that have joined NATO, and its means of subversion are even more limited in the West. Still, efforts to improve the rule of law, strengthen alternatives to Russian energy exports, and strengthen cybersecurity may be valuable where there are particular gaps.

Improving Deterrence by Punishment

The United States can also better deter Russia by more clearly linking punishments to specific Russian subversive activities. To be most effective, punishments of Russian subversion should be threatened and enacted in an incremental way, with each additional element clearly associated with an identified Russian subversive action. A transparent logic of why a punishment is being enacted and how Russia can change its behavior to remove a punishment is also desirable. To change Russian behavior, punishments must also be significant or meaningful enough to convince these actors that it is not worthwhile to pursue subversive actions. In some cases, it may be necessary to enact a punishment even if that is unlikely to convince Russia to moderate its behavior. In these circumstances, it may be worth developing new sanctions that can be added or removed depending on more or less cooperative Russian behavior.

Punishments of Russian subversion should also focus especially on covert or denied Russian activities, rather than overt economic activity or information campaigns. Overt activities, such as RT or Russian energy investments, could certainly be harmful to U.S. interests. Punishing these behaviors, however, makes it easier for Russian officials to believe and to convince others that the United States is against everything Russian or that it is pursuing a Cold War–style, zero-sum competition with Russia. Sanctioning overt activities also puts at risk parallel U.S. activities in Russia or its neighbors, such as U.S. social media companies, other business investment, and U.S. foundations (e.g., Eurasia Foundation, 2019; Petroff, 2017). Avoiding punishing overt Russian economic activities makes it easier to imagine a transition to a less adversarial U.S.-Russia relationship.

One potential, but ill-advised, route for responding to Russian subversion is to intensify U.S. efforts to subvert Russia. Encouraging shifts in democratic government in Russia could hypothetically make Russia pursue a less adversarial foreign policy and could lead to dramatic improvements in the well-being of Russia's population. Given Russia's belief that the United States is already engaged in subversion, there may also seem to be little to lose from increasing U.S. effort to achieve regime change. However, intensified U.S. subversion has several potential downsides. It is unlikely to succeed; despite past U.S. efforts, Putin remains popular and in power (e.g., Kimmage, 2018; McFaul, 2018). Intensified U.S. subversion could also result in undesired Russian escalation, up to and including kinetic military action against the United States, its allies, or its partners.

Additional Research About When Russian Subversion Is Effective

There is significant uncertainty about when and to what extent Russian subversion is effective. With some tools at Russia's disposal, like military activities in Ukraine, the effects of Moscow's efforts are more evident. The influence of political, information, and economic tools is less well understood, as the uncertain effectiveness of Russian interference in the 2016 U.S. election clearly shows. Whatever its effectiveness, Russian subversion is clearly undesirable. But without understanding the actual effects of subversion, it is difficult to fully articulate a proportionate response or to understand how this response should be prioritized among other U.S. efforts. Any response to Russian subversion will have costs, such as establishing new government bodies, increasing regulation for social media, or building new infrastructure. Evaluating the effectiveness of Russian subversion is essential to determine whether to accept such costs. Such an evaluation may be difficult but is possible through further study, including increasing understanding of Russian objectives; evaluating how Russian activities affect countries' security; and applying alternative methods, such as social media analysis and survey research.

> Without understanding the actual effects of subversion, it is difficult to fully articulate a proportionate response or to understand how this response should be prioritized among other U.S. efforts.

Improving Attribution

Rapid attribution is critically important—it makes covert activities overt and makes it harder for Russia to deny its actions. Attribution thereby limits the effectiveness of Russian subversion. For example, if the campaign led by the Internet Research Agency had been rapidly attributed to the Russian government, the credibility and effectiveness of the campaign messaging would likely have been diminished. The Internet Research Agency's involvement ultimately became publicly known, but that organization had a great deal of time to shape public attitudes before being unmasked. A delay in attribution can therefore be almost as harmful as a lack of attribution. Brattberg and

Maurer similarly argue that rapid attribution and response on the part of French authorities in response to alleged Russian interference in the 2017 French election was one potential reason the "Macron leaks" had such limited effects (Brattberg and Maurer, 2018; see also Vilmer, 2018, p. 4). Attribution is also critical for justifying the imposition of punitive measures. One possible way to facilitate faster attribution is to strengthen coordination within and across governments to better combine disparate sources of information. With improved defense and more-targeted punishment, better attribution may be effective at persuading Russia not to undertake subversion in the future.

Abbreviations

AfD	Alternative für Deutschland [Alternative for Germany]
AIDS	acquired immunodeficiency syndrome
APT	advanced persistent threat
CAATSA	Countering America's Adversaries Through Sanctions Act
CIA	Central Intelligence Agency
DNC	Democratic National Committee
EU	European Union
FSB	Federalnaya sluzhba bezopasnosti [Federal Security Service]
GRU	Glavnoye razvedyvatelnoye upravleniye [Main Intelligence Directorate]
GRU-Spetsnaz	Special Forces of the GRU
KGB	Komitet Gosudarstvennoy Bezopasnosti (Soviet Secret Service)
NATO	North Atlantic Treaty Organization
RT	Originally *Russia Today*, now known only by the acronym RT
SVR	Sluzhba vneshney razvedki [Foreign Intelligence Service]
TNK-BP	a former Russian oil company
VDV	Vozdushno-desantnye voyska [Russian Airborne Troops]

Notes

[1] On hybrid warfare, see, for example, Charap, 2015, pp. 51–58; Kofman, 2016.

[2] Interviews with Russian analysts, Moscow, July 2017. See Radin et al., 2019.

[3] We thank Stephanie Young and Brenna Allen for unpublished research related to this report.

[4] We thank Stephanie Young and Brenna Allen for unpublished research related to this report.

[5] For the original text of the article, see Gerasimov, 2013. For an English translation with commentary, see Galeotti, 2014.

[6] Other Russian writers, such as Igor Dylevski, have also published work on particular elements of subversion, such as information confrontation. Similarly to Gerasimov, Dylevski believes that the United States is responsible for the spread of information threats. See Dylevski et al., 2015, pp. 7–16.

[7] This breakdown draws from the framework of the U.S. instruments of national power outlined in Joint Publication 1, 2017, p. I-1, including diplomatic, informational, military, and economic instruments, although it has been adapted for the specific context of Russian subversion; see also Robinson et al., *2*018, pp. 57–83.

[8] For more detailed analysis of this scenario, see Radin, 2017, pp. 25–27.

[9] In Latvia, for example, Cohen and Radin note that Russia has found common cause with conservatives opposing same-sex marriage (Cohen and Radin, 2019, p. 32).

[10] Front National is now known as Rassemblement national [National Rally].

[11] Jānis Bērziņš, 2014, p. 6, for example, wrote that "the Russians have placed the idea of influence at the very center of their operational planning and used all possible levers to achieve this: the skillful internal communications; deception operations; psychological operations and well-constructed external communications."

[12] For a discussion of reflexive control theory in English, see Thomas, 2004, pp. 237–245. For a discussion of informational struggle, see Adamsky, 2015.

[13] The term *maidan* refers to antigovernment protests held in Kyiv's Maidan Square, primarily the 2013–2014 protests in Ukraine in response to then-President Viktor Yanukovych's suspension of Ukraine's association agreement with the EU. Since then, actors affiliated with the Russian government have attempted to incite unrest in Ukraine by propagating messages of another, "Third Maidan," antigovernment movement, with the first *maidan* referencing the 2004–2005 Orange Revolution.

[14] According to Ferrara et al., 2016, a *social bot* is a "computer algorithm that automatically produces content and interacts with humans on social media, trying to emulate and possibly alter their behavior." A *troll* is defined as an individual who "posts a deliberately proactive message to a newsgroup or message board with the intention of causing maximum disruption and argument," according to NATO Strategic Communications Centre of Excellence, 2016, p. 9.

[15] Attribution in this case was based on political indicators. The first wave of the attack was a response to the removal of a Soviet war memorial from Tallinn. The second wave started on May 8–9, 2007, when Russians traditionally celebrate the victory over Nazis in the Second World War. Russian officials denied any involvement in the attacks but praised the perpetrators of the attack. For a discussion of this case, see Connell and Vogler, 2017, pp. 13–16.

[16] In particular, we draw from and extend the criteria listed in Bodine-Baron et al., 2018, pp. 4–5.

[17] Snyder was the first to make the distinction between two forms of deterrence—deterrence by punishment and deterrence by denial.

[18] For the original text of the Executive Order authorizing these sanctions, see Executive Order 13661, 2014.

[19] For the full text of the act, see Public Law 115-44, 2017.

[20] See media reports on ongoing debate of whether to lift sanctions on Rusal, such as Rappeport, 2019.

References

Adamsky, Dmitry, *Cross-Domain Coercion: The Current Russian Art of Strategy*, Paris: Security Studies Center, Institut français des relations internationales (Ifri), Proliferation Papers 54, November 2015. As of July 3, 2018: https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

Alperovitch, Dmitri, "Bears in the Midst: Intrusion into the Democratic National Committee," *Crowdstrike*, blog, June 15, 2016. As of July 3, 2018: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/

Ayres, Sabra, "Russia's Shadowy World of Military Contractors: Independent Mercenaries, or Working for the Kremlin?" *Los Angeles Times*, February 18, 2019. As of May 31, 2019: https://www.latimes.com/world/europe/la-fg-russia-mercenaries-20180218-story.html

Balzer, Haley, "The Ukraine Invasion and Public Opinion," *Georgetown Journal of International Affairs,* March 19, 2015.

Bartholomew, Brian, and Juan Andrés Guerrero-Saade, "Wave Your False Flags! . . . or the Nightmares and Nuances of Self-Aware Attribution Space," SecureList website, October 6, 2016. As of July 3, 2018: https://securelist.com/wave-your-false-flags/76273/

Bērziņš, Jānis, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Riga, Latvia: National Defence Academy of Latvia, Center for Security and Strategic Research, Policy Paper No. 2, April 2014.

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence,* Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018. As of November 1, 2018: https://www.rand.org/pubs/research_reports/RR2740.html

Boghardt, Thomas, "Operation Infektion: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence,* Vol. 53, No. 4, December 2009. As of July 3, 2018: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf

Borak, Donna, "US Imposes Sanctions Against Russian Oligarchs and Government Officials," CNN, April 6, 2018. As of April 5, 2019: https://www.cnn.com/2018/04/06/politics/russia-sanctions-oligarchs/index.html

Brattberg, Erik, and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Washington, D.C.: Carnegie Endowment for International Peace, 2018. As of April 5, 2019: https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

Cardenal, Juan Pablo, Jacek Kucharczyk, Grigorij Mesežnikov, and Gabriela Pleschová, *Sharp Power: Rising Authoritarian Influence*, Washington, D.C.: International Forum for Democratic Studies, National Endowment for Democracy, December 5, 2017. As of July 3, 2018: https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf

Central Intelligence Agency, "Soviet Radio Propaganda About Yugoslavia Since the Cominform-Tito Split," Langley, Va., CIA-RDP80-00809A000500730119-6, September 14, 1949.

———, "The Crisis in Czechoslovakia," memorandum for the Director, Langley, Va.: Office of National Estimates, July 12, 1968a. As of July 11, 2019: https://www.cia.gov/library/readingroom/docs/DOC_0000677560.pdf

———,"The I. Aleksandrov Article in Pravda: Inception of a New Stage in Pressure on Czechoslovakia," Langley, Va.: Foreign Broadcast Information Service, July 18, 1968b. As of July 11, 2019: https://www.cia.gov/library/readingroom/docs/1968-07-18.pdf

———, *Soviet Presence in the Third World: Developments in the Past Decade*, Langley, Va.: Directorate of Intelligence, October 1982. As of July 11, 2019: https://www.cia.gov/library/readingroom/docs/CIA-RDP83B00851R000300090002-3.pdf

Charap, Samuel, "The Ghost of Hybrid Warfare," *Survival,* Vol. 57, No. 6, November 23, 2015, pp. 51–58. As of July 31, 2019: https://www.tandfonline.com/doi/full/10.1080/00396338.2015.1116147

Charbonneau, Louis, "Russia: Yanukovich Asked Putin to Use Force to Save Ukraine," Reuters, March 3, 2014, As of July 18, 2018: https://www.reuters.com/article/us-ukraine-crisis-un/russia-yanukovich-asked-putin-to-use-force-to-save-ukraine-idUSBREA2224720140304

Chen, Adrian, "The Agency," *New York Times Magazine*, June 2, 2015. As of July 3, 2018: https://www.nytimes.com/2015/06/07/magazine/the-agency.html

CIA—*See* Central Intelligence Agency.

Cohen, Raphael S., and Andrew Radin, *Russia's Hostile Measures in Europe: Understanding the Threat*, Santa Monica, Calif.: RAND Corporation, RR-1793-A, 2019. As of January 28, 2019: https://www.rand.org/pubs/research_reports/RR1793.html

Conley, Heather, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, Washington, D.C.: Center for Strategic and International Studies, October 2016. As of January 27, 2019: https://www.csis.org/analysis/kremlin-playbook

Connell, Michael, and Sarah Vogler, *Russia's Approach to Cyber Warfare*, Arlington, Va.: CNA, March 2017. As of July 3, 2018: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Darczewska, Jolanta, *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*, Warsaw, Poland: Centre for Eastern Studies, May 2014. As of July 3, 2018: https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study

Davis, John S., II, Benjamin Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, and Michael S. Chase, *Stateless Attribution: Toward International Accountability in Cyberspace*, Santa Monica, Calif.: RAND Corporation, RR-2081-MS, 2017. As of July 3, 2018: https://www.rand.org/pubs/research_reports/RR2081.html

Dempsey, Judy, "Lithuanians Suspect Russia of Dirty Tricks," *New York Times*, August 7, 2006. As of July 3, 2018: https://www.nytimes.com/2006/08/07/world/europe/07iht-pipeline.2410161.html

Digital Forensics Research Lab, "Breaking Down the Surkov Leaks," Medium website, October 25, 2016. As of July 3, 2018: https://medium.com/dfrlab/breaking-down-the-surkov-leaks-b2feec1423cb

Director of Central Intelligence, *Trends in Soviet Policy Toward Sub-Saharan Africa*, Langley, Va., NIE 11-12-62, December 5, 1962. As of April 5, 2019: https://www.cia.gov/library/readingroom/docs/DOC_0000272880.pdf

———, *Soviet Military Capabilities to Project Power and Influence in Distant Areas*, Langley, Va., NIE 11-10-79, 1979. As of July 3, 2018: https://www.cia.gov/library/readingroom/docs/DOC_0000278536.pdf

Dylevski, Igor, V. P. Elyas, S. A. Komov, A. N. Petrunin, and V. O. Zapivakhin, "Political and Military Aspects of the Russian Federation's State Policy on International Information Security," *Military Thought*, Vol. 24, No. 1, 2015, pp. 7–16.

Estonian Foreign Intelligence Service, *International Security and Estonia 2018*, February 9, 2018. As of July 3, 2018: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

Eurasia Foundation, "Programs," webpage, 2019. As of January 21, 2019: http://www.eurasia.org/Programs#Eurasia

Executive Order 13660, *Blocking Property of Certain Persons Contributing to the Situation in Ukraine*, March 6, 2014. As of April 5, 2019: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_eo.pdf

Federal Bureau of Investigation, "Soviet Active Measures in the United States—An Updated Report by the FBI," extension of remarks, *Congressional Record*, December 9, 1987. As of July 3, 2018: https://www.cia.gov/library/readingroom/docs/CIA-RDP11M01338R000400470089-2.pdf

Ferrara, Emilio, Onur Varol, Clayton Davis, Filippo Menczer, and Alessandro Flammini, "The Rise of Social Bots," *Communications of the ACM*, Vol. 59, No. 7, July 2016, pp. 96–104. As of July 3, 2018: https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext

FireEye iSight Intelligence, "APT28: At the Center of the Storm, Russia Strategically Evolves Its Cyber Operations," *Threat Research*, blog, January 11, 2017. As of July 31, 2019: https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html

Fly, Jamie, Laura Rosenberger, and David Salvo, *The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies*, Washington, D.C.: German Marshall Fund of the United States, June 26, 2018.

Frederick, Bryan, Matthew Povlock, Stephen Watts, Miranda Priebe, and Edward Geist, *Assessing Russian Reactions to U.S. and NATO Posture Enhancements*, Santa Monica, Calif.: RAND Corporation, RR-1879-AF, 2017. As of November 1, 2018: https://www.rand.org/pubs/research_reports/RR1879.html

Fried, Daniel, and Alina Polyakova, *Democratic Defense Against Disinformation*, Washington, D.C.: Atlantic Council, February 2018. As of July 1, 2018: http://www.atlanticcouncil.org/publications/reports/democratic-defense-against-disinformation

F-Secure, "The Dukes: 7 Years of Russian Cyberespionage," Warren, N.J., 2016. As of July 3, 2018: https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf

Galeotti, Mark, “The ‘Gerasimov Doctrine’ and Russian Non-Linear War,” *In Moscow’s Shadows*, blog, July 6, 2014. As of July 3, 2018: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

———, “Putin’s Hydra: Inside Russia’s Intelligence Services,” policy brief, Berlin: European Council on Foreign Relations, May 2016. As of July 3, 2018: http://www.ecfr.eu/page/-/ECFR_169_-_INSIDE_RUSSIAS_INTELLIGENCE_SERVICES_(WEB_AND_PRINT)_2.pdf

———, “Controlling Chaos: How Russia Manages Its Political War in Europe,” policy brief, Berlin: European Council on Foreign Relations, September 1, 2017. As of July 3, 2018: http://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe

———, “I’m Sorry for Creating the ‘Gerasimov Doctrine,’” *Foreign Policy*, March 5, 2018. As of July 3, 2018: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

Gerasimov, Valery, “Nauki v predvidenii,” *Voenno-promyshlenni kurier* (in Russian), 2013. As of July 3, 2018: https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

Greene, Sam, and Graeme Robertson, “Explaining Putin’s Popularity: Rallying Round the Russian Flag,” *Washington Post*, September 9, 2014. As of July 3, 2018: https://www.washingtonpost.com/news/monkey-cage/wp/2014/09/09/explaining-putins-popularity-rallying-round-the-russian-flag/?utm_term=.541b625e6f54

Helmus, Todd C., Elizabeth Bodine-Baron, Andrew Radin, Madeline Magnuson, Joshua Mendelsohn, William Marcellino, Andriy Bega, and Zev Winkelman, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, Santa Monica, Calif.: RAND Corporation, RR-2237-OSD, 2018. As of July 3, 2018: https://www.rand.org/pubs/research_reports/RR2237.html

Joint Publication 1, *Doctrine for the Armed Forces of the United States*, Washington, D.C.: U.S. Department of Defense, July 12, 2017. As of July 3, 2018: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

Kennan, George [“X”], “The Sources of Soviet Conduct,” *Foreign Affairs*, July 1947. As of July 3, 2018: https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct

Kimmage, Michael, “Russian Elegies: Candide Goes to Moscow,” War on the Rocks website, June 31, 2018. As of July 31, 2019: https://warontherocks.com/2018/06/russian-elegies-candide-goes-to-moscow/

Kofman, Michael, “Russian Hybrid Warfare and Other Dark Arts,” War on the Rocks website, March 11, 2016. As of July 3, 2018: https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia’s Operations in Crimea and Eastern Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1498-A, 2017. As of July 3, 2018: https://www.rand.org/pubs/research_reports/RR1498.html

Korsunskaya, Darya, “Putin Says Russia Must Prevent ‘Color Revolution,’” Reuters, November 20, 2014. As of July 3, 2018: https://www.reuters.com/article/us-russia-putin-security-idUSKCN0J41J620141120

Kramer, Andrew E., “Ukrainian Hackers Release Emails Tying Top Russian Official to Uprising,” *New York Times*, October 27, 2016. As of July 3, 2018: https://www.nytimes.com/2016/10/28/world/europe/ukraine-russia-emails.html

Larrabee, F. Stephen, Stephanie Pezard, Andrew Radin, Nathan Chandler, Keith Crane, and Thomas S. Szayna, *Russia and the West After the Ukrainian Crisis: European Vulnerabilities to Russian Pressures*, Santa Monica, Calif.: RAND Corporation, RR-1305-A, 2017. As of February 13, 2019: https://www.rand.org/pubs/research_reports/RR1305.html

Mattis, Jim, “Summary of the 2018 National Defense Strategy of the United States of America,” Washington, D.C.: U.S. Department of Defense, 2018. As of April 5, 2019: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

McFaul, Michael, *From Cold War to Hot Peace: An American Ambassador in Putin’s Russia*, Boston: Houghton Mifflin Harcourt, 2018.

Ministry of Foreign Affairs of the Russian Federation, *National Security Concept of the Russian Federation*, January 10, 2000. As of July 3, 2018: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768

———, *Doctrine of Information Security of the Russian Federation*, December 5, 2016. As of July 3, 2018: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Nakashima, Ellen, "Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post,* January 12, 2018. As of April 5, 2019: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.6156b660496d

National Security Agency, "Dodging Armageddon: The Third World War That Almost Was, 1950," *Cryptologic Quarterly*, February 24, 1998. As of July 11, 2019: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/Dodging_Armageddon.pdf

NATO Strategic Communications Centre of Excellence, *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*, Riga, Latvia: 2016. As of July 3, 2018: https://www.stratcomcoe.org/internet-trolling-hybrid-warfare-tool-case-latvia-0

Obama, Barack, "Statement by the President on Ukraine," Washington, D.C.: The White House, Office of the Press Secretary, March 6, 2014a. As of April 5, 2019: https://obamawhitehouse.archives.gov/the-press-office/2014/03/06/statement-president-ukraine

———, "Statement by the President on Ukraine," Washington, D.C.: The White House, Office of the Press Secretary, March 20, 2014b. As of April 9, 2019: https://obamawhitehouse.archives.gov/the-press-office/2014/03/20/statement-president-ukraine

Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, Intelligence Community Assessment, January 6, 2017. As of July 3, 2018: https://www.dni.gov/files/documents/ICA_2017_01.pdf

Oliker, Olga, Keith Crane, Lowell H. Schwartz, and Catherine Yusupov, *Russian Foreign Policy: Sources and Implications*, Santa Monica, Calif.: RAND Corporation, MG-768-AF, 2009. As of July 3, 2018: https://www.rand.org/pubs/monographs/MG768.html

Pasha-Robinson, Lucy, "Marine Le Pen Backs Vladimir Putin and Denies Invasion of Crimea," *Independent*, February 7, 2017. As of July 3, 2018: https://www.independent.co.uk/news/world/europe/marine-le-pen-front-national-russian-kremlin-putin-invasion-annexation-crimea-ukraine-2014-a7566196.html

Paul, Christopher, and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of May 26, 2018: https://www.rand.org/pubs/perspectives/PE198.html

Petroff, Alanna, "U.S.-Russia Business Ties: 5 Things You Need to Know," CNN, July 7, 2017. As of January 21, 2019: https://money.cnn.com/2017/07/06/news/economy/us-russia-trump-putin-business-trade/index.html

Pezard, Stephanie, Andrew Radin, Thomas S. Szayna, and F. Stephen Larrabee, *European Relations with Russia: Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis*, Santa Monica, Calif.: RAND Corporation, RR-1579-A, 2017. As of May 25, 2018: https://www.rand.org/pubs/research_reports/RR1579.html

PKN ORLEN, "PKN ORLEN Has Signed An Agreement with Yukos That Enables the Company to Acquire Mažeikių Nafta," Warsaw, Poland, May 26, 2006. As of July 3, 2018: https://www.orlen.pl/EN/PressOffice/Pages/PKNORLENhassignedanagreem.aspx

Public Law 115-44, Countering America's Adversaries Through Sanctions Act (CAATSA), August 2, 2017. As of April 5, 2019: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/hr3364_pl115-44.pdf

Radin, Andrew, *Hybrid Warfare in the Baltics: Threats and Potential Responses,* Santa Monica, Calif.: RAND Corporation, RR-1577-AF, 2017. As of July 3, 2018: https://www.rand.org/pubs/research_reports/RR1577.html

Radin, Andrew, Lynn Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clinton Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston, and Austin Long, *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition*, Santa Monica, Calif.: RAND Corporation, RR-3099-A, 2019. As of July 31, 2019: https://www.rand.org/pubs/research_reports/RR3099.html

Radin, Andrew, and Clint Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017. As of July 3, 2018: https://www.rand.org/pubs/research_reports/RR1826.html

RAND Corporation, "Building a Sustainable International Order," project page, undated. As of April 5, 2019: https://www.rand.org/nsrd/projects/international-order.html

Rappeport, Alan, "Mnuchin Defends Plan to Lift Sanctions on Russian Oligarch's Companies," *New York Times,* January 10, 2019. As of January 19, 2019: https://www.nytimes.com/2019/01/10/us/politics/mnuchin-russia-sanctions.html

ReedSmith, "Overview of the U.S. and EU Sanctions on Russia," special update, October 2014. As of April 5, 2019: https://www.reedsmith.com/-/media/files/perspectives/2014/10/overview-of-the-us-and-eu-sanctions-on-russia/files/overview-of-the-us-and-eu-sanctions-on-russia/fileattachment/alert_14255.pdf

Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, Santa Monica, Calif.: RAND Corporation, RR-1772-A, 2018. As of July 3, 2018: https://www.rand.org/pubs/research_reports/RR1772.html

Rosneft, "Board of Directors: Gerhard Schroeder," webpage, 2018. As of October 24, 2018: https://www.rosneft.com/governance/board/item/187923/

Russian Armed Services, *Military Doctrine of the Russian Federation*, December 26, 2014.

Samokhvalova, Lana, "The Russian Organizers of a 'Third Maidan' in Ukraine," *Euromaidan Press*, February 14, 2016. As of July 3, 2018: http://euromaidanpress.com/2016/02/14/the-russian-organizers-of-a-third-maidan-in-ukraine/

Satter, Raphael, "Russian Hackers Posed as IS to Threaten Military Wives," Associated Press, May 8, 2018, As of July 18, 2018: https://www.apnews.com/4d174e45ef5843a0ba82e804f080988f

"SBU Releases Intercepted Comms Between PMC Wagner Chief, Russian Army General on Donbas Incursion," UNIAN Information Agency, January 23, 2018. As of July 3, 2018: https://www.unian.info/war/2360147-sbu-releases-intercepted-communications-between-russian-pmc-wagner-chief-russian-army-general-on-donbas-incursion.html

Schmitt, Eric, and Steve Lee Myers, "NATO Refocuses on the Kremlin, Its Original Foe," *New York Times*, June 23, 2015. As of January 21, 2019: https://www.nytimes.com/2015/06/24/world/europe/nato-returns-its-attention-to-an-old-foe-russia.html

Snyder, Glenn H., "Deterrence and Power," *Journal of Conflict Resolution*, Vol. 4., No. 2, June 1, 1960, pp. 163–178. As of April 5, 2019: https://journals.sagepub.com/doi/pdf/10.1177/002200276000400201

———, *Deterrence and Defense: Toward a Theory of National Security*, 1961, Princeton, N.J.: Princeton University Press, 1961.

"Spy Poisoning: NATO Expels Russian Diplomats," BBC, March 27, 2018. As of November 1, 2018: https://www.bbc.com/news/world-asia-43550938

Stuttaford, Andrew, "On Shooting 'Little Green Men,'" *National Review*, May 14, 2015. As of January 21, 2019: https://www.nationalreview.com/corner/shooting-little-green-men-andrew-stuttaford/

Thomas, Timothy, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies*, Vol. 17, No. 2, 2004. As of July 3, 2018: https://www.tandfonline.com/doi/abs/10.1080/13518040490450529

ThreatConnect, "Belling the BEAR," webpage, September 28, 2016. As of July 3, 2018: https://threatconnect.com/blog/russia-hacks-bellingcat-mh17-investigation/

United States of America v. Internet Research Agency LLC, Washington, D.C.: United States District Court for the District of Columbia, Case 1:18-cr-00032-DLF, February 16, 2018. As of July 3, 2018: https://www.justice.gov/file/1035477/download

U.S. Congress, *Soviet Covert Action: The Forgery Offensive*, 1980. Partial text, as of June 6, 2019: https://archive.org/stream/ForeignIntelAnalysis19721988/FBI-HQ-74480-ForeignIntelAnal_1972-1988_djvu.txt

U.S. Department of State, "Ukraine and Russia Sanctions," webpage, undated. As of April 5, 2019: https://www.state.gov/e/eb/tfs/spi/ukrainerussia/

———, "Probability of an Invasion of Yugoslavia in 1951," Washington, D.C., National Intelligence Estimate 29, March 20, 1951. As of July 11, 2019: https://history.state.gov/historicaldocuments/frus1951v04p2/d411

———, "Joint Statement on U.S.-Ukraine Strategic Partnership," November 16, 2018. As of January 29, 2020: https://ua.usembassy.gov/joint-statement-on-u-s-ukraine-strategic-partnership/

Vilmer, Jean-Baptiste Jeangène, "Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks," brief, Washington, D.C.: Center for Strategic and International Studies, June 2018. As of October 24, 2018: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf?qFOz5qjpEuTzu5cvUa.UgOj0Dg3FklQP

Voltz, Dustin, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage," Reuters, February 25, 2016. As of July 3, 2018: https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K

Wilkes, William, "U.S. Warns Sanctions Possible if Nord Stream 2 Pipe Proceeds," Bloomberg, May 17, 2018. As of July 3, 2018: https://www.bloomberg.com/news/articles/2018-05-17/u-s-warns-sanctions-possible-if-nord-stream-2-pipe-proceeds

Wilson, Andrew, *Virtual Politics: Faking Democracy in the Post-Soviet World*, New Haven, Conn.: Yale University Press, 2005.

Zengerle, Patricia, "U.S. Senators Introduce Russia Sanctions 'Bill from Hell,'" Reuters, August 2, 2018. As of August 2, 2018: https://www.reuters.com/article/us-usa-russia-sanctions/us-senators-introduce-russia-sanctions-bill-from-hell-idUSKBN1KN22Q

Zhdannikov, Dmitry, Richard Lough, and Lesley Wroughton, "How Rusal Escaped the Noose of U.S. Sanctions," Reuters, May 15, 2018. As of April 5, 2019: https://www.reuters.com/article/us-usa-sanctions-rusal-insight/how-rusal-escaped-the-noose-of-u-s-sanctions-idUSKCN1IG3G6

Acknowledgments

We would like to thank several individuals who made this report possible. First, we would like to thank MG Christopher McPadden, MG William Hix, and Walter Vanderbeek for funding and supervising this project. At RAND, we also would like to thank Sally Sleeper, Karl Mueller, and Abby Doll, the project leaders, for providing us the funding and guidance for this research. Joseph Cheravitch also offered helpful suggestions. We very much appreciate the helpful peer reviews by Raphael Cohen of RAND and Jeffrey Edmonds of the Center for Naval Analyses.

About This Perspective

This report documents research and analysis conducted as part of a project entitled Comprehensive Strategy for Meeting Five Russian Challenges, sponsored by the Office of the Deputy Chief of Staff, G-3/5/7, U.S. Army. The purpose of the project was to develop a strategy to assess the connections and interactions among the major problems and challenges the U.S. and NATO might face with Russia in a war or other hostile environment, and provide policy options for decisionmakers.

This research was conducted within RAND Arroyo Center's Strategy, Doctrine, and Resources Program. RAND Arroyo Center, part of the RAND Corporation, is a federally funded research and development center (FFRDC) sponsored by the United States Army.

RAND operates under a "Federal-Wide Assurance" (FWA00003425) and complies with the Code of Federal Regulations for the Protection of Human Subjects Under United States Law (45 CFR 46), also known as "the Common Rule," as well as with the implementation guidance set forth in DoD Instruction 3216.02. As applicable, this compliance includes reviews and approvals by RAND's Institutional Review Board (the Human Subjects Protection Committee) and by the U.S. Army. The views of sources utilized in this study are solely their own and do not represent the official policy or position of DoD or the U.S. Government.

About the Authors

Alyssa Demus is a policy analyst at the RAND Corporation. Her work focuses on Russian and Eurasian security and political issues, the use of information efforts to influence populations, and deterrence.

Krystyna Marcinek is an assistant policy researcher at RAND Corporation and a Ph.D. candidate at the Pardee RAND Graduate School. Her research focuses on Russia and the future environment of warfighting.

Andrew Radin is a political scientist at the RAND Corporation. His work has focused on Russia and European security, including the threat of Russian political warfare, hybrid warfare, and measures short of war.

For more information on this publication, visit www.rand.org/t/PE331.

RAND
CORPORATION

www.rand.org