FOUNDATION FOR DEFENSE OF DEMOCRACIES

Russian Hybrid Warfare:
How to Confront a New Challenge to the West

Pasi Eronen

Center on Sanctions
& Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

June 2016

Russian Hybrid Warfare: How to Confront a New Challenge to the West

Pasi Eronen

June 2016

FDD PRESS

A division of the
FOUNDATION FOR DEFENSE OF DEMOCRACIES
Washington, DC

Table of Contents

Executive Summary

In 2013, General Valery Gerasimov, chief of Russia's Armed Forces, publicly unveiled a fresh idea. In what came to be called the Gerasimov Doctrine,[1] he described "new-generation" warfare – pre-emptive operations employing a mixture of nonmilitary and military measures to achieve political goals, deploying all elements of society.[2]

Gerasimov suggested that such mobilization was urgent because Russia was already behind its enemies – implicitly the West, which was wielding a strategy that it called "hybrid warfare." Russia, Gerasimov said, needed not only to catch up, but to get out well in front. Technically, he was right – the United States does enjoy considerable global reach in cyber espionage, for example. But Gerasimov found hybrid warfare where there was none, such as the West's insistence on a no-fly zone in Libya and in Syrian humanitarian missions, operations that Gerasimov called camouflaged strategies of aiding one side (the rebels) for political gain.[3] And the Russian general's appraisal of Moscow's combat readiness in the new age was disingenuous: Russia began to build up cyberspace expertise in the 1990s, when its Soviet-era military capability had wilted, and it embarked on a determined hunt for an arena to confront the West.

This paper examines the threat posed by Russia's new generation warfare to the interests and security of the U.S. and its allies – in the military arena, and in technology, economics, and culture.[4] It is the first in a three-part series on the dynamics and specific contours of the intensifying financial, military, and geopolitical conflict between the West and Russia.

An End to a Largely Peaceful Post-Soviet Period

When the worst of the Balkan wars ended almost two decades ago, a period of general European calm unfolded, disturbed only in 1999 by brief fighting in Kosovo. Because of the relative quiet, the West came to expect a lasting return of its prior post-World War II insulation from major combat. European militaries dialed back and came to resemble more of an

[1] Валерий Герасимов, "Новые вызовы требуют переосмысле- ния форм и способов ведения боевых действий (New challenges require a rethink of the forms and methods of warfare)," *Военно- промышленный курьер* (Russia), March 5, 2013. (http://www.vpk-news.ru/articles/14632)

[2] Jānis Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," *National Defence Academy of Latvia*, April 2014. (http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx); Mark Galeotti, "The 'Gerasimov Doctrine' and Russian NonLinear War," *In Moscow's Shadows,* July 6, 2014. (https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/); S. G. Chekinov and S. A. Bogdanov, "The Nature and Content of a New-Generation War," *Military Thought,* October-December 2013. (http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf)

[3] In August 2014, the world witnessed columns of Russian military trucks painted in white crossing the border mostly uninspected into the separatist areas in Ukraine under a humanitarian pretext. Michael Weiss, "A White Shining Lie," *Foreign Policy,* August 22, 2014. (http://foreignpolicy.com/2014/08/22/a-white-shining-lie/)

[4] For clarity, this paper will use the term "hybrid warfare" to describe both Western and Russian strategy and capability in this arena.

international policing force than a well-oiled fighting machine prepared to defend the NATO alliance.

But the Putin era – and the pursuit of a restoration of Moscow's international stature – has forced a re-contemplation of the historical arc.

Since his rise to power, Russian President Vladimir Putin has repeatedly surprised the West with demonstrations of an emboldened Kremlin, and revived some of the most troubling aspects of Cold War politics. But most recently, he has pursued his political goals through hybrid warfare.

In what is effectively a permanent state of war, Putin holds together a Russian national consensus through tightly scripted, state-controlled media that sustain a drumbeat against a morally bankrupt and power-obsessed West. The instruments of this asymmetrical battle often involve major regime-linked corporations, cyber weapons, and propaganda. Wielded by a nimble, opportunistic Putin, they pose a long-term policy challenge to the United States and Europe.

On December 31, 2015, Putin named the United States a national security threat, the first time Russia has so designated Washington since the Soviet collapse about a quarter-century ago.[5] The U.S. has done the same – the Department of Defense's updated Cyber Strategy names Russia as the top threat to American interests and security.[6]

Putin, who has served alternately as prime minister or president since 1999, launched his new brinksmanship four years ago when he returned to the presidency for the second time. His apparent new objective has been to revive Russia's strategic global parity with the United States.

This is not new: Since the Soviet disintegration, Moscow has relentlessly sought, generally without success, to recover its lost role as an essential superpower. But Putin's recent actions – from military offensives in Ukraine and Syria to a confrontation with the International Monetary Fund, the World Bank, and the SWIFT banking system – demonstrate a new sense of determination. Taken as a whole, Putin is attempting to overturn pillars of the post-World War II political and economic order.

Some analysts attribute the current tensions to NATO enlargement and a supposed Western disregard for Moscow's voice in international affairs.[7] But the brinksmanship with Putin more accurately fits into a much longer history of conflict with the West,[8] one rooted in a narrative of victimhood, resentment, and "encirclement." In Putin's mind, the U.S. has embarked on an imperious campaign to humiliate and unseat him – a conspiracy whose "color revolutions" have already taken down governments in Georgia and Ukraine, along with those of several Arab states, and whose next target is him.[9] Much of the Russian leader's tension with the U.S. has flowed from his inability to shed that conception.

[5] Vladimir Soldatkin, "Putin names United States among threats in new Russian security strategy," *Reuters,* January 2, 2016. (http://www.reuters.com/article/russia-security-strategy-idUSKBN0UG09Q20160102)

[6] U.S. Department of Defense, "The Department of Defense Cyber Strategy," April 2015. (http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf)

[7] Steven R. Hurst, "Ukraine crisis has roots in end of Cold War, disregard of Russian sensitivities," *Associated Press,* March 20, 2014. (https://www.neweurope.eu/article/analysis-ukraine-crisis-has-roots-end-cold-war-disregard-russian-sensitivities-0/)

[8] Kadri Liik, "The limits and necessity of Europe's Russia sanctions," *European Council on Foreign Relations,* August 3, 2015. (http://www.ecfr.eu/article/commentary_the_limits_and_necessity_of_europes_russia_sanctions3091)

[9] Evgenia Pismennaya and Henry Meyer, "Russia Accuses U.S. of Plot to Oust Putin Via Opposition Aid," *Bloomberg,* March 4, 2015. (http://www.bloomberg.com/news/articles/2015-03-04/russia-accuses-u-s-of-plot-to-oust-putin-by-funding-opposition)

In 2014, Putin annexed Crimea and destabilized eastern Ukraine.[10] The West responded with punishing economic sanctions on Russia's next-generation oil production in the Arctic and Siberia. Yet Putin has doubled down with an air-led offensive into Syria – 3,400 miles from Russian territory – Moscow's first venture outside its former imperial realm since the Soviet collapse.

Amid a show of hybrid tactics, Putin has awarded financial support to fringe political movements in Western Europe, launched cyberattacks and espionage in Europe, and ordered probing and actual attacks on U.S. and European energy and communications infrastructure. He has continued to attempt to use control over energy – pipelines, nuclear plants, natural gas supplies – to wield influence across Europe. Western intelligence reports say Russia has exacerbated the Syrian migrant crisis. And, compounding the threat, Russia has formed a growing alliance with Iran and China, countries that possess their own hybrid toolboxes of proxy warfare and cyber infiltration.[11]

To Western queries about Russian intentions, Putin has replied that he has consistently made Moscow's interests clear, but that the West has ignored him. That history is beyond the scope of this report. Suffice it to say, however, that while Russia is going through the diplomatic motions, it is resorting to hybrid war tactics as a first order of geostrategic business.

What Is Hybrid Warfare?

Hybrid combat – the combination of violent and nonviolent means in the service of political goals – is an age-old concept.[12] At relatively low expense,[13] an aggressive player intentionally blurs and exploits distinctions of war and peace, civilian and military operations, and state and non-state actors.

In the last century, the U.S. and the Soviet Union carried out countless examples of hybrid warfare, what their intelligence apparatuses called *active measures*. Short of actual fighting, this dimension of the superpower rivalry included, from the U.S. side, the CIA's 27-year, $75 million funding of Italy's Christian Democrats; and, from the Soviets, the 1978 murder of Bulgarian dissident Georgi Markov with a poison-tipped umbrella.[14] Some Russian tactics in Ukraine over the past two years resemble Moscow's political absorption – its Sovietization – of the Warsaw Bloc in the late 1940s and early 1950s.[15]

In a way, today's actions appear to be merely a return to the Soviet-era status quo. Yet, this is not the Soviet period: Notwithstanding Putin's declaration of a Western threat and the daggers-drawn conclusions of their respective intelligence communities, Russia and the United States are not sworn enemies. And Western European countries are by and large demilitarized and generally violence-averse.

[10] András Rácz, "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist," The *Finnish Institute of International Affairs,* June 16, 2015. (http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine/)

[11] Michael J. Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict," *Strategic Studies Institute,* December 2, 2015, pages 1, 44. (http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1303.pdf); Barbara Slavin and Jason Healey, "Iran: How a Third Tier Cyber Power Can Still Threaten the United States," *Atlantic Council,* July 29, 2013. (http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf); Peter Pomerantsev, "Brave New War," *The Atlantic,* December 29, 2015. (http://www.theatlantic.com/international/archive/2015/12/war2015chinarussiaisis/422085/)

[12] Frank Hoffman, "On Not-So-New Warfare: Political Warfare vs Hybrid Threats," *War on the Rocks,* July 28, 2014. (http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/)

[13] Michael J. Mazarr, "Mastering the Gray Zone: Understanding a Changing Era of Conflict," *Strategic Studies Institute,* December 2, 2015, pages 55-57. (http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1303.pdf)

[14] Kevin A. O'Brien, "The 'Quiet Option' in International Statecraft," *Strategic Intelligence, Volume 3: Covert Action: Behind the Veils of Secret Foreign Policy,* Ed. Loch K. Johnson, (Westport, CT: Praeger Security International, 2007), pages 27-60.

[15] Anne Applebaum, *Iron Curtain: The Crushing of Eastern Europe, 1944-1956,* (Doubleday, 2012).

Russia's conduct is in fact novel in the modern age, deploying comparatively few conventional forces explicitly aimed at attacking the West, but focusing instead on the agile coordination of other instruments of national power.[16] Since Russia cannot hope to match U.S. capability head-to-head, these tools are by necessity asymmetrical, and are unleashed where they are not expected. Moscow's over-arching tactic is *maskirovka*, which loosely translated means subterfuge – the elements of surprise, diversion, and deception. All in all, Russia's conduct capitalizes on Putin's readiness to act outside the post-war operational norms within which the West has built its military and political response mechanisms.

Cyberspace is a primary theater of Russia's asymmetrical activity. This is because cyberspace offers a way to easily combine fighting arenas, including espionage, information operations, and conventional combat, and to do so behind a curtain of plausible deniability, for example by taking advantage of proxy operators. A perpetrator can stealthily cross great distances without physical barriers and reach the target.[17]

In addition, such actions can combine two or more instruments: political, intelligence, diplomatic, cyber, or information. Russia can do so with no emphasis on speed: Rapid, decisive victory is unnecessary because the ebb and flow of combat can exhaust a target's resources, or generate confusion, and trigger a response that serves Russian goals just as well. Active combat can be followed by frozen conflict, which also can serve the original political purpose and constitute "winning." In the parlance of the art, exploiting such responses is *reflexive control.*

Autocratic societies such as Russia and China are best positioned to engage in hybrid warfare. As centralized decision-makers, they can move fast, unhindered by democratic checks and balances, such as an independent legislative branch. They can prolong operations without the need to publicly justify the use of resources, or, in many cases, explain battlefield casualties. For these and other reasons, they can easily wage hybrid war in perceived peacetime, when it is harder for Western liberal democracies to build public and legislative support for the government expense and risk to troops.

Russia begins with most of the preconditions for successful hybrid warfare: strong political leadership to order an attack, a sophisticated intelligence apparatus to identify vulnerabilities, control over a wide array of resources that can be rapidly deployed, and a highly developed information and propaganda capability for both internal and external communications.[18]

In practice, Russian hybrid attacks have employed diplomacy; cyberspace and information warfare; the threat of and actual use of military force, including scorched-Earth tactics against civilians; economic inducement and coercion; and legal tactics such as utilizing court systems.[19]

[16] Nadia Schadlow, "The Problem with Hybrid Warfare," *War on the Rocks,* April 2, 2015. (http://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/)

[17] Aapo Cederberg, "Future Challenges in Cyberspace," *Geneva Centre for Security Policy,* April 2015. (http://www.gcsp.ch/News-Knowledge/Publications/Future-Challenges-in-Cyberspace)

[18] Aapo Cederberg and Pasi Eronen, "How are Societies Defended against Hybrid Threats?" *Geneva Centre for Security Policy,* September 2015. (http://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats); Keir Giles, "Western Media Must Get Creative in Infowar," *The Moscow Times* (Russia), August 4, 2015. (http://www.themoscowtimes.com/opinion/article/western-media-must-get-creative-in-infowar/527000.html)

[19] Keir Giles, Philip Hanson, Roderic Lyne, James Nixey, James Sherr, and Andrew Wood, "The Russian Challenge," *Chatham House,* June 2015, pages 40-49. (https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150605RussianChallengeGilesHansonLyneNixeySherrWood.pdf)

Understanding Russia's View of Cyberwarfare

To understand the scope of Russia's preoccupation with cyberspace, go back to the mid-1980s when Clifford Stoll, an astronomer-turned-computer-administrator, helped to uncover one of the world's first well-documented cyber incidents, the so-called *Cuckoo's Egg*. West German hackers had penetrated the computers of several U.S.-based research institutions and military installations in a hunt for secret information that they sold to the KGB. Among other keyword-based searches, the perpetrators were seeking classified information related to the Strategic Defense Initiative and KH-11, a state-of-the-art digital imaging reconnaissance satellite.[20] There also was the offer of more basic but – to the Soviets, subject to western technological restrictions – highly valuable data including source code to the Unix operating system and the design of integrated circuits.

While a cyber espionage case harking back nearly 30 years may sound dated, it highlights Moscow's long, keen interest in an advantage in cyberspace, and its grasp of its strategic importance. [21]

As practiced by Russia, cyberwarfare is actually a broader concept than conventionally understood. In 2012, the White House issued Presidential Policy Directive 20, which defined cyberspace as "the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded processors and controllers."[22] This is the technology-centric domain of offensive and defensive cyberwarfare.

But Russia has broadened the domain to allow for information warfare as well.[23] This distinction becomes clear in Russia's operational thinking, which divides information warfare into two areas: information-technical, which aligns with the West's definition of electronic warfare and cyber warfare, and information-psychological, which absorbs the Western idea of strategic communications and psychological operations.[24]

The distinction is important because of the prominent role of information warfare. Russia aggressively manipulates news and other public data with a military doctrine under which the operating environment is continuously shaped, in times of war and peace. The Russian military conducts operations both in the country's own information sphere – its media and Internet space – and outside its borders.[25]

A first sign of this new era of hybrid war came in a five-year string of hacking attacks from 1998 to 2003 called *Moonlight Maze*. While many details are still publicly unknown, hackers traced to Russia stole thousands of U.S. military documents containing sensitive information, including encryption technologies. The hackers installed back doors in an effort to maintain access once their active attack was over.[26]

[20] Clifford Stoll, "Stalking the Wily Hacker," *Communications of the ACM,* May 1988. (http://pdf.textfiles.com/academics/wilyhacker.pdf)
[21] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," *Cyber War in Perspective: Russian Aggression against Ukraine,* Ed. Kenneth Geers, (Tallinn, Estonia: NATO CCD COE Publications, 2015), pages 29-37.
[22] The White House, "Presidential Policy Directive 20 U.S. Cyber Operations Policy," October 16, 2012. (https://fas.org/irp/offdocs/ppd/ppd-20.pdf)
[23] Kier Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," *5th International Conference on Cyber Conflict,* 2013, pages 1-17. (https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf)
[24] Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies,* 2014.
[25] Jolanta Darczewska, "The Devil Is in the Details: Information Warfare in the Light of Russia's Military Doctrine," *Ośrodek Studiów Wschodnich* (Poland), May 2015. (http://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf)
[26] Adam Elkus, "Moonlight Maze," *A Fierce Domain: Conflict*

Subsequent cyberattacks in Estonia in 2007, Georgia in 2008, and present-day Ukraine show Russia further honing its cyber game. In Estonia, suspected Russian hackers were deployed in a political dispute over an Estonian decision to shift the Soviet-era Bronze Soldier from central Tallinn to the Defense Forces cemetery, two miles away. In some cases using Kremlin IP addresses, the hackers, in an apparent effort to punish and intimidate the Estonians, launched distributed denial of service attacks against local government websites, the country's Internet infrastructure, and its financial industry.[27]

The 2008 cyberattacks against Georgia, coinciding with the Russian-Georgian war, may be the first time that Moscow tightly integrated cyber tools into military planning and operations. These attacks, conducted by proxy actors – self-declared "patriotic" Russian hackers and the nationalist youth group Nashi – went a step further than the Estonia operation to include infrastructure system break-ins and Internet traffic diversions and blocking.[28] While the hackers did their work, Russian conventional forces rolled out a textbook example of reflexive control (described above), using feints[29] on their side of the border to tempt Georgia to initiate combat, thus justifying the Russian invasion.

Russian cyber operations advanced the furthest yet in Ukraine, demonstrating sophisticated capability in electronic and information warfare. The operation began in February 2014 with the Crimean deployment of what Russia called "polite men" (and the Western media labeled "little green men") – special forces wearing no insignia.[30] In support of special forces operations, Russia jammed and intercepted Kiev signals and communications, hampering the other side's operations, and effectively detaching the peninsula from Ukraine's information space.[31] Russian hacker groups later targeted Ukrainian elections and governmental bodies.[32] The Russian hacker group CyberBerkut[33] attacked routers, software, and hard drives at Ukraine's National Election Commission with the objective of hobbling the release of the official vote count and producing false results. Russian hackers also penetrated Ukrainian government ministries and embassies, and Western targets such as NATO.[34]

in Cyberspace, 1986 to 2012, Eds. Jason Healey and Karl Grindal, (Cyber Conflict Studies Association, 2013).

[27] Andreas Schmidt, "The Estonian Cyberattacks," *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* Eds. Jason Healey and Karl Grindal, (Cyber Conflict Studies Association, 2013), pages 174-93.

[28] Andreas Hagen, "The Russo-Georgian War 2008," *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* Eds. Jason Healey and Karl Grindal, (Cyber Conflict Studies Association, 2013), pages 194-204.

[29] "Georgia on Their Minds," *The Wall Street Journal,* October 1, 2009. (http://www.wsj.com/articles/SB10001424052748704471504574446582129281924)

[30] Gogo Lidz, "'Polite People' of Russia: Not Who You Might Expect," *Newsweek,* April 11, 2015. (http://www.newsweek.com/polite-people-russia-321759)

[31] Paul McLeary, "Russia's Winning the Electronic War," *Foreign Policy,* October 21, 2015. (http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/)

[32] Margaret Coker and Paul Sonne, "Ukraine: Cyberwar's Hottest Front," *The Wall Street Journal,* November 10, 2015. (http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671)

[33] For more information on Russian state-sponsored hacker groups, see Jen Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," *Cyber War in Perspective: Russian Aggression against Ukraine,* Ed. Kenneth Geers, (Tallinn, Estonia: NATO CCD COE Publications, 2015), pages 67-77.

[34] Margaret Coker and Paul Sonne, "Ukraine: Cyberwar's Hottest Front," T*he Wall Street Journal,* November 10, 2015. (http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671); David E. Sanger and Steven Erlanger, "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government," *The New York Times,* March 8, 2014. (http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html); Ellen Nakashima, "Russian hackers use 'zeroday' to hack NATO, Ukraine in cyber-spy campaign," *The Washington Post,* October 13, 2014. (https://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html)

In the latter half of 2015, Russia shifted to protect the gains achieved in the Ukraine hybrid operation. That shift included the Syrian mission, which, though a traditional conventional war, has reverberated with hybrid impacts in Europe. The Syrian campaign has been aimed at both Russia's domestic and global audiences. For Russians, the showy mission is a reminder of their superpower days a quarter century ago, and has thus again shored up Putin's support. Abroad, the campaign has reestablished Russia's Soviet-era reputation for far-flung military capability, forced the West to accept a Russian role in this key international affair, and in part diverted attention from Ukraine.[35]

As it advanced, the Syrian offensive appeared to take on the further objective of exacerbating the refugee crisis, pushing more migrants north and stirring former Soviet immigrants living in Europe into a disruptive force on the continent. A politically wrought and divided Europe is to the advantage of a Russia seeking concessions on questions from sanctions to natural gas infrastructure.

Another consequential achievement of the Syrian operation was to allow Russia – the world's second-largest arms exporter next to the U.S. – to test some of its latest conventional weaponry in a surprising and impressive display of battlefield prowess. This was a signal to the West that Russia is a long way from its decrepit military state in the 1990s, and much readier to confront a challenge.[36]

The Layers of Cyberspace

What follows is a structured description of cyberspace in three relevant layers:[37] technology; content and communication; and socio-cultural.

Cyberspace is a human-made *technological* entity. It is comprised of parts with distinctive roles – computers, their wired and wireless network interfaces, digital communications, routers, servers, and storage devices.

But without *content*, cyberspace would be only a hollow shell. Content includes data and information, of course, but also several layers of software that animate physical devices, such as communications protocols, operating systems, and applications. Content combined with technology is what gives rise to a networked system connecting individual computers in various places and roles. The network can include personal computers, servers, and controllers of other devices such as systems that operate dams, electric grids, industrial plants, and natural gas pipelines.

Finally, because of the human-made dimensions of both the physical platform and the content residing in it, cyberspace also has a *socio-cultural* aspect. Cyberspace is integral to communications and social media, and thus provides a path to manipulate the information sphere and influence public opinion and policy decisions.

[35] Angela Stent, "Putin's Power Play in Syria," *Foreign Affairs,* December 14, 2015. (https://www.foreignaffairs.com/articles/united-states/2015-12-14/putins-power-play-syria); Natalie Nougayrède, "What happens next in Aleppo will shape Europe's future," *The Guardian* (UK), February 5, 2016. (http://www.theguardian.com/commentisfree/2016/feb/05/aleppo-europe-vladimir-putin-russian-military)

[36] Reid Standish, "Russia Is Using Syria as a Training Ground for Its Revamped Military and Shiny New Toys," *Foreign Policy,* December 9, 2015. (http://foreignpolicy.com/2015/12/09/russia-is-using-syria-as-a-training-ground-for-its-revamped-military-and-shiny-new-toys/)

[37] The approach has been inspired by: Edward Skoudis and Elihu Zimet, "A Graphical Introduction to the Structural Elements of Cyberspace," *Cyberpower and National Security,* Eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (Washington, DC: National Defense University Press, 2010); Martin C. Libicki and Project Air Force, *Cyberdeterrence and Cyberwar,* (Santa Monica, CA: Rand Corporation, 2009).

Technology

During the initial days after seizing Crimea, Russia sought first to sever the local population and regionally-based military units from mainland Ukraine. It attacked physical communications infrastructure such as fiber connections between Crimea and mainland Ukraine, captured the peninsula's sole Internet exchange point, and jammed radio connections.[38] Russia carried out similar jamming in Eastern Ukraine, but for more tactical reasons: to hamper the use of information-gathering drones by the Organization for Security and Co-operation in Europe, the diplomatic forum for the West and the former Soviet Union.[39]

In addition to espionage, Russia has the capability to disrupt and deter Western activities, should open war break out. In October 2015, the United States detected Russian intelligence-gathering vessels and submarines operating near critical undersea data cables.[40] About the same time, U.S. officials became nervous over a Russian satellite that had veered extremely close to an Intelsat satellite that enabled Western cyber operations, prompting concern because Russia possesses traditional anti-satellite capabilities that can knock out or commandeer targeted satellites.[41]

Content and Communications

From a content and communications perspective, cyberspace is simply a medium to create, read, store, manipulate, delete, search, share, and transmit data. Examples of such data include operating instructions to industrial controllers, and government documents residing in network servers. But possessing control over such data can be powerful, including the capacity to sabotage infrastructure.

An illustration of Russian capabilities in the content and communications space came in August 2008. Three days before the launch of the war with Georgia, an explosion in Turkey ruptured the Baku-Tbilisi-Ceyhan oil pipeline and put it out of operation for almost three weeks. According to Western intelligence agencies, Russia triggered the explosion through a cyberattack that penetrated the pipeline's control systems.[42] In December 2014, Russian hackers reportedly damaged a German steel plant owned by ThyssenKrupp AG. The hackers penetrated the plant's control systems, specifically the shutdown mechanism in the blast furnace, leading to massive damage.[43] And in December 2015, a Russian hacker group identified

[38] Keir Giles, "Russia and Its Neighbours: Old Attitudes, New Capabilities," *Cyber War in Perspective: Russian Aggression against Ukraine,* Ed. Kenneth Geers, (NATO Cooperative Cyber Defence Centre of Excellence, 2015), pages 19-28; Piret Pernik, "Is All Quiet on the Cyber Front in the Ukrainian Crisis?" *International Centre for Defense and Security* (Estonia), March 7, 2014.

[39] Paul McLeary, "Russia's Winning the Electronic War," *Foreign Policy,* October 21, 2015. (http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/)

[40] David E. Sanger and Eric Schmitt, "Russian Ships Near Data Cables Are Too Close for U.S. Comfort," The New York Times, October 25, 2015. (http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html); Michael Pizzi, "Could Russia really cut the Internet?" AlJazeera America, October 26, 2015. (http://america.aljazeera.com/articles/2015/10/26/could-russia-really-cut-the-internet.html)

[41] Mike Gruss, "Russian Satellite Maneuvers, Silence Worry Intelsat," SpaceNews, October 9, 2015. (http://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/); Laurence Peter, "Russia shrugs off US anxiety over military satellite," BBC (UK), October 20, 2015. (http://www.bbc.com/news/world-europe-34581089); Sam Jones, "Satellite wars," Financial Times (UK), November 20, 2015. (http://www.ft.com/cms/s/2/637bf054-8e34-11e5-8be4-3506bf20cc2b.html)

[42] Jordan Robertson and Michael Riley, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era," *Bloomberg,* December 10, 2014. (http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar)

[43] Robert M. Lee, Michael J. Assante, and Tim Conway, "German Steel Mill Cyber Attack," *SANS Industrial Control Systems,* December 30, 2014. (https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf); Michael Riley and Jordan Robertson, "Cyberspace Becomes Second Front in Russia's Clash With NATO," *Bloomberg,* October 14, 2015. (http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato)

as the Sandworm Team was reportedly responsible for power blackouts in western Ukraine, the first publicly recorded electric outage blamed explicitly on a cyberattack.[44]

But these cyberattacks should have surprised no one, since experts, including the United States Computer Emergency Readiness Team, have long indicated such Russian capabilities.[45] In this new age, these and other active measures are the main battleground.

There are numerous examples of Russian cyber espionage. In October 2014, Russian hackers gained access to President Obama's unclassified email and schedules, according to a report in *The New York Times*.[46] Russian hackers penetrated State Department computers, remaining in the system for at least three months, as well as the Pentagon, including the Joint Chiefs' email system.[47] And in 2014 and 2015, hacker groups tied to the Russian government penetrated NATO, the Ukrainian government, the German parliament, and several other EU governments, according to news reports and private investigations.[48] An especially clever though ultimately unsuccessful operation took place in April 2015, when a Russian hacker group close to the Kremlin – Advanced Persistent Threat 28, or APT28 – was caught spying on Western discussions of the sanctions regime against Moscow. It did so by exploiting "zero days," then-unknown vulnerabilities in Microsoft Windows and Adobe Flash software. The infiltration was halted before any data was lost.[49]

[44] Pavel Polityuk, "Ukraine to probe suspected Russian cyber attack on grid," *Reuters,* December 31, 2015. (http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231); Robert M. Lee, "Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered," *SANS Industrial Control Systems Security Blog,* January 1, 2016. (https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered); John Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks," *iSIGHT Partners,* January 7, 2016. (http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/)

[45] U.S. Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team, "Ongoing Sophisticated Malware Campaign Compromising ICS," December 10, 2014. (https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B); Jack Cloherty and Pierre Thomas, "'Trojan Horse' Bug Lurking in Vital US Computers," *ABC,* November 6, 2014. (http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476)

[46] Michael S. Schmidt and David E. Sanger, "Russian Hackers Read Obama's Unclassified Emails, Officials Say," *The New York Times,* April 25, 2015. (http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html)

[47] Danny Yadron, "Three Months Later, State Department Hasn't Rooted Out Hackers," *The Wall Street Journal,* February 19, 2015. (http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453); Shane Harris, "Exclusive: Russian Hackers Target The Pentagon," *The Daily Beast,* July 18, 2015. (http://www.thedailybeast.com/articles/2015/07/18/russian-hackers-target-the-pentagon.html); Barbara Starr, "Official: Russia suspected in Joint Chiefs email server intrusion," *CNN,* August 7, 2015. (http://www.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/)

[48] Ellen Nakashima, "Russian hackers use 'zeroday' to hack NATO, Ukraine in cyber-spy campaign," *The Washington Post,* October 13, 2014. (https://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html); Stephen Ward, "iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign," *iSIGHT Partners,* October 14, 2014. (http://www.isightpartners.com/2014/10/cve-2014-4114/); Anton Troianovski, "German Parliament Struggles to Purge Hackers From Computer Network," *The Wall Street Journal,* June 12, 2015. (http://www.wsj.com/articles/german-parliament-struggles-to-purge-hackers-from-computer-network-1434127532); Sam Jones, "Russian government behind cyber attacks, says security group," *Financial Times* (UK), October 28, 2014. (http://www.ft.com/intl/cms/s/0/93108ba0-5ebe-11e4-a807-00144feabdc0.html#axzz3yH44O5XY)

[49] Alan Katz and Michael Riley, "Russian Hackers Use Zero-Days to Try to Get Sanctions Data," *Bloomberg,* April 18, 2015. (http://www.bloomberg.com/news/articles/2015-04-18/russian-hackers-use-zero-days-in-attempt-to-get-sanctions-data)

Socio-cultural

As discussed above, Russian military thinkers have raised the social-cultural aspect as the core of their vision of future war and military operations. Russia foresees information warfare as a way to mobilize all of Russian society, and thereby protect the state against internal and foreign enemies.[50]

Much of Russian media is concentrated either in state hands or those of parties close to the Kremlin.[51] Russia has introduced further controls through tight regulation.[52] A 2014 law limits foreign media ownership to a 20 percent stake, which has led many foreign media companies to abandon or restructure their Russian businesses, such as Germany's Axel Springer, publisher of *Forbes Russia,* and Finland's Sanoma Independent Media, former publisher of the English-language *Moscow Times.*[53]

In addition, Russia has introduced a new version of its surveillance technology called SORM, which intercepts and stores phone calls and Internet traffic. SORM provides state security services, particularly the domestic Federal Security Service, with backdoor access to local Internet services and social media platforms such as Vkontakte, the Russian Facebook alternative.[54] Facebook and Twitter are subject to traffic filtering at the network level; they are also compelled to store the data of Russian users in Russia, to provide it on the request of Russian authorities, and to block content if the Kremlin so desires.[55]

Moreover, Russia has introduced the equivalent of information troops – individuals typically known in the West as *trolls,* or Internet provocateurs, who flood social media and media Web pages with their "alternate" interpretation of the news. These actors' function is in part to muddy the ability of Western decision makers and their populations to separate fact from fiction, and thus hobble their capacity to respond effectively to Russian actions. But they also aim to intimidate those not sharing the "correct" narrative, and recruit sympathetic voices around the world, whether witting or unwitting.[56] A role in this is played by official media such as RT, Sputnik and Russia24, which target Russian speakers living in the other ex-Soviet states, Europe and the U.S.,[57] and potentially supportive western audiences.

Taken together, these tactics allow the Kremlin to effectively sequester the Russian-speaking audience

[50] Jolanta Darczewska, "The Devil Is in the Details: Information Warfare in the Light of Russia's Military Doctrine," *Ośrodek Studiów Wschodnich* (Poland), May 2015. (http://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf)
[51] Martin Russell, "Russian media – under state control," *European Parliamentary Research Service,* May 2015. (http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/559467/EPRS_ATA(2015)559467_EN.pdf)
[52] "2016 World Press Freedom Index," *Reporters without Borders,* 2016. (https://rsf.org/en/russia)
[53] Alec Luhn, "Russia tightens limit on foreign ownership of media," *The Guardian* (UK), September 26, 2014. (http://www.theguardian.com/world/2014/sep/26/russia-limit-foreign-ownership-media); Anastasia Bazenkova, "Foreign Publishers Quit Russia Over Media Ownership Law," *The Moscow Times* (Russia), September 9, 2015. (http://www.themoscowtimes.com/business/article/foreign-publishers-quit-russia-over-media-ownership-law/529645.html)
[54] Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal,* Fall 2013. (http://www.worldpolicy.org/journal/fall2013/Russia-surveillance)
[55] Kathrin Hille, "Twitter told to store Russian data in Russia," *Financial Times* (UK), November 10, 2015. (http://www.ft.com/intl/cms/s/0/e04e035c-87c6-11e5-90de-f44762bf9896.html#axzz3yH44O5XY)
[56] Alec Luhn, "Game of trolls: the hip digikids helping Putin's fight for online supremacy," *The Guardian* (UK), August 18, 2015. (http://www.theguardian.com/world/2015/aug/18/trolls-putin-russia-savchuk)
[57] "Vladimir Putin's global Orwellian campaign to undermine the West," *The Week,* May 9, 2015. (http://theweek.com/articles/553716/vladimir-putins-global-orwellian-campaign-undermine-west)

from Western mainstream media, creating an all-Kremlin information bubble, and thus both inoculating Putin from outside pressure, and strengthening his hand. Putin becomes answerable to no one.

An example of the impact is the Russian public reaction to the tragic July 14, 2014 flight of MH17. The Malaysia Airlines jet was shot down over Ukraine by a Russian-made BUK anti-aircraft system originating from the 53rd Brigade near the Russian city of Kursk, and all 298 passengers and crew were killed. By the time Western investigators concluded that Russian-backed separatists were probably responsible, intensive Kremlin-driven propaganda and Internet trolls had created a competing narrative: Kiev or the West, not the separatists, were behind the crash in yet another U.S.-led conspiracy to tarnish Russia. According to polls, the Russian public by-and-large accepted the Kremlin line.[58]

The Kremlin has also run Western tests of its capacity to create an alternative reality abroad.[59] In one case in September 2014, the St. Petersburg-based Internet Research Agency concocted a deadly chemical plant explosion in Louisiana. The group created a Wikipedia page about the supposed disaster, video clips of the aftermath, social media commentary from ostensible local victims, falsified news coverage, and even a message from jihadist terrorists claiming responsibility.[60] While the operation failed to gain traction and ignite panic, it demonstrated a will to operate on an insidious level designed – if and when the scriptwriters get good at it – to disrupt Western societies, in this case through stagecraft.

A few months earlier, the Russian hacking group APT28 penetrated and took over TV5, a French television channel, and masked it as a jihadist cyberattack. The attack took the globally broadcast television channel off the air for hours, during which the perpetrators posted ISIS-related updates on its social media accounts.[61] The hackers were identified, but had demonstrated their capabilities and European vulnerability to such attack.

Most recently, on January 16, 2016, Russian media and officials created public hysteria and a diplomatic fracas in Germany over the alleged rape of a 13-year-old Russian immigrant by a Middle East migrant. Inflamed by the reports, Russian-speaking migrants poured into the streets to protest the alleged attack, and Russian Foreign Minister Sergey Lavrov said the Germans must be covering something up, what specifically he did not say. In the end, it turned out that the girl, in a spat with her parents, had run off to the apartment of a 19-year-old German friend. There had been no rape.[62] But by then, the image of an out-of-control situation had already been exacerbated. With German opinion already deeply ambivalent over the inundation of Syrian migrants into the country, Chancellor Angela Merkel's already-waning public support plunged

[58] Alec Luhn, "Russia's Reality Trolls and the MH17 War of Misinformation," *Foreign Policy,* October 13, 2015. (http://foreignpolicy.com/2015/10/13/russias-reality-trolls-and-the-mh17-war-of-misinformation-buk-missile/); Eliot Higgins, "MH17 The Open Source Evidence," *Bellingcat,* October 8, 2015. (https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/)

[59] "Vladimir Putin's global Orwellian campaign to undermine the West," *The Week,* May 9, 2015. (http://theweek.com/articles/553716/vladimir-putins-global-orwellian-campaign-undermine-west)

[60] Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015. (http://www.nytimes.com/2015/06/07/magazine/the-agency.html)

[61] Aurelien Breeden and Alissa J. Rubin, "French Broadcaster TV5 Monde Recovers After Hacking," *The New York Times,* April 9, 2015. (http://www.nytimes.com/2015/04/10/world/europe/french-broadcaster-tv5-monde-recovers-after-hacking.html); Cale Guthrie Weissman, "France: Russian hackers posed as ISIS to hack a French TV broadcaster," *Business Insider,* June 11, 2015. (http://www.businessinsider.com/new-discovery-indicates-that-russian-hackers-apt28-are-behind-the-tv5-monde-hack-2015-6)

[62] Lucian Kim, "Russia having success in hybrid war against Germany," *Reuters,* February 7, 2016. (http://blogs.reuters.com/great-debate/2016/02/07/russia-having-success-in-hybrid-war-against-germany/)

further. Putin had furthered his objective of dividing Europe to, among other reasons, undermine solidarity on sanctions against Russia.

Other Components of Russia's Hybrid War with the West

Another aspect of Russia's hybrid war is a significant expansion of traditional espionage: In December 2014, a senior EU intelligence officer estimated that a full third of the Russian diplomats assigned to Brussels are members of Russian intelligence.[63] Just a month later, the FBI broke up a U.S.-based spy ring run by the SVR, the Russian foreign intelligence service.[64]

When it comes to Kremlin spy games, the return of active measures – which take espionage a step further into the attempt to shape, manipulate, and sabotage events – includes financial support for Marie Le Pen's Front National in France (a €40 million loan from First Czech Bank, linked to Gennady Timchenko, a Putin associate, in September 2014);[65] the bankrolling of anti-fracking protesters in Bulgaria, Lithuania, and Romania;[66] and backing for pro-Russian political parties in Belgium, Hungary (which was promised a $10 billion loan to finance a nuclear power plant expansion[67]), and the United Kingdom.[68]

These particular episodes are not different from traditional spycraft; active measures are a staple of the playbooks of all major intelligence agencies. For example, Russia has rattled Europe with the appearance of preparations for a military assault. In June 2014, Russia carried out a simulated attack on Denmark; and in 2014 and 2015, it penetrated the maritime and air space of Sweden and Finland.[69] Over the same two years, Russian planes buzzed a U.S. aircraft carrier and a destroyer in the Pacific and the Black Sea,[70] and on July 4, 2015, Russian strategic bombers flew close to Alaska and California.[71]

[63] Elisabeth Braw, "Russian Spies Return to Europe in 'New Cold War,'" *Newsweek,* December 10, 2014. (http://www.newsweek.com/2014/12/19/spies-are-back-espionage-booming-new-cold-war-290686.html)
[64] Adam Goldman, "FBI breaks up a Russian spy ring in New York City," *The Washington Post,* January 26, 2015. (https://www.washingtonpost.com/world/national-security/fbi-breaks-up-a-russian-spy-ring-in-new-york-city/2015/01/26/d3f8cee8-a595-11e4-a2b2-776095f393b2_story.html)
[65] Anton Shekhovtsov, "Russia and Front National: Following the Money," *Anton Shekhovtsov's Blog,* May 2, 2015. (http://anton-shekhovtsov.blogspot.com/2015/05/russia-and-front-national-following.html)
[66] Sam Jones, Guy Chazan, and Christian Oliver, "Nato claims Moscow funding antifracking groups," *Financial Times* (UK), June 19, 2014. (http://www.ft.com/intl/cms/s/0/20201c36-f7db-11e3-baf5-00144feabdc0.html#axzz3yH44O5XY); Keith Johnson, "Russia's Quiet War Against European Fracking," *Foreign Policy,* June 20, 2014. (http://foreignpolicy.com/2014/06/20/russias-quiet-war-against-european-fracking/)
[67] Krisztina Than, "Special Report: Inside Hungary's $10.8 billion nuclear deal with Russia," *Reuters,* March 30, 2015. (http://www.reuters.com/article/us-russia-europe-hungary-specialreport-idUSKBN0MQ0MP20150330)
[68] Andrew Higgins, "Far-Right Fever for a Europe Tied to Russia," *The New York Times,* May 20, 2014.(http://www.nytimes.com/2014/05/21/world/europe/europes-far-right-looks-to-russia-as-a-guiding-force.html); "The Russian Connection: The spread of pro-Russian policies on the European far right," *Political Capital Institute,* March 14, 2014. (http://www.riskandforecast.com/useruploads/files/pc_flash_report_russian_connection.pdf)
[69] Edward Lucas, "The Coming Storm: Baltic Sea Security Report," *Center for European Policy Analysis,* June 2015, pages 9-10. (http://www.cepa.org/sites/default/files/styles/medium/Baltic%20Sea%20Security%20Report-%20(2).compressed.pdf)
[70] Ryan Browne and Jim Sciutto, "Russian jets keep buzzing U.S. ships and planes. What can the U.S. do," *CNN,* April 19, 2016. (http://edition.cnn.com/2016/04/18/politics/russia-jets-buzz-u-s-ship-rules-of-engagement/)
[71] Laura SmithSpark,"Why Is Russia Sending Bombers close to U.S. Airspace?," *CNN,* July 27, 2015. (http://www.cnn.com/2015/07/27/world/us-russia-bombers-intentions/)

These are arguably probing operations, but Russia has been blunt as well: In the summer of 2015, the Russian ambassador to Sweden, Viktor Tatarintsev, relayed a Putin threat of unspecified military consequences should Sweden or Finland try to join NATO.[72] In March 2015, Russia's ambassador to Denmark, Mikhail Vanin, threatened to target Danish warships with nuclear weapons should Denmark join NATO's anti-ballistic missile defense system.[73] Around the same time, Russian officials threatened a nuclear strike should NATO use force in an attempt to reverse Moscow's absorption of Crimea.[74] And Russian air forces have simulated nuclear strikes against Poland and Sweden.[75]

The examples presented in this report exemplify the vigor and sophistication of Russian hybrid operations. Russia has developed its hybrid capabilities over a two-decade period and incorporated its evolving doctrine and capabilities into its strategic thinking. Its years of on-the-ground experience include increasingly complex examples of *maskirovka* and hybrid operations that, taken as a whole, give Russian hybrid warfare a stature all its own. Moscow appears to understand that it must continue to improve if it wants to compete and win.

Policy Recommendations

The West has entered a more turbulent era of aggressive competition with powers dedicated to overturning foundational aspects of post-World War II institutions and structures. Asymmetrical hybrid warfare tactics have enabled less-powerful players to punch above their weight, and sometimes seize the initiative.

The United States, the EU, and NATO possess the capacity to meet the challenge. The requirements include defensive measures to shield government, economic, and public infrastructure targets, and offensive methods to exact a high price from transgressors. Moreover, Russia's access to hybrid warfare instruments can be reduced, and its ability to field its existing hybrid weapons curtailed.

It is impossible from a practical perspective, and wasteful of resources, to attempt to counter every move by a Kremlin whose strategy includes tempting the West into needless and costly operations. Instead, the West should clearly identify crucial strategic and economic assets for possible targeting, while acting to undermine Russian capabilities.

A paramount objective should be persistent intelligence operations aimed at a continuing understanding of Russian goals, tactics, and means. The Kremlin should be denied access to crucial aspects of its tool kit. Finally, the West should turn to its own asymmetric tools and influence to counter and diminish the effectiveness of Moscow's strategy and deter Russian aggression.

Defensively, the U.S. and the EU should:

1. **Build up dedicated national and international coordinating centers for hybrid defense.** The U.S. and the EU should build up permanent local and supra-national coordinating centers, to be integrated within current agencies and organizations such as

[72] Jorge Benitez, "The Bully to the East," *U.S. News & World Report,* August 6, 2015. (http://www.usnews.com/opinion/blogs/world-report/2015/08/06/russia-bullies-sweden-and-finland-away-from-joining-nato)
[73] Anne Applebaum, "War in Europe is not a hysterical idea," *The Washington Post,* August 29, 2014. (https://www.washingtonpost.com/opinions/anne-applebaum-war-in-europe-is-not-a-hysterical-idea/2014/08/29/815f29d4-2f93-11e4-bb9b-997ae96fad33_story.html); Teis Jensen and Adrian Croft, "UPDATE 1-Russia threatens to aim nuclear missiles at Denmark ships if it joins NATO shield," *Reuters,* March 22, 2015. (http://www.reuters.com/article/denmark-russia-idUSL6N0WO0KX20150322)
[74] Umberto Bacchi, "Russia issues nuclear threat over Crimea and Baltic States," *International Business Times,* April 2, 2015. (http://www.ibtimes.co.uk/russia-issues-nuclear-threat-over-crimea-baltic-states-1494675)
[75] "Russia carried out practice nuclear strike against Sweden," *The Local* (Sweden), February 3, 2016. (http://www.thelocal.se/20160203/russia-did-practice-a-nuclear-strike-against-sweden)

NATO. These interagency centers should gather and analyze information on Russian hybrid activities, and propose defensive action and resilience against current and future threats.

2. **Build on existing measures to shore up energy resilience.** The U.S. and the EU should use the same new interagency centers to systematically probe for vulnerabilities in Western economic, governmental, and energy infrastructure, and recommend patches. They should:

   - Continue to develop more robust infrastructure to capitalize on vast new gas supplies coming onto the market from the U.S., the eastern Mediterranean, Africa, and elsewhere;
   - Continue to develop new technologies that can cushion the EU's reliance on Russian natural gas;
   - Elevate coordination among the U.S. Department of Energy, counterpart energy ministries, and private actors as a way to signal a concerted policy of reducing dependence on Russian gas; and
   - Continue to deny access to Western energy know-how, capital, and technology using export controls and sanctions.

3. **Tighten cyber- and information-security.** The U.S. and the EU should enhance a common defense against cyber-intrusion and information warfare, including military and civilian exercises and public-private partnerships. Western forces deployed to the Baltic republics and Eastern Europe should be equipped and trained to continue to operate even when lacking control of the information space or the electro-magnetic spectrum.

4. **Develop defensive economic warfare capabilities and alliances.** The U.S. and the EU should create tools to protect allies from Russian economic and financial warfare and influence. They should:

   - Form new trade, supply, and economic alliances with the specific aim of shielding the U.S. and EU from Russian economic and financial tactics;
   - Create information-sharing mechanisms on Russian threats, initiatives, and resources; and
   - Develop longer-term strategies to displace and undermine Russia economic weapons, to be coordinated with the U.S. Treasury and Commerce departments, NATO, and vulnerable non-NATO allies.

5. **Counter nuclear threats.** Clearly reiterate that the use of nuclear weapons against any allied member would lead to a proportional nuclear response from the United States. In addition, the U.S. and the EU should:

   - Enhance the enforcement of existing sanctions against illegal and suspected transfers and exchanges of technology, materiel, and personnel relevant to nuclear development.

Offensively, the U.S. and the EU should:

1. **Tighten and expand economic sanctions and financial measures.** The U.S. and the EU should maintain pressure on Russia to withdraw from eastern Ukraine and cease other hybrid attacks in Europe and the U.S., including cyber and information warfare. They should:

- Amplify the application of financial tools, enforcement measures, and sanctions against illicit Russian behavior. The focus should be on the underlying conduct to which sanctions are attached, such as the facilitation of transnational organized crime and money laundering, businesses that help to prop up the Russian state.

- Prioritize the identification of Russian hackers, organizations, and businesses engaged in or profiting from malicious cyber activity against key systems in the U.S. and the EU, in line with Executive Order 13694.

2. **Focus on anti-bribery and anti-corruption weapons.** The U.S. and the EU should step up the battle against state and non-state Russia corruption, which corrodes confidence in the government and leads to instability that Russia can exploit using hybrid tactics. Western authorities should:

- Coordinate targeted anti-corruption prosecutions, especially those tied to Russian influence;

- Ensure that Western investment and interests are observing international anti-bribery and anti-corruption practices; and

- Through sanctions, exclude actors involved or associated with Russian corruption from legitimate financial and commercial transactions.

3. **Explore strategic investment in areas where Russia seeks influence.** The U.S., EU, and other allies should incentivize, facilitate, and invest in sectors and markets in which Russian economic and financial influence challenges Western strategic interests. They should:

- Leverage international financial institutions (such as Overseas Private Investment Corporation in the United States) and development in an effort to displace Russian interests; and

- Incentivize the private sector to take advantage of market opportunities.

This report aims to contribute to an understanding of the threat posed by Russian hybrid warfare to U.S. and EU geostrategy and domestic security, and to propose recommendations on how to lessen the risk. It is the first of an envisioned three-part project on Russia under Putin during an age of sanctions and low oil prices. Much more time and work is required to continue to evaluate the new geopolitical challenges posed by a freshly assertive Russia, confronting Western influence and foundational institutions.

Bibliography

"2015 World Press Freedom Index." *Reporters without Borders,* 2015. https://index.rsf.org/#!/index-details/RUS.

Applebaum, Anne. Iron Curtain: *The Crushing of Eastern Europe,* 1944-1956. Doubleday, 2012.

– – – . "War in Europe Is Not a Hysterical Idea." *The Washington Post,* August 29, 2014. https://www.washingtonpost.com/opinions/anne-applebaum-war-in-europe-is-not-a-hysterical-idea/2014/08/29/815f29d4-2f93-11e4-bb9b-997ae96fad33_story.html.

Bacchi, Umberto. "Russia Issues Nuclear Threat over Crimea and Baltic States." *International Business Times,* April 2, 2015. http://www.ibtimes.co.uk/russia-issues-nuclear-threat-over-crimea-baltic-states-1494675.

Bazenkova, Anastasia. "Foreign Publishers Quit Russia Over Media Ownership Law." *The Moscow Times,* September 9, 2015. http://www.themoscowtimes.com/business/article/foreign-publishers-quit-russia-over-media-ownership-law/529645.html.

Benitez, Jorge. "The Bully to the East." *US News & World Report,* August 6, 2015. http://www.usnews.com/opinion/blogs/world-report/2015/08/06/russia-bullies-sweden-and-finland-away-from-joining-nato.

Bērziņš, Jānis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy." National Defence Academy of Latvia - Center for Security and Strategic Research, April 2014. http://www.sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf.

Braw, Elisabeth. "Russian Spies Return to Europe in 'New Cold War.'" *Newsweek,* December 10, 2014. http://www.newsweek.com/2014/12/19/spies-are-back-espionage-booming-new-cold-war-290686.html.

Breeden, Aurelien, and Alissa J. Rubin. "French Broadcaster TV5 Monde Recovers After Hacking." *The New York Times,* April 9, 2015. http://www.nytimes.com/2015/04/10/world/europe/french-broadcaster-tv5-monde-recovers-after-hacking.html.

Burke, Garance, and Jonathan Fahey. "AP Investigation: US Power Grid Vulnerable to Foreign Hacks." *AP,* December 21, 2015. http://bigstory.ap.org/urn:publicid:ap.org:19a230cf90024e46b13a0b2b50fc4c97 .

Cederberg, Aapo. "Future Challenges in Cyberspace." *Geneva Centre for Security Policy,* April 2015. http://www.gcsp.ch/News-Knowledge/Publications/Future-Challenges-in-Cyberspace.

Cederberg, Aapo, and Pasi Eronen. "How Are Societies Defended against Hybrid Threats?" *Geneva Centre for Security Policy,* September 2015. http://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats.

Chekinov, S. G., and S. A. Bogdanov. "The Nature and Content of a New-Generation War." *Military Thought,* no. 4 (October - December 2013): 12–23.

Chen, Adrian. "The Agency." *The New York Times Magazine,* June 2, 2015. http://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Clapper, James R. "Worldwide Threat Assessment of the US Intelligence Community." Office of the Director of National Intelligence (ODNI), February 26, 2015. http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

Cloherty, Jack, and Pierre Thomas. "'Trojan Horse' Bug Lurking in Vital US Computers." *ABC News,* November 6, 2014. http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.

Coker, Margaret, and Paul Sonne. "Ukraine: Cyberwar's Hottest Front." *The Wall Street Journal.* November 10, 2015. http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671.

Coskun, Orhan, and Humeyra Pamuk. "Russia Halts Work in Turkey's First Nuclear Power Plant after Spat - Officials." *Reuters,* December 9, 2015. http://www.reuters.com/article/mideast-crisis-turkey-russia-nuclear-idUSL8N13Y2WB20151209.

Darczewska, Jolanta. "The Devil Is in the Details: Information Warfare in the Light of Russia's Military Doctrine." *OSW | Centre for Eastern Studies,* May 2015. http://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf.

Dilanian, Ken. "Russian Spies Exposed in 2010 Were Succeeding, FBI Official Says." *Los Angeles Times,* October 31, 2011. http://articles.latimes.com/2011/oct/31/nation/la-na-russian-spies-20111101.

"'Disinformation Review' - New EU Information Product." *Delegation of the European Union to Ukraine,* November 4, 2015. http://eeas.europa.eu/delegations/ukraine/press_corner/all_news/news/2015/2016_11_04_1_en.htm.

Doff, Natasha, and Kateryna Choursina. "Ukraine Defaults on $3 Billion Bond to Russia." *Bloomberg Business,* December 18, 2015. http://www.bloomberg.com/news/articles/2015-12-18/ukraine-defaults-on-3-billion-russia-bond-as-court-battle-looms.

Elkus, Adam. "Moonlight Maze." In *A Fierce Domain: Conflict in Cyberspace,* 1986 to 2012, edited by Jason Healey and Karl Grindal, 152–63. Cyber Conflict Studies Association (CCSA), 2013.

Evans, Robert. "Moscow Signals Concern for Russians in Estonia." *Reuters,* March 19, 2014. http://www.reuters.com/article/us-russia-estonia-idUSBREA2I1J620140319.

Farchy, Jack, and Roman Olearchyk. "Moscow Votes to Suspend Free-Trade Zone with Ukraine." *Financial Times,* December 22, 2015. http://www.ft.com/intl/cms/s/0/d799d1a0-a8c8-11e5-9700-2b669a5aeb83.html.

FireEye. "HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group," July 2015. https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf.

F-Secure Labs. "The Dukes: Over 7 Years of Russian Cyberespionage," September 17, 2015. 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,* July 6, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

"Georgia on Their Minds." *The Wall Street Journal,* October 1, 2009. http://www.wsj.com/articles/SB10001424052748704471504574446582129281924.

Giles, Keir. "Russia and Its Neighbours: Old Attitudes, New Capabilities." In *Cyber War in Perspective: Russian Aggression against Ukraine,* edited by Kenneth Geers, 19–28. NATO Cooperative Cyber Defence Centre of Excellence, 2015.

– – – . "Western Media Must Get Creative in Infowar." *The Moscow Times,* August 4, 2015. http://www.themoscowtimes.com/opinion/article/western-media-must-get-creative-in-infowar/527000.html.

Giles, Keir, Philip Hanson, Roderic Lyne, James Nixey, James Sherr, and Andrew Wood. "The Russian Challenge." Chatham House, June 2015. http://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20150605RussianChallengeGilesHansonLyneNixeySherrWoodUpdate.pdf.

Giles, K., and W. Hagestad. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." In *Cyber Conflict (CyCon), 2013 5th International Conference on*, 1–17, 2013.

Goldman, Adam. "A Russian Banker in Manhattan Is Accused of Being an Agent for the Kremlin's Foreign Intelligence Service." *The Washington Post,* January 26, 2015. https://www.washingtonpost.com/world/national-security/fbi-breaks-up-a-russian-spy-ring-in-new-york-city/2015/01/26/d3f8cee8-a595-11e4-a2b2-776095f393b2_story.html.

Gruss, Mike. "Russian Satellite Maneuvers, Silence Worry Intelsat." *SpaceNews.com,* October 9, 2015. http://spacenews.com/russian-satellite-maneuvers-silence-worry-intelsat/.

Hagen, Andreas. "The Russo-Georgian War 2008." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* edited by Jason Healey and Karl Grindal, 194–204. Cyber Conflict Studies Association (CCSA), 2013.

Harris, Shane. "Exclusive: Russian Hackers Target The Pentagon." *The Daily Beast,* July 18, 2015. http://www.thedailybeast.com/articles/2015/07/18/russian-hackers-target-the-pentagon.html.

Higgins, Andrew. "Far-Right Fever for a Europe Tied to Russia." *The New York Times,* May 20, 2014. http://www.nytimes.com/2014/05/21/world/europe/europes-far-right-looks-to-russia-as-a-guiding-force.html.

Higgins, Eliot. "MH17 - The Open Source Evidence." *Bellingcat,* October 8, 2015. https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/.

Hille, Kathrin. "Twitter Told to Store Russian Data in Russia." *Financial Times,* November 10, 2015. http://www.ft.com/intl/cms/s/0/e04e035c-87c6-11e5-90de-f44762bf9896.html#axzz3u71ozG00.

Hill, Fiona. "Hybrid War: The Real Reason Fighting Stopped in Ukraine – for Now." *Reuters,* February 26, 2015. http://blogs.reuters.com/great-debate/2015/02/26/hybrid-war-the-real-reason-fighting-stopped-in-ukraine-for-now/.

Hoffman, Frank. "On Not-so-New Warfare: Political Warfare vs Hybrid Threats." *War on the Rocks,* July 28, 2014. http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Hultquist, John. "Sandworm Team and the Ukrainian Power Authority Attacks." *iSIGHT Partners,* January 7, 2016. http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/.

Jensen, Teis, and Adrian Croft. "Russia Threatens to Aim Nuclear Missiles at Denmark Ships If It Joins NATO Shield." *Reuters,* March 22, 2015. http://www.reuters.com/article/2015/03/22/us-denmark-russia-idUSKBN0MI0ML20150322.

Johnson, Keith. "Russia's Quiet War Against European Fracking." *Foreign Policy,* June 20, 2014. https://foreignpolicy.com/2014/06/20/russias-quiet-war-against-european-fracking/.

Jones, Sam. "Russian Government behind Cyber Attacks, Says Security Group." *Financial Times,* October 28, 2014. http://www.ft.com/cms/s/0/93108ba0-5ebe-11e4-a807-00144feabdc0.html.

– – – . "Satellite Wars." *Financial Times,* November 20, 2015. http://www.ft.com/cms/s/2/637bf054-8e34-11e5-8be4-3506bf20cc2b.html.

Jones, Sam, Guy Chazan, and Christian Oliver. "Nato Claims Moscow Funding Anti-Fracking Groups." *Financial Times*, June 19, 2014. http://www.ft.com/cms/s/0/20201c36-f7db-11e3-baf5-00144feabdc0.html.

Katz, Alan, and Michael Riley. "Russian Hackers Use Zero-Days to Try to Get Sanctions Data." *Bloomberg Business,* April 18, 2015. http://www.bloomberg.com/news/articles/2015-04-18/russian-hackers-use-zero-days-in-attempt-to-get-sanctions-data.

Kennedy, Will, and Andy Hoffman. "How Putin's Russia Gained Control of a U.S. Uranium Mine." *Bloomberg Business,* April 23, 2015. http://www.bloomberg.com/news/articles/2015-04-23/how-putin-s-russia-gained-control-of-a-u-s-uranium-mine.

Kramer, Andrew E. "Russia Expands Sanctions Against Turkey After Downing of Jet." *The New York Times,* December 30, 2015. http://www.nytimes.com/2015/12/31/world/europe/russia-putin-turkey-sanctions.html.

Krebs, Brian. Spam Nation: *The inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door.* Sourcebooks, Inc., 2014.

Lee, Robert M. "Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered." *SANS Industrial Control Systems Security Blog,* January 1, 2016. https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered.

Lee, Robert M., Michael J. Assante, and Tim Conway. "ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper – German Steel Mill Cyber Attack." SANS ICS, December 30, 2014. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

Lidz, Gogo. "'Polite People' of Russia: Not Who You Might Expect." Newsweek, April 11, 2015. http://europe.newsweek.com/polite-people-russia-321759.

Liik, Kadri. "The Limits and Necessity of Europe's Russia Sanctions." *European Council on Foreign Relations,* August 3, 2015. http://www.ecfr.eu/article/commentary_the_limits_and_necessity_of_europes_russia_sanctions3091.

Lovas, Gabriella, and Edith Balazs. "Hungary to Push on With Russian Nuclear Deal Chided by EU." *Bloomberg Business,* November 20, 2015. http://www.bloomberg.com/news/articles/2015-11-20/hungary-s-orban-presses-ahead-on-nuclear-deal-in-defiance-of-eu.

Lucas, Edward. "The Coming Storm - Baltic Sea Security Report." The Center for European Policy Analysis (CEPA), June 2015. http://www.cepa.org/sites/default/files/styles/medium/Baltic%20Sea%20Security%20Report-%20%282%29.compressed.pdf.

Luhn, Alec. "Game of Trolls: The Hip Digi-Kids Helping Putin's Fight for Online Supremacy." *The Guardian,* August 18, 2015. http://www.theguardian.com/world/2015/aug/18/trolls-putin-russia-savchuk.

– – – . "Russia's Reality Trolls and the MH17 War of Misinformation." *Foreign Policy,* October 13, 2015. http://foreignpolicy.com/2015/10/13/russias-reality-trolls-and-the-mh17-war-of-misinformation-buk-missile/.

– – – . "Russia Tightens Limit on Foreign Ownership of Media." *The Guardian,* September 26, 2014. http://www.theguardian.com/world/2014/sep/26/russia-limit-foreign-ownership-media.

MacFarquhar, Neil. "Russia and Turkey Hurl Insults as Feud Deepens." *The New York Times,* December 3, 2015. http://www.nytimes.com/2015/12/04/world/europe/putin-russia-turkey.html.

Matthews, Owen. "Russia's Greatest Weapon May Be Its Hackers." *Newsweek,* May 7, 2015. http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.

Mazarr, Michael J. *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* Advancing Strategic Thought Series. The Strategic Studies Institute, 2015.

McLeary, Paul. "Russia's Winning the Electronic War." *Foreign Policy,* October 21, 2015. https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/.

Melvin, Don, Michael Martinez, and Zeynep Bilginsoy. "Putin Calls Jet's Downing by Turkey 'Stab in the Back' - Turkey Says Warning Ignored." *CNN,* November 24, 2015. http://www.cnn.com/2015/11/24/middleeast/warplane-crashes-near-syria-turkey-border/index.html.

Murgia, Madhumita. "Could Cyberattack on Turkey Be a Russian Retaliation?" *The Telegraph,* December 18, 2015. http://www.telegraph.co.uk/technology/internet-security/12057478/Could-cyberattack-on-Turkey-be-a-Russian-retaliation.html.

Nakashima, Ellen. "Russian Hackers Use 'zero-Day' to Hack NATO, Ukraine in Cyber-Spy Campaign." *The Washington Post,* October 13, 2014. https://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html.

O'Brien, Kevin A. "The 'Quiet Option' in International Statecraft." In *Strategic Intelligence, Volume 3: Covert Action: Behind the Veils of Secret Foreign Policy,* edited by Loch K. Johnson, 27–60. Westport, CT: Praeger Security International, 2007.

"Ongoing Sophisticated Malware Campaign Compromising ICS (Update B) | ICS-CERT." ICS-CERT - *U.S. Department of Homeland Security,* December 10, 2014. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

Pernik, Piret. "Is All Quiet on the Cyber Front in the Ukrainian Crisis?" *ICDS - International Centre for Defense and Security,* March 7, 2014. http://www.icds.ee/blog/article/is-all-quiet-on-the-cyber-front-in-the-ukrainian-crisis/.

Peter, Laurence. "Russia Shrugs off US Anxiety over Military Satellite." *BBC News,* October 20, 2015. http://www.bbc.com/news/world-europe-34581089.

Pizzi, Michael. "Could Russia Really Cut the Internet?" *AlJazeera America,* October 26, 2015. http://america.aljazeera.com/articles/2015/10/26/could-russia-really-cut-the-internet.html.

Polityuk, Pavel. "Ukraine to Probe Suspected Russian Cyber Attack on Grid." *Reuters,* December 31, 2015. http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231.

Pomerantsev, Peter. "Brave New War." *The Atlantic,* December 29, 2015. http://www.theatlantic.com/international/archive/2015/12/war-2015-china-russia-isis/422085/.

Pomerantsev, Peter, and Michael Weiss. "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money." The Institute of Modern Russia, November 2014. http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf.

Rachman, Gideon. "Is Moscow behind the Bugging of Poland's Sikorski?" *Financial Times,* June 24, 2014. http://blogs.ft.com/the-world/2014/06/is-moscow-behind-the-bugging-of-polands-sikorski/.

Rácz, András. "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist." FIIA Report. The Finnish Institute of International Affairs, June 16, 2015. http://www.fiia.fi/assets/publications/FIIAReport43.pdf.

Riley, Michael, and Jordan Robertson. "Cyberspace Becomes Second Front in Russia's Clash With NATO." *Bloomberg Business,* October 14, 2015. http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato.

Robertson, Jordan, and Michael Riley. "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar Era." *Bloomberg Business,* December 10, 2014. http://www.bloomberg.com/news/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.html.

Russell, Martin. "At Glance: Russian Media – under State Control." EPRS | European Parliamentary Research Service, May 2015. http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/559467/EPRS_ATA(2015)559467_EN.pdf.

"Russia Accused of Disrupting New Energy Link between Sweden and Lithuania." *EurActiv,* May 4, 2015. http://www.euractiv.com/sections/global-europe/russia-accused-disrupting-new-energy-link-between-sweden-and-lithuania-314279.

Sanger, David E., and Steven Erlanger. "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government." *The New York Times,* March 8, 2014. http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.

Sanger, David E., and Eric Schmitt. "Russian Ships Near Data Cables Are Too Close for U.S. Comfort." *The New York Times,* October 25, 2015. http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html.

Schadlow, Nadia. "The Problem with Hybrid Warfare." *War on the Rocks,* April 2, 2015. http://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/.

Schmidt, Andreas. "The Estonian Cyberattacks." In *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012,* edited by Jason Healey and Karl Grindal, 174–93. Cyber Conflict Studies Association (CCSA), 2013.

Schmidt, Michael S., and David E. Sanger. "Russian Hackers Read Obama's Unclassified Emails, Officials Say." *The New York Times,* April 25, 2015. http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html.

Shekhovtsov, Anton. "Russia and Front National: Following the Money." *Anton Shekhovtsov's Blog,* May 2, 2015. http://anton-shekhovtsov.blogspot.com/2015/05/russia-and-front-national-following.html.

Slavin, Barbara, and Jason Healey. "Iran: How a Third Tier Cyber Power Can Still Threaten the United States." Atlantic Council - South Asia Center, July 2013. http://www.atlanticcouncil.org/images/publications/iran_third_tier_cyber_power.pdf.

Smolenova, Ivana. "Russia's Propaganda War." *Forbes,* March 25, 2015. http://www.forbes.com/sites/realspin/2015/03/25/russias-propaganda-war/.

Soldatkin, Vladimir. "Putin Names United States among Threats in New Russian Security Strategy." *Reuters,* January 2, 2016. http://www.reuters.com/article/russia-security-strategy-idUSKBN0UG09Q20160102.

Soldatov, Andrei, and Irina Borogan. "Russia's Surveillance State." *World Policy Journal,* fall 2013. http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

Starr, Barbara. "Official: Russia Eyed in Joint Chiefs Email Intrusion." *CNN,* August 5, 2015. http://www.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/index.html.

Stent, Angela. "Putin's Power Play in Syria." *Foreign Affairs,* December 14, 2015. https://www.foreignaffairs.com/articles/united-states/2015-12-14/putins-power-play-syria.

Stoll, Clifford. "Stalking the Wily Hacker." *Communications of the ACM* 31, no. 5 (May 1988): 484–500.

Teivainen, Aleksi, Arola Heikki, and Jyrki Iivonen. "Fennovoima's Project Nudged Forward." *Helsinki Times,* August 6, 2015. http://www.helsinkitimes.fi/business/13484-fennovoima-s-project-nudged-forward.html.

Than, Krisztina. "Special Report: Inside Hungary's $10.8 Billion Nuclear Deal with Russia." *Reuters,* March 30, 2015. http://www.reuters.com/article/us-russia-europe-hungary-specialreport-idUSKBN0MQ0MP20150330.

"The Department of Defense Cyber Strategy." The Department of Defense, April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

"The Russian Connection - The Spread of pro-Russian Policies on the European Far Right." Political Capital Institute, March 14, 2014. http://www.riskandforecast.com/useruploads/files/pc_flash_report_russian_connection.pdf.

The White House. "Presidential Policy Directive 20 - U.S. Cyber Operations Policy," October 16, 2012. http://fas.org/irp/offdocs/ppd/ppd-20.pdf.

Thomas, Timothy. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies* 27, no. 1 (2014): 101–30.

Troianovski, Anton. "German Parliament Struggles to Purge Hackers From Computer Network." *The Wall Street Journal.* June 12, 2015. http://www.wsj.com/articles/german-parliament-struggles-to-purge-hackers-from-computer-network-1434127532.

"Turkish Stream Pipeline Project a Go If Turkey Gets Guarantees from Brussels: Putin." *Hurriyet Daily News,* December 17, 2015. http://www.hurriyetdailynews.com/turkish-stream-pipeline-project-a-go-if-turkey-gets-guarantees-from-brussels-putin.aspx?pageID=238&nID=92664&NewsCatID=348.

"U.S. Government Asks Firms to Check Networks after 'Energetic Bear' Attacks." *Reuters,* July 2, 2014. http://www.reuters.com/article/2014/07/02/us-cybersecurity-energeticbear-idUSKBN0F722V20140702.

Ward, Stephen. "Sandworm Zero Day Vulnerability | iSIGHT Partners." *iSIGHT Partners,* October 14, 2014. http://www.isightpartners.com/2014/10/cve-2014-4114/.

Weedon, Jen. "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." In *Cyber War in Perspective: Russian Aggression against Ukraine,* edited by Kenneth Geers, 67–77. Tallinn, Estonia: NATO CCD COE Publications, 2015.

Weissman, Cale Guthrie. "France: Russian Hackers Posed as ISIS to Hack a French TV Broadcaster." *Business Insider.* Accessed December 12, 2015. http://uk.businessinsider.com/new-discovery-indicates-that-russian-hackers-apt28-are-behind-the-tv5-monde-hack-2015-6.

Wirtz, James J. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy." In *Cyber War in Perspective: Russian Aggression against Ukraine,* edited by Kenneth Geers, 29–37. Tallinn, Estonia: NATO CCD COE Publications, 2015.

Wolf, Martin. "Resist Russia's Blackmail over Ukraine's Debt." *Financial Times,* October 20, 2015. http://www.ft.com/intl/cms/s/0/5e295484-7647-11e5-a95a-27d368e1ddf7.html#axzz3uEN4ecZr.

Yadron, Danny. "Three Months Later, State Department Hasn't Rooted Out Hackers." *The Wall Street Journal.* February 20, 2015. http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453.

Zander, Christina. "Undersea Electricity Cable Generates Friction Between Russia and Baltics." *The Wall Street Journal.* May 6, 2015. http://www.wsj.com/articles/undersea-electricity-cable-generates-friction-between-russia-and-baltics-1430931797.

Герасимов, Валерий. "Новые вызовы требуют переосмысле- ния форм и способов ведения боевых действвий." *Военно-промышленный курьер,* March 5, 2013. http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf.

Acknowledgements

The author would like to thank Aapo Cederberg, William Courtney, Mark Dubowitz, Annie Fixler, Clifford Gaddy, Steve LeVine, Phillip Lohaus, Jeffrey Mankoff, David S. Maxwell, Aki Peritz, Matthew Rojansky, Peter A. Wilson, Juan Zarate, Boris Zilberman, the Center on Sanctions and Illicit Finance, and The Geneva Centre for Security Policy for their help and support. Furthermore, the author wishes to thank all the interviewees and sparring partners: Dmitri Alperovitch, James Dickey, Allan Friedman, Kenneth Geers, Keir Giles, Jussi Jaakonaho, Mikko Jakonen, Saara Jantunen, Jarno Niemelä, Klara Tothova Jordan, András Rácz, Samuel Visner, and the anonymous participants of several meetings, seminars and other gatherings for their valuable suggestions and insights.

Cover photo credits:
Left: (Reuters/Thomas Peter)
Center: (Shutterstock/Vicente Barcelo Varona)

About The Author

Pasi Eronen is the lead researcher for FDD's Russia project, where his work focuses on economic coercion, hybrid threats, and their nexus with cyber and information warfare.

His professional career includes a tour as an expert in the EU's European Police Mission in Afghanistan, and as a military officer with the Finnish Defense Forces in NATO's Kosovo Force.

Eronen has previously authored a report for the Finnish Ministry of Defense on the use of public-private partnerships in the development of national cyber defenses. He helped to develop Finland's Cyber Security Strategy while working for the Ministry of Defense. Eronen also has worked almost a decade in management consulting and serves on the advisory board of Sparta Consulting, a Finnish cyber security start-up.

Pasi earned a master's degree in Security Studies from Georgetown University and a master's degree in Computer Science from the University of Joensuu, Finland.

About the Foundation for Defense of Democracies

The Foundation for Defense of Democracies is a non-profit, non-partisan policy institute dedicated exclusively to promoting pluralism, defending democratic values, and fighting the ideologies that drive terrorism. Founded shortly after the attacks of 9/11, FDD combines policy research, democracy and counterterrorism education, strategic communications, and investigative journalism in support of its mission.

FDD focuses its efforts where opinions are formed and decisions are made, providing cutting-edge research, investigative journalism and public education - transforming ideas into action and policy.

FDD holds events throughout the year, including the Leading Thinkers series, briefings on Capitol Hill, expert roundtables for public officials, diplomats and military officers, book releases, and panel discussions and debates within the policy community.

About FDD's Center on Sanctions and Illicit Finance (CSIF)

The Foundation for Defense of Democracies' (FDD) Center on Sanctions and Illicit Finance (CSIF) expands upon FDD's success as a leading think tank on the use of financial and economic measures in national security. The Center's purpose is to provide policy and subject matter expertise in areas of illicit finance, financial power, and economic pressure to the global policy community.

CSIF seeks to illuminate the critical intersection between the full range of illicit finance and national security, including money laundering, terrorist financing, sanctions evasion, proliferation financing, cyber crime and economic espionage, and corruption and kleptocracy. This includes understanding how America can best use and preserve its financial and economic power to promote its interests and the integrity of the financial system. The Center also examines how America's adversaries may be leveraging economic tools and power.

CSIF focuses on global illicit finance, including the financing of terrorism, weapons and nuclear proliferation, corruption, and environmental crime. It has a particular emphasis on Iran, Saudi Arabia, Kuwait, Qatar, Turkey, Russia, and other autocratic states as well as drug cartels and terrorist groups including Hamas, Hezbollah, al-Qaeda, and the Islamic State.

For more information, please visit www.defenddemocracy.org.

FOUNDATION FOR
DEFENSE OF DEMOCRACIES

P.O. Box 33249
Washington, DC 20033-3249
(202) 207-0190
www.defenddemocracy.org