Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

William Chim, *Connections QJ* 17, no. 2 (2018): 5-17
https://doi.org/10.11610/Connections.17.2.01

Research Article

Russia's Digital Awakening

William Chim

Georgetown University, https://www.georgetown.edu/

Abstract: Since the fall of the Soviet Union, Russia has been unprecedented in its embrace of modern technology for the execution of its foreign policy and intelligence operation. This article examines Russia's relationship to the internet and computer technology, beginning with the early 1990s and detailing the growth of technology's popularity with the Russian public and Russian government up through 2017. Particular attention is paid to the skill with which Russia's illiberal political institutions and security services exploit the 'wild west' nature of the internet and the manipulable nature of modern technology and media, as well as how and why the West and U.S. failed to anticipate Russia's rise as a digital superpower and continue to fail to counter its dominance.

Keywords: Russia, cybersecurity, cyber warfare, intelligence, foreign policy, information operations, Eastern Europe.

A popular anecdote about modern Russia claims that the post-Cold War Russian Federation was until recently so backwards in its economic and technological development that few Russians understood anything about the internet or computers. This is likely an exaggerated claim which plays on comedic moments like then-President Dmitri Medvedev's visit to Twitter in 2010 during which he sent his awkward, first tweet and appeared charmingly lost around technology. The anecdote goes on to say that Russia did not figure out what a blog was until a few years ago, but now Russia has an enormous web presence and the Kremlin has weaponized the internet into an impressively powerful cyber tool. Within the last 20 years the Russian government expertly learned how to use technology and the internet in pursuit of its broader political goals. Russian cyber dominance is a direct result of its theatrical political culture and history, as well as its rich intelligence tradecraft in misdirection and deception. Russia's political culture is a perfect fit for the internet era and allows it the unique ability to deftly manipulate the potential of the internet more than other major cyber actors. The U.S. failed to see Russia's dominance coming and can learn much from an examination of Russia's cyber policy, including how to better counter Russia and develop a more cohesive cyber policy of its own.

To understand the centrality of cyber capabilities to Russian policy and government, one must first examine the development of its modern political culture and major cyber policy successes: implementation of early cyber operations abroad, blending of organized crime and hacktivist groups with state security, and Russia's overall aura of denial and deception concerning its cyber prowess. Outlining these major points elucidates why Russia has been very successful in transitioning into the internet age and how the United States can adapt and respond to Russian dominance.

Russia's adoption of the internet and technology as a key element of their political and military power projection was a foregone conclusion if one looks back to the rich history of Soviet intelligence and national security policy. Many Western pundits and analysts today focus heavily on what they deem as 'new' Russian 'hybrid warfare' capabilities which include a significant cyber component, in particular Russia's information operations within Ukraine and the United States during the last few years.[1] However, not only is there broad debate around the term 'hybrid warfare' (and it is just one of many similar concepts trying to pin down a complex phenomenon), but Russia's use of mixed political, military, economic, and information coercion tactics are not a new phenomenon – a critical missed point in many popular analyses.

The Soviet strategy of 'active measures' is the precursor to what is known today as hybrid warfare. The term refers to Soviet actions of political warfare used to influence the course of world events, including supporting communist and socialist opposition groups, revolutionary conflicts in other countries, terrorist and criminal groups, and general targeting of Western institutions. Former KGB Major General Oleg Kalugin referred to active measure as "the heart and soul of Soviet intelligence."[2] Active measures sought to conduct "subversion and measures to weaken the West, drive wedges in the Western community alliances, particularly NATO, to sow discord among allies, weaken the U.S., and prepare the ground in case war really occurs."[3] Former KGB informant Yuri Bezmenov estimated that in the 1970s, active measures comprised around 85 % of total KGB activities, yet the programs received far less attention and scrutiny

[1] Molly K. McKew, "The Gerasimov Doctrine," *Politico*, September/October 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

[2] Oleg Kalugin, "Inside the KGB: An Interview with Retired KGB Maj. Gen. Oleg Kalugin," *Cold War Experience*, *CNN*, January 1998, http://web.archive.org/web/20070627183623/ and http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin.

[3] Kalugin, "Inside the KGB."

from the international community compared to more popular conceptions of espionage and intelligence activity.[4] Active measures were about exploiting asymmetries in one's adversary – recognizing your state's inability to prevail in conventional conflict but identifying where a target had disproportionate weaknesses that could be exploited efficiently. For the Soviet Union, the openness of Western media, politics, and culture were a prime target for destabilization through disinformation and manipulation. This remains true today, except Russia has far more tools at its disposal to achieve the same ends.

With the history of Soviet active measures in mind, Russia's impressive transition into the internet age makes perfect sense and functions as a modernization of Soviet policy. The strategy of active measures translates cleanly into the digital age and such techniques are enhanced through the vast anonymity and manipulability of the internet. While active measures during the Soviet era constituted broad information operations, media manipulation, disinformation, counterfeiting, supporting insurgent or opposition political movements, etc., these campaigns required significantly more effort, time, and funding during the Cold War than in the 21st century. Russia quickly recognized that increasing globalization and interconnectivity of technology via the internet could facilitate the use of active measures as Russia sought to reestablish its presence in the world after the fall of the Soviet Union. Explicit articulations of this policy position by two of Putin's closest advisers since 1999 cemented Russia's tech-centric approach to projecting power and influence around the world.

While Russian active measures and hybrid warfare are not new phenomena, Russian officials Vladislav Surkov and Chief of the General Staff of the Armed Forces Valery Gerasimov of Russia are two individuals who helped make cyber capabilities a central part of the Kremlin's grand strategy. Gerasimov wrote an article in the Russian Academy of Military Science's *Military-Industrial Courier* in 2013 titled "The Value of Science in Prediction," in which he laid out the necessity to strengthen and evolve existing policy for the conflicts of the 21st century.[5] Gerasimov wrote, "In the 21st century we have seen a tendency toward the blurring the lines between the states of war and peace. Wars are no longer declared, and having begun, proceed according to an unfamiliar template."[6] Gerasimov proposed a ratio of non-military to military measures of 4 to 1, emphasizing political, economic, and social measures to shape the landscape of the target state through subversion, espionage, and propaganda in concert with cyberattacks.[7]

[4] Yuri Bezmenov and G. Edward Griffin, *Soviet Subversion of the Free World Press: A Conversation with Yuri Bezmenov, former propagandist for the KGB* (Westlake Village, CA: American Media, 1984), www.youtube.com/watch?v=RzKl6OF9yvM.

[5] Mary Ellen Connell and Ryan Evans, "Russia's 'Ambiguous Warfare' and Implications for the U.S. Marine Corps," Occasional Paper (Arlington, VA: Center for Naval Analyses, May 2015), 3, https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf, accessed May 18, 2018.

[6] Connell and Evans, "Russia's 'Ambiguous Warfare'."

[7] Connell and Evans, "Russia's 'Ambiguous Warfare'," 4.

The classic Soviet doctrine of *maskirovka*, focusing on denial and deception, is once again front and center in Gerasimov's writings in order to keep opponents wondering and hesitating through the denial of Russian involvement in ongoing operations.[8]

Similarly, top Putin aide Vladislav Surkov's major achievement is his masterful blending of politics and theater, arguably a core characteristic of the Putin era, as well as the development of his "sovereign democracy" ideology and the implementation of his policies in Chechnya and Ukraine, among others. Surkov was the main ideologist of the early 2000s Kremlin which articulated a Russian version of "guided democracy" in which a state calls itself democratic but in practice exhibits more authoritarian qualities.[9] Via "sovereign democracy" Surkov enabled the Kremlin to pursue its goals of consolidating rule by squashing civil society, free press, and liberalism under this illusion of democracy. He also developed modern Kremlin policies of co-opting, marginalizing, and manipulating political opponents wherein the Russian government did not shut down opposition media outlets but instead gained control of the entire media cycle and pushed opposition groups to the margins, effectively disarming them but maintaining plausible deniability.[10]

Surkov also articulated the Kremlin strategy for destabilization in Ukraine via tacit support for separatists in the Donbas region, something greatly facilitated by the manipulation of international media in a broad information campaign to sow confusion about the identities of rebel forces in the region.[11] Surkov combined the use of new technologies and the internet with traditional Russian forms of coercion and control – he in essence modernized Soviet-era political machinations for the 21st century.

While the work of these two men may not appear to have a direct hand in Russia's cyber presence, their contributions to Russian national security policy have actually played a critical role in Russia's dominant position today. Gerasimov was correct in identifying modern conflicts as no longer having concrete beginnings and ends, and this point has influenced Russia's involvement in the Ukraine conflict, its ongoing aggression toward the United States, and other political destabilization campaigns across Europe. Gerasimov and Surkov's fondness for misdirection and deception is central to Russia's cyberstrategy of causing widespread confusion about Russia's intentions and pervasive uncertainty about what is fact and fiction. Russia arguably succeeded more than any country

[8] Connell and Evans, "Russia's 'Ambiguous Warfare'."

[9] Julia Ioffe, "Kremlin Henchman: The Only Thing I Like About America is Tupac (And Sanctions Won't Keep Me from Listening)," *New Republic*, March 17, 2014, https://newrepublic.com/article/117053/vladislav-surkov-responds-sanctions-will-miss-tupac-shakur.

[10] Ioffe, "Kremlin Henchman: The Only Thing I Like About America is Tupac."

[11] Reid Standish, "Hacked: Putin Aide's Emails Detail Alleged Plot to Destabilize Ukraine," *Foreign Policy*, October 25, 2016, https://foreignpolicy.com/2016/10/25/ hacked-putin-aides-emails-detail-alleged-plot-to-destabilize-kiev-surkov-ukraine-leaks/.

at weaponizing the internet in a cost-effective and efficient manner. Surkov's "managed democracy" also allowed the Kremlin to reestablish centralized power and rule over Russia as well as the country's nascent internet presence, leading to Russia's infamous surveillance and communications interception program.

Russia's System for Operative-Investigative Activities (SORM) is the government's lawful system for private communications surveillance in Russia, launched by the Federal Security Service (FSB) in 1995. While the program on paper only allowed FSB access to communications data with a warrant, SORM required the installation of "black box" rerouting devices in every Internet Service Provider (ISP) which routed traffic through the FSB and in practice granted the agency total access to all communications regardless of legal procedure.[12] From a 2017 perspective, skeptics may balk at the idea that Russia's SORM is any worse than programs like China's *Great Firewall* or the U.S.'s infamous PRISM system, but analysts tracking SORM have described it as "PRISM on steroids" due to its increasingly-invasive evolutions since 1995.[13]

As of 2017, SORM-3 allows for the following: monitoring phone calls, email traffic, web browsing, IP addresses, all credit card transactions, monitoring all social networking sites and requiring them to install the black box tracking systems, user phone numbers, email addresses, and has the ability to perform deep packet inspection (DPI).[14] DPI ability is significant as it allows the reading of not just the metadata or header of information packets sent and received, but also the payload or content of the packets themselves.[15] As well, the law was quickly expanded upon inception to grant surveillance access to the Russian tax police, Kremlin/Duma/Presidential security guards, border patrol, and customs agents.[16] More recently, this year Putin finally moved to ban the use of proxies, virtual private networks (VPNs), and anonymous messaging apps in a further move to restrict dissent.[17]

It is easy to overlook SORM as one drop in the sea of Russian authoritarianism, but it is key to Russia's cyber presence and a significant Kremlin weapon for

[12] Jen Tracy, "New KGB Takes Internet by SORM," *Mother Jones,* February 4, 2000, http://www.motherjones.com/politics/2000/02/new-kgb-takes-internet-sorm/.

[13] Nick Shchetko, "Forget its Hotels, Sochi's Tech Has Been Up for the Olympic Challenge," *Ars Technica*, February 20, 2014, https://arstechnica.com/information-technology/2014/02/forget-its-hotels-sochis-tech-has-been-up-for-the-olympic-challenge/.

[14] Nathalie Marechal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," *Media and Communications* 5, no. 1 (2017): 29-41, 33.

[15] Marechal, "Networked Authoritarianism and the Geopolitics of Information."

[16] Tracy, "New KGB Takes Internet by SORM."

[17] Harriet Sinclair, "Putin Bans VPNs in Crackdown on Anonymous Internet Use in Russia," *Newsweek*, July 31, 2017, http://www.newsweek.com/putin-bans-vpns-crackdown-anonymous-internet-use-russia-644136.

disarming and targeting opposition leaders and enemies.[18] It is clear the Putin regime established control and dominance over the "Russian internet" and internal Russian connectivity and communications in the late 1990s and early 2000s. From there, as the government began to further understand how the internet could function as a force multiplier for Russian influence and power projection, the Kremlin began to experiment with using cyberattacks to destabilize its neighbors.

The era of rapid technological development of the 21st century, beginning with the advent of the internet, has always been rife with issues of attribution and anonymity. Security professionals have long grappled with the difficulty of attributing cyber intrusions and attacks and how to prove attribution and appropriately respond to them. However, within the last decade the world has become even more interconnected through the development of smart phones, social media, and the Internet of Things (IoT) as more personal devices become networked and part of the broader internet. Today is an era in which there is an overabundance of information available to anyone at any time. Humans created and stored more information and data in 2017 than in the previous 5,000 years of human history combined.[19]

The world today is one in which the average person accesses a staggering amount of information, news, and content on a daily basis and there are no substantial barriers to publishing on the internet. This is a double-edged sword – the internet has allowed unprecedented advancement in areas of education, research and development, and social connection among people around the world. Those who strive to make the internet a free and fair marketplace of ideas have proliferated accessible, truthful information so others may learn and grow. However, due to the unrestricted nature of the internet and the proliferation of social media and anonymity, there are also many with nefarious intentions who seek to flood the cyber marketplace of ideas with deliberate disinformation to intentionally make the truth both difficult to determine, and ultimately meaningless. One can certainly argue that the objective fact and truth have to some degree lost their power as the foundation of society as the internet has developed into a figurative hall of mirrors where information is distorted and it becomes near impossible to determine objective fact. Denial and disinformation are two key consequences of information proliferation, both of which have been weaponized by the Russian Federation.

Russia first tested out its cyber capabilities in cyberattack campaigns in Estonia in 2007 and since then has incorporated other aspects of traditional Kremlin control into its cyber measures, such as private industry and Russian organized

[18] Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal* September 12, 2013, www.worldpolicy.org/journal/fall2013/Russia-surveillance.

[19] Richard Harris, "More Data Will Be Created in 2017 than the Previous 5,000 Years of Humanity," *App Developer Magazine,* December 23, 2016, https://appdevelopermagazine.com/4773/2016/12/23/more-data-will-be-created-in-2017-than-the-previous-5,000-years-of-humanity-/.

crime. Organized Russian distributed denial of service attacks (DDoS) against Estonia's government and civic infrastructure were the first large-scale coordinated use of cyber capabilities by Russia to affect a strategic goal in an adjacent state, supposedly in response to a diplomatic spat over the relocation of a statue of a Soviet soldier in Tallinn.[20] The Estonia attacks were a coming-out party for Russia's cyber capabilities and succeeded in taking down Estonian websites and other technical infrastructure for over a month, a significant attack for a country that prides itself on being technologically advanced and having an essentially paperless government.[21] The attackers, which included organized crime and private hacking groups, used botnets worldwide inflicting DDoS attacks to overwhelm Estonian servers, including servers of governmental organizations, banks, political parties, and most news media websites. In the real world, the Russian government applauded and encouraged the hackers but denied any involvement in the attacks themselves.[22]

While the Estonia attacks appeared to accomplish little in terms of concrete gain for Russia, they were crucial in demonstrating the value of simple, widespread cyberattacks, especially when used alongside other economic and political coercion. While NATO created the Cooperative Cyber Defense Centre for Excellence in Tallinn after the attacks, the tolerable international response and Russia's ability to deny and deflect accusations of involvement surely emboldened the Kremlin to wield cyberattacks more. Russia would go on to combine cyber operations with kinetic military operations in the 2008 Georgian War, the first combined cyber-military conflict of its kind, and continue to use destabilizing cyberattacks in Ukraine starting in 2014. Russia's ability to feign innocence while combining state security and criminal hackers in their operations has been key to their success.

The U.S. Intelligence Community's 2015 Worldwide Threat Assessment concluded that Russia and china are the "most sophisticated nation-state actors" in cyberwarfare and that Russian hackers "lead in terms of sophistication, programming power, and inventiveness" – an assessment that holds true today.[23] Putin's Russia appears to have put substantial effort into developing cadres of state hackers, often co-opted from the ranks of the criminal underground. FireEye cyber threat analyst Jonathan Wrolstad concluded Russia has had a "symbiotic relationship" with organized cybercrime syndicates for "at least 10 years, if not longer," developing a quid pro quo where pending criminal cases against hackers

[20] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," Occasional Paper (Arlington, VA: Center for Naval Analyses, March 2017), 13, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

[21] Connell and Vogler, "Russia's Approach to Cyber Warfare," 13.

[22] Connell and Vogler, "Russia's Approach to Cyber Warfare," 14.

[23] Owen Matthews, "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.

mysteriously disappear in return for assistance to the security services.[24] The Kremlin receives expert hacking teams, as well as "the best pieces of malware," and importantly maintains plausible deniability from the activities of co-opted groups.[25] This practice again goes hand in hand with traditional Russian and Soviet active measures and smokescreens designed to knock adversaries off balance and create confusion and discord.

Furthermore, Russia's ability to co-opt private business and industry into its web of security services has also proven to be an effective tactic for extending its cyber reach globally. No case better demonstrates this than that of Kaspersky Labs, the Russian cybersecurity and antivirus company popularly used around the world and long suspected of having ties to Russian security and intelligence agencies. While there was a time in which Kaspersky was a respected name in personal cybersecurity and its antivirus products have been used by hundreds of millions the world over, including U.S. government agencies, questions about its relationship to the Russian government, willing or otherwise, have bubbled up over recent years. The company has always dismissed such inquiry as dubious and absurd, but in a country where SORM and the FSB essentially monitor and control the entirety of the Russian internet, it certainly is not out of consideration. Those scrutinizing Kaspersky's operations were rewarded in 2017 when leaked emails and details of hacks involving Kaspersky revealed a close-knit relationship with FSB, with Kaspersky directly developing security technology for the agency and working on joint projects.[26] The relationship was further revealed by a high-profile hack of a U.S. National Security Agency contractor's personal computer upon which he improperly stored classified NSA documents – the NSA discovered that the contractor has Kaspersky software on his PC which played an active role in scanning for classified U.S. files and transmitted them to either Russian hackers (government affiliated or otherwise) or directly to Russian intelligence.[27]

One can estimate that the Russian government has had a long and fruitful relationship with Kaspersky as a technically overt tool for spying on Russian adversaries – but it is safe to say that relationship may be coming to an end as Kaspersky's reputation is now crashing and the U.S. government has banned its use. Kaspersky is now suing the U.S. government over the ban, a lawsuit that

[24] Cory Bennett, "Kremlin's Ties to Russian Cyber Gangs Sow US Concerns," *The Hill*, October 11, 2015, http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns.

[25] Bennett, "Kremlin's Ties to Russian Cyber Gangs Sow US Concerns."

[26] Jordan Robertson and Michael Riley, "Kaspersky Lab Has Been Working With Russian Intelligence," *Bloomberg Businessweek*, July 11, 2017, accessed May 28, 2018, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence.

[27] Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *New York Times*, October 10, 2017, www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

itself could be considered a continuance of Russian operations as it will likely entangle the U.S. (at least to an extent) in an annoying legal battle to prove Kaspersky's duplicity.[28] The point still stands – Russia has proven itself adept at finding creative ways to insert Kremlin influence in all facets of Russian cyberspace in pursuit of its policy and intelligence goals around the world. Russia's digital journey arguably culminated in the creation of the "Internet Research Agency" and the destabilization of the United States political system.

A New York Times article from June 2015 titled "The Agency" gave a prescient look into Russia's "troll factories" and disinformation campaigns long before such operations achieved worldwide notoriety in 2016. The article, one of the first major published pieces to reveal Russia's cyber information operations, detailed what is known as the Kremlin's "Internet Research Agency," an organization based out of a nondescript office complex in St. Petersburg with several hundred employees tasked with waging "information war" – spreading disparate and false narratives about a multitude of political and social issues around the world to blur the line between truth and falsehood for the benefit of the Kremlin.[29] The article clearly describes what is the precursor to Russia's information operations in the U.S. in 2016 but fails to make the connection between the phenomenon of government-funded disinformation campaigns and how vulnerable the United States was and is to such a strategy on a grand level. "The Agency" article is reflective of the attitudes and perspectives of the American government and public back in 2015 – capturing so much detail about this dangerous phenomenon but falling short of understanding why Russia is doing this and what its full potential is. One can draw a straight line from the operations described in the article to the Kremlin campaign to destabilize the 2016 U.S. election, which gave Putin a staggering return for a reported cost of under $500,000.[30] Even two years later, "The Agency" article feels dated and naïve after recent world events. It remains a perfect example of the lack of imagination of the U.S. concerning cyber capabilities and demonstrates some of the qualities that allowed Russian leadership and intelligence to evolve so quickly in cyberspace.

Russia's cyber development from the late 1990s to today shows a consistent pattern of skillful adaptation to the changing realities of the world and a clear adjustment of traditional Soviet intelligence strategy and tradecraft to new technology. One can make a clear argument that Russia's ascent to cyber proliferation and dominance is owed in large part to the unique qualities of Russia's his-

[28] Dustin Volz and Jim Finkle, "Kaspersky Lab Asks Court to Overturn U.S. Government Software Ban," *Reuters*, December 18, 2017, https://www.reuters.com/article/us-usa-cyber-kasperskylab/kaspersky-lab-asks-court-to-overturn-u-s-government-software-ban-idUSKBN1EC2CK.

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

[30] Greg Miller, Greg Jaffe, and Philip Rucker, "Doubting the intelligence, Trump Pursues Putin and Leaves a Russian Threat Unchecked," *The Denver Post*, December 14, 2017, https://www.denverpost.com/2017/12/14/trump-pursues-putin.

torical, cultural, and political character. Russia, albeit initially slow to recognize the possibilities of the internet and 21st century technology, eventually made cyber a crucial part of its national security and foreign policy strategy in a way that even China and the United States have not done. The major exploitation of cyber as a tool for power projection and foreign interference is arguably most possible in states with an authoritarian nature such as Russia, which acted quickly in the late 1990s and early 2000s to re-centralize power in the hands of Putin and the Kremlin and curbed media and internet freedom in such a way that greatly empowered the state security services and government. The Russian state, despite the vocal proclamations of Vladimir Putin and others in Russia's leadership, is arguably amoral at its core, which allows it to fully exploit the political and disruptive potential of the internet and modern technology without grappling with the moral and ethical quandaries inherent in such technology.

Russia also benefits from the very nature of the global tech industry – Silicon Valley and other tech hubs continue to fail to recognize that the platforms and applications they develop have the potential to be wielded unethically to cause political and economic chaos, a failure in perspective which greatly benefits groups and states like Russia. Again, it is not just a failure to predict how hostile states and non-state groups could commandeer social media, journalism, and cyber infrastructure to destabilize entire states, but Silicon Valley's lack of a moral conscience and deliberate refusal to engage with the reality that technology is not ethically neutral. For a state like Russia whose government is unconcerned with such considerations in the pursuit of realpolitik-based international power goals, the shortsightedness of American and Western tech companies is one of the greatest boons to Russia and other such states. Only after the events of the 2016 U.S. election is American society beginning to grapple with these questions and asking how technology affects and shapes American democracy and society.[31]

Finally, Russia also skillfully adapted to the internet age because its culture of anonymity, duplicity, and distortion is perfectly suited to Russia's rich history of deception and confusion at the heart of its political culture. A core characteristic of the Soviet Union's active measures strategy was to create mass confusion and uncertainty about Russia's global activities, policy positions and goals, and disorient popular perceptions of other states and create broad political and economic destabilization. The nature of 21st century technology and the internet acts as a powerful force multiplier for these purposes. One should not give Russia too much credit – it is unlikely that Russia actually predicted this future and specifically planned for a reality in which the global population is inundated with information and disinformation and simple, cheap information operations could be surprisingly effective in achieving major policy goals. However, it certainly was not difficult to predict such a future, as authors such as Aldous Huxley in 1932's

[31] Irina Raicu, "Rethinking Ethics Training in Silicon Valley," *The Atlantic*, May 26, 2017, https://www.theatlantic.com/technology/archive/2017/05/rethinking-ethics-training-in-silicon-valley/525456/.

Brave New World anticipated a dystopian future in which "the truth is drowned in a sea of irrelevance," rather than the information-deprived society of George Orwell's *1984*.[32] Huxley himself later remarked in his follow-up essay *Brave New World Revisited* in 1958 that, "The development of a vast mass communications industry, concerned in the main neither with the true nor the false, but with the unreal, the more or less totally irrelevant. In a word, they failed to take into account man's almost infinite appetite for distractions."[33] It is neither difficult nor unrealistic to see how much society today resembles this predicted future and how states like Russia have exploited to an almost unfathomable degree the deluge of information and noise that individuals encounter daily. Hague Center for Strategic Studies Fellow Alexander Klimburg described cyberspace today as "like Europe in 1914, before World War I – governments are like sleepwalkers, they do not comprehend the power of new technology and consequences of misunderstanding each other's activities."[34] This is a reality that will not soon change – Russia's cyber supremacy acknowledges and embraces that. What remains to be seen is how the United States and Russia's neighbors will respond to this challenge.

U.S. cyber intelligence in the 21st century must acknowledge a number of realities to adapt to the ever-changing present and develop effective policy and response to countries like Russia. The U.S. Intelligence Community (USIC) must take seriously the vulnerabilities inherent in consumer technology all over the world – Russia already demonstrated the immense chaotic power of social media, and Silicon Valley has been slow to take the issue seriously and genuinely address the ways in which its products can be abused by malicious actors. It is difficult to claim that the USIC should have a hand in the entirety of the private tech industry, but more cooperation is needed with the U.S. government to ensure events like the 2016 election interference do not happen again. Some analysts argue the old adage "the best defense is a good offense" is key here, that the U.S. must put its offensive cybercapabilities front and center.[35] This is to some degree misguided – while it would be foolish to argue that offense should not be a focus of U.S. cyberpolicy, the experiences of the Russian government's cyberattacks (and those of other states and groups) show that cyberwar of the present and future targets political, economic, and social infrastructure of countries through their weak defenses and cultural qualities of transparency and free exchange. These are the parts of American society most requiring a robust cyber defense. Certainly, the U.S. must protect concrete infrastructure, borders, and

[32] Neil Postman, *Amusing Ourselves to Death* (Upper Saddle River, NJ: Pearson Education, 2007), xix.

[33] Aldous Huxley, *Brave New World Revisited* (New York: RosettaBooks, 2000), 31.

[34] Matthews, "Russia's Greatest Weapon May Be Its Hackers."

[35] Gillian Rich, "As Russia Hacks, Is the Best Cyber Defense a Terrifying Cyber Offense?" *Investor's Business Daily*, December 19, 2016, https://www.investors.com/news/preventing-cyberattacks-is-the-best-defense-an-almighty-offense/.

possess strong kinetic deterrents, but as 2016 demonstrated, manipulating information and public perception can be more effective than bullets and bombs.

However, like with most things relating to modern Russia and its current resurgence, there is a timer on Russia's cyber dominance of which the Kremlin must be wary. Russia today has a number of serious political, economic, and demographic issues that will play a significant factor in the state's ability to wield power even in the case of cost-effective cyberattacks and relationships with criminal hacking groups. There is significant danger in working with non-state actors and groups that lack the experience and temperament of government and military officials – any mistakes by hacking groups could quickly and dangerously escalate into a situation beyond the Kremlin's control.[36] The Kremlin also risks getting "in too deep" with criminal groups that it may not be able to control. Putin succeeded wildly in redefining Russian political and cultural identity around his vision of nationalism and conservatism, which drew in cadres of "patriotic hackers" more than willing to contribute to Russia's resurgence – patriotic Russians contributed to the botnets which targeted Georgia in 2008. But nationalism will not likely be enough to continue bonding private hackers to the Russian state in the long-term – Russia's negative economic outlook due to its overreliance on oil and gas and the country's aging population and continuing brain drain may eventually deprive the Kremlin of its elite criminal hackers.[37] Especially as hacking becomes a more globalized and widespread criminal phenomenon and with the advent of cryptocurrencies, Russian hackers may eventually not need Kremlin backing in order to launder their ill-gotten funds and many will likely move outside Russia's borders and beyond the reach of Kremlin coercion.[38]

Russia's cyber goliath appears to be an insurmountable challenge, and while in 2017 Russia was at a high point of cyber dominance, there will be an inevitable decline. Russia's supremacy is not sustainable, both due to its internal economic, political, and demographic issues, and to the fact that the world is taking notice now and countries like the U.S. and China are ramping up their cyber strategies and preparedness. However, the Kremlin too likely understands that its preeminence may be temporary, and for this reason policymakers and intelligence officers should expect Russia to wield its formidable power with a degree of brazen impulsivity while it still can and especially as the Putin regime begins to decline. Though any number of factors could also influence the timeline and allow Russia more time on top. The fact that the world should have seen earlier remains – the internet and globalized technology as they exist today are the perfect tools for

[36] Cyberreason Intel Team, "Russia and Nation-State Hacking Tactics: A Report from Cyberreason Intelligence Group," *Cyberreason.com*, June 5, 2017, https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity.

[37] Cyberreason Intel Team, "Russia and Nation-State Hacking Tactics."

[38] John Leyden, "Russia is struggling to keep its cybercrime groups on a tight leash," *The Register*, June 6, 2017, https://www.theregister.co.uk/2017/06/06/russia_cyber_militia_analysis/.

modern Russia and its long mastery of duplicity and distraction. Recognizing that Russia has outplayed the world and understanding how and why are the first steps to stopping the Kremlin.

About the Author

William Chim is a current M.A. student in the Security Studies Program at Georgetown University's Walsh School of Foreign Service and holds a B.A. from the University of Pennsylvania. He specializes in Russian political and foreign policy analysis, as well as intelligence studies. His other academic interests include Balkans area studies and ethics in national security and intelligence. He has previously worked at the U.S. Department of State and interned at the U.S. National Defense University's College of International Security Affairs.
E-mail: wm.a.chim@gmail.com.

Bibliography

Bennett, Cory, "Kremlin's Ties to Russian Cyber Gangs Sow US Concerns," *The Hill*, October 11, 2015, https://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns.

Bezmenov, Yuri, and Edward G. Griffin, *Soviet Subversion of the Free World Press: A Conversation with Yuri Bezmenov, Former Propagandist for the KGB*. Westlake Village, CA: American Media, 1984, https://www.youtube.com/watch?v=RzKl6OF9yvM.

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

Connell, Mary Ellen, and Ryan Evans, "Russia's 'Ambiguous Warfare' and Implications for the U.S. Marine Corps," *Occasional Paper*. Arlington, VA: Center for Naval Analyses, 2015, https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf.

Connell, Michael, and Sarah Vogler, "Russia's Approach to Cyber Warfare," *Occasional Paper*, 2017. Arlington, VA: Center for Naval Analyses, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Cyberreason Intel Team, "Russia and Nation-State Hacking Tactics: A Report from Cyberreason Intelligence Group," *Cyberreason.com*, June 5, 2017, https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity.

Harris, Richard, "More Data Will Be Created in 2017 than the Previous 5,000 Years of Humanity," *App Developer Magazine*, December 23, 2016, https://appdevelopermagazine.com/4773/2016/12/23/more-data-will-be-created-in-2017-than-the-previous-5,000-years-of-humanity-/.

Huxley, Aldous, *Brave New World Revisited*. New York: RosettaBooks, 2000.

Ioffe, Julia, "Kremlin Henchman: The Only Thing I Like About America is Tupac (And Sanctions Won't Keep Me from Listening)," *New Republic*, 2014, https://newrepublic.com/article/117053/vladislav-surkov-responds-sanctions-will-miss-tupac-shakur.

Kalugin, Oleg, "Inside the KGB: An Interview with Retired KGB Maj. Gen. Oleg Kalugin," *Cold War Experience, CNN*, 1998, http://web.archive.org/.

Leyden, John, "Russia is struggling to keep its cybercrime groups on a tight leash," *The Register*, June 6, 2017, https://www.theregister.co.uk/2017/06/06/russia_cyber_militia_analysis/.

Marechal, Nathalie, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," *Media and Communications* 5, no. 1 (2017): 29-41.

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

McKew, Molly K., "The Gerasimov Doctrine," Politico (September/October 2017), https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

Miller, Greg, Greg Jaffe, and Philip Rucker, "Doubting the intelligence, Trump Pursues Putin and Leaves a Russian Threat Unchecked," *The Denver Post*, December 14, 2017, https://www.denverpost.com/2017/12/14/trump-pursues-putin.

Perlroth, Nicole, and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *The New York Times*, October 10, 2017, https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

Postman, Neil, *Amusing Ourselves to Death*. Upper Saddle River, NJ: Pearson Education, 2007.

Raicu, Irina, "Rethinking Ethics Training in Silicon Valley," *The Atlantic*, May 26 2017, https://www.theatlantic.com/technology/archive/2017/05/rethinking-ethics-training-in-silicon-valley/525456.

Rich, Gillian, "As Russia Hacks, Is the Best Cyber Defense a Terrifying Cyber Offense?" *Investor's Business Daily*, December 19, 2016, www.investors.com/news/preventing-cyberattacks-is-the-best-defense-an-almighty-offense/.

Robertson, Jordan, and Michael Riley, "Kaspersky Lab Has Been Working with Russian Intelligence," *Bloomberg Businessweek*, July 11, 2017, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence.

Shchetko, Nick, "Forget its Hotels, Sochi's Tech Has Been Up for the Olympic Challenge," *Ars Technica*, February 20, 2014, https://arstechnica.com/information-technology/2014/02/forget-its-hotels-sochis-tech-has-been-up-for-the-olympic-challenge/.

Sinclair, Harriet, "Putin Bans VPNs in Crackdown on Anonymous Internet Use in Russia," *Newsweek*, July 31, 2017, https://www.newsweek.com/putin-bans-vpns-crackdown-anonymous-internet-use-russia-644136.

Soldatov, Andrei, and Irina Borogan, "Russia's Surveillance State," *World Policy Journal*, September 12, 2013, https://worldpolicy.org/2013/09/12/russias-surveillance-state/.

Standish, Reid, "Hacked: Putin Aide's Emails Detail Alleged Plot to Destabilize Ukraine," *Foreign Policy* (October 2016), https://foreignpolicy.com/2016/10/25/hacked-putin-aides-emails-detail-alleged-plot-to-destabilize-kiev-surkov-ukraine-leaks/.

Tracy, Jen, "New KGB Takes Internet by SORM," *Mother Jones*, 2000, https://www.motherjones.com/politics/2000/02/new-kgb-takes-internet-sorm/.

Volz, Dustin, and Jim Finkle, "Kaspersky Lab Asks Court to Overturn U.S. Government Software Ban," *Reuters*, December 18, 2017, https://www.reuters.com/article/us-usa-cyber-kasperskylab/kaspersky-lab-asks-court-to-overturn-u-s-government-software-ban-idUSKBN1EC2CK.