Russian Cyber Information Warfare
International Distribution and Domestic Control

Lev Topor, PhD, and Alexander Tabachnik, PhD

Abstract: Cyber information warfare (IW) is a double-edged sword. States use IW to shape the hearts and minds of foreign societies and policy makers. However, states are also prone to foreign influence through IW. This assumption applies mainly to liberal democratic societies. The question examined in this article is how Russia uses IW on other countries but protects itself from the same activities. The authors' main argument is that while Russia executes influence operations and IW in cyberspace, it strives for uncompromising control over its domestic cyberspace, thus restricting undesirable informational influence over its population.

Keywords: cyber warfare, information warfare, IW, Russia, cyber policy, sharp power

Introduction

Cyber information warfare (IW) is a double-edged sword. On the one hand, states can use IW to shape the mindset of foreign societies and policy makers. On the other hand, states are also prone to foreign influence through IW. This applies mainly to liberal democratic societies such as the United States, Britain, and most of Western Europe. Russia is a distinct case in this regard as it is a nondemocratic state that uses *sharp power*—it takes advantage of the asymmetry between open and democratic political systems and restricted nondemocratic political systems.[1] In an open society, freedom of speech and freedom of the press can facilitate disinformation and misinforma-

Dr. Lev Topor is a senior research fellow at the Center for Cyber, Law and Policy, University of Haifa, Israel. Dr. Alexander Tabachnik is also a senior research fellow at the Center for Cyber, Law and Policy.

Journal of Advanced Military Studies vol. 12, no. 1
Spring 2021
www.usmcu.edu/mcupress
https://doi.org/10.21140/mcuj.20211201005

tion while restricted political systems where speech and press are limited can restrict intervention through IW.[2]

The question examined in this article is how Russia uses IW on other countries in the international arena but protects itself from it. The article's argument is that while Russia executes influence operations and IW using cyberspace, it strives for uncompromising control over its domestic cyberspace, thus restricting undesirable informational influence over its population. Moreover, as Daria Litvinova suggests, Russia not only restricts its media and communication systems but, simultaneously, manipulates these systems for political control. The vast majority of Russian citizens consume state-sponsored media and news that promote pro-Kremlin narratives.[3]

As discovered in the case of the Russian intervention in the Scandinavian, East-Central European, and Baltic states since 2017, Russia's bots and trolls are very effective in negatively impacting Western democracies. Russia undermines the democratic nature of its adversaries, dividing their societies between competing groups—supporters of the right and supporters of the left, liberals and conservatives, and even racial divisions. In fact, any social rift can be used to divide and incite. Therefore, divisions created or amplified harm the governance of Russia's adversaries. In Russia's domestic arena, however, legislation is used strategically to ensure domestic obedience. For instance, the Yarovaya Law, which was enacted in 2016 alongside other laws and policies regarding its sovereign internet, allows Russia to restrict the flow of undesirable information. Moscow is obligated to supervise information even at the expense of the civil right for privacy, growing criticism from its domestic telecommunication companies, from other information technology (IT) giants, and despite substantial economic and reputational losses.

From Soviet Hard Power to Russian Sophisticated Information Warfare

The dissolution of the Soviet Union occurred on 26 December 1991. The Cold War ended with an ideational and material collapse as the Soviet Union could not compete with American and Western progress, mainly in economic and technological areas. Furthermore, the Soviet authorities failed to establish a unifying ideology as each ethnic group had different national narratives, needs, and privileges.[4] The military and economic power of the United States, along with its appealing competing ideology, slowly influenced the Soviet people and mainly the Soviet elite.[5] Though there are numerous explanations for the collapse of the Soviet Union, it is unquestionable that the American and Western combination of hard power and soft power superiority pushed the Soviet Union to its limit.[6] Ernest J. Wilson III and Joseph S. Nye Jr. regard this combination of power types as smart power. *Smart power* is the capability to combine hard

and soft power in an effective way to amplify one's influence on others.[7] The Soviet Union did employ soft power such as economic pressure and propaganda, mainly on less developed countries but could not compete with Western diplomacy and economic power. Indeed, the Soviet Union mainly leaned on hard power for its international affairs and policies.[8]

Russia now makes use of sharp power with cyber influence operations and hybrid warfare.[9] In the last two decades, Russia emerged again and began to recover. In the twenty-first century, instead of fighting hard power with hard power, Russia uses smart power and information warfare to achieve its strategic objectives.[10] Since the end of the Cold War, a state of uncertainty was generated regarding American and Russian relations. The Cold War was over but struggle and competition for global primacy remained.

In Western terms, Russia employed *hybrid warfare*, which, as Timothy McCulloh and Richard Johnson define, is the generation of an uncertain situation between adversaries where it is unclear whether a state of war exists, and it is unclear who is a combatant and who is not.[11] Indeed, Russia used hybrid strategies and tactics in some cases, as in the case of Eastern Ukraine and Crimea. For example, it wielded irregular fighters, proxy fighters, and information and psychological warfare along with economic and diplomatic pressure to justify its actions.[12]

However, IW is not just a part of hybrid warfare, but it is a stand-alone strategy to promote policies and strategies to pressure one's adversary without the use of brute force. These strategies and tactics are not new and were frequently used by the Soviet Union. The Soviet, or Russian, term for IW is *active measures*—covert and overt techniques to influence events and behaviors of foreign countries. In these cases, information was manipulated and promoted by Soviet-supporting front organizations, agents of influence such as local politicians or even spies, by fake stories, and forgeries in non-Soviet media outlets.[13]

In the twenty-first century, for instance, the U.S. Global Engagement Center (GEC) issued a report in August 2020, stating that Russia has created a sophisticated "ecosystem" of propaganda outlets via official and unofficial channels like news agencies, websites, or social media bots and trolls. The actual impact of this ecosystem is yet to be clear as measuring information, influence, and reach is complex and inaccurate. Yet, this ecosystem does create a certain amount of debate, hostility among parties, and instability within the targeted state.[14] As it seems, the Russian ecosystem is an iteration of Soviet disinformation campaigns, in particular Soviet active measures.

Moreover, Russia uses IW as a complementary power to fit alongside other types of power. In a document issued by the Russian Federation Council titled "The Concept of the Cyber Security Strategy of the Russian Federation," Russia has emphasized the importance of cyber warfare, information and communica-

tion technologies (ICT), and use of cyber-related actions to accommodate and complement other types of acts in the international arena such as hard or soft power.[15] However, Russian security officials do not use the term cyber warfare. Instead, they conceptualize cyber warfare within the broader framework of information warfare and perceive it as a holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations.[16]

Traditionally, international actors sought control over resources, actions, and certain events and outcomes.[17] However, Russia does not always seek physical control. Through an efficient use of IW, it spreads domestic chaos for its adversaries—a form of psychological control.[18] Misinformation and disinformation is a tool used by the Soviets, but Russia has frequently deployed them again, especially with the proliferation of the internet and social media—it is another sophisticated tool in its international relations toolbox.[19] The 2016 U.S. presidential elections and the chaos that followed exemplify this point.[20] The Russian IW strategy uses ICT platforms to undermine, manipulate, and mislead the information people consume as it believes this can advance its political and military objectives. Further, information warfare can disorganize governance and governments. It can "reeducate" certain groups and societies with a specifically designed curriculum that will yield Russia's desired outcomes in the future. It is also important to mention that in order to control global events, Russia does not rely solely on new media and social networks but also on more traditional media such as television and print media.[21]

Russian Cyber IW: Methods of Strategic International Distribution

The Russian IW in the Baltic, Scandinavian, and East-Central European states serves as a very significant and insightful lesson and helps explain how IW operations are designed and executed and how they are a continuation of Soviet active measures. As this article suggests, Russia's use of sharp power exposes the systematic asymmetry between its restricted cyber domain and the openly free cyber domain of its adversaries. To understand why Russia is spreading disinformation in the above-mentioned region, it is important to understand why the region is of strategic significance to Russia. The Baltic, Scandinavian, and East-Central European regions consist of Denmark, Sweden, Norway, Finland, Germany, Poland, Estonia, Lithuania, Latvia, and Russia. It is Russia's geopolitical backyard and some of its members are ex-Soviet states. Since 1994, Estonia, Latvia, and Lithuania joined the Partnership for Peace program and became North Atlantic Treaty Organization (NATO) members as well as European Union (EU) members in 2004. From that moment on, Russia sought more influence in the region in order to resist Western military and economic influ-

ence. NATO's growing power in the Baltic and Scandinavian region had effectively created a security dilemma for Russia—it had no choice but to resist.[22]

Most of the Baltic and Scandinavian states are NATO members apart from Sweden and Finland. Thus, learning from past mistakes, Russia chose to protect its backyard not with hard power, as the Soviet Union had once done, but with a smart use of IW power. In case Sweden and Finland were to join NATO, it could deter Russia from engaging in conflicts and seeking more influence in the region, as an attack on the alliance could trigger NATO's article 5, meaning that an attack on any ally is considered an attack on all allies. In such a scenario, Russia risks engaging in a conventional war with all NATO allies on its Western border and a potential direct conflict with the United States, if not worse.[23]

Moreover, as Richard D. Hooker Jr. argues, Russia has strengthened itself and its borders in Georgia (2008) and Ukraine (2014) with a calculated risk between annexation, international escalation, and Russia's least favorite option of letting Georgia or Ukraine get even closer to the West—indeed, after Russia's actions, the Georgian attempt to join NATO halted and the pro-European movement in Ukraine faded away to some extent.[24] The next point of conflict will probably be in the Baltic or Scandinavian region where, on the one hand, Russia will pressure NATO members to reduce their activities with the alliance, while, on the other hand, pressure nonmember states such as Sweden and Finland to reject alliance membership. Russia seeks to keep the status quo of isolating Estonia, Latvia, and Lithuania from the rest of NATO by sabotaging Western efforts to bring Sweden and Finland into NATO.[25] To keep Sweden and Finland away, Russia knows it must win their hearts and minds. Rather than creating a zero-sum game, Moscow attempts to win the information war—to persuade the Swedish and the Finnish citizens into pressuring their policy makers, via elections, out of any future NATO cooperation and agreement. Thus, a successful disinformation campaign can effectively undermine Western presence and NATO's power, or perception of power, by its members.[26] In fact, Russia's strategic concept is simple but effective; instead of resisting the West and NATO as an entire bloc, head-to-head, it uses the technique of divide et impera, spreading disinformation in each of its adversaries to divide them.

In January 2017, the Swedish Institute of International Affairs accused Russia of spreading disinformation and misinformation as part of a coordinated IW campaign to influence public opinion and decision making in Sweden. As Anders Thornberg, former head of Sweden's security service, the SÄPO, argued in January 2018, Russia tried to spread chaos in Swedish society before the September 2018 elections to prevent a unanimous decision of joining NATO.[27] In Finland, Russia had spread disinformation about the European migration problem to promote nationalism, xenophobia, Islamophobia, and divide the left and right political spectrums.[28] In another example, Russia promoted social

media bots and trolls and created a smear campaign against Finnish journalists and researchers who educated the public about the Russian misinformation campaigns. Another more prominent example is the "Lisa case" in Germany. To spread xenophobia in Europe in general—Sweden and Finland in particular as well as in Germany—Russia backed a false news story claiming a German-Russian girl was raped by Arab migrants.[29] Further, Russia promoted misleading information to make the Finnish and the Swedes fear Westerners—not just migrants from other cultures. It has spread a false rumor that NATO soldiers could potentially rape Swedish women without fear of prosecution as they are immune from it due to their NATO service.[30] It had also spread a debate on whether NATO would stockpile nuclear weapons on Swedish and Finnish soil in secret places due to its proximity with Russia, if they should join NATO.[31]

In general, recent Russian IW tactics include disinformation and misinformation, use of bots and trolls in social media and in other websites, and the "authentication" of forged information by assigning them to allegedly legitimate news agencies that cover such stories. Russian state-sponsored news agencies include RT and Sputnik. Ahead of the 2020 election in the United States, Daniel Ray Coats, former director of U.S. national intelligence, highlighted the Russian cyber-IW threat:

> We assess that Russia poses a cyber espionage, influence and attack threat to the United States and our allies. Moscow continues to be a highly capable and effective adversary, integrating cyber espionage, attack and influence operations to achieve its political and military objectives. Moscow is now staging cyber-attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat—an issue discussed in the Online Influence Operations and Election Interference section of this report.[32]

Liberal democracies are worried since some cyber warfare tactics such as espionage, propaganda, and data manipulation are not illegal in the current state of affairs between states. Though each state has or can have laws and regulations, they cannot compel other states. There is no applicable law regarding cyber warfare. According to the 2017 revision of the *Tallinn Manual on the International Law Applicable to Cyber Operations*, which is only a proposal for cyber warfare for international laws, the previously mentioned cyber tactics are not illegal. That is, misinformation and disinformation and espionage for the purpose of misinformation and/or disinformation is legal. Moreover, cyber warfare attacks in general can be treated as kinetic attacks and retaliation can be justified only if the victim can prove who initiated the attack, with full forensic

details.[33] This cyber forensic process is currently very problematic due to the use of privacy and anonymity tools as well as the use of proxy players. Further, punishment against cyber warfare is not practiced and deterrence is slow, blunt, and ineffective.[34] Russia and every international player for that matter can spread disinformation freely. Retaliation may come, but it would not be justified by international law and could further escalate the conflict into kinetic means. As Yochai Benkler, Robert Faris, and Hal Roberts argue, a fundamental technological change occurred with the rapid development of social media and other forms of communication in recent years that created echo chambers, which in turn reinforced people's internal biases, removed their indicia of trustworthiness and, in general, overwhelmed the world.[35]

Further, in February 2020, Federal Bureau of Investigation (FBI) Director Christopher A. Wray said that Russia was engaged in IW attempts to influence the 2020 presidential elections, as it did in 2016 as well. Russia relies on a covert social media campaign aimed at dividing American public opinion and sowing discord, just as it had made in the Baltic, Scandinavian, and East-Central European states. Russia promotes fictional personas, bots, trolls, social media postings, and disinformation. These attempts raise the question of how democracies should resist. Interestingly, Wray had no positive answer, stating that the First Amendment restricts authorities from monitoring disinformation.[36]

Interestingly, Moscow's bots and trolls can spread chaos without the fear of prosecution. Russia spreads chaos and disorder in the United States, in potential NATO members, and in the rest of Europe while risking no legal retaliation. It wins by undermining the democratic nature of its adversaries, spreading chaos in their societies. A probable measure for countering this is more regulation—but if the United States, Sweden, or Finland regulate online activities, they will also harm independent parties and voices—an essential part of democracy, as these efforts would risk mistaking legitimate narrative campaigns for Russian IW.[37]

Russian Domestic Control: Resisting Foreign Influence and Domestic Antigovernment Activists

Russian authorities perceive cyberspace not only as an opportunity to manage IW against the West but also as a major threat to Russian national security, stability, and regime legitimacy as the free flow of information in cyberspace could undermine the regime and promote the so-called "colour revolution"—a term used to describe nonviolent protests and uprisings in autocracies and former Soviet states.[38] To execute IW operations without the fear of becoming the victim of IW operations itself, Russian authorities have strived to secure and protect the Russian information domain from foreign influence. In the 2000s, Russian

authorities established control (direct and indirect) over the major television channels and newspapers, while in the 2010s most of the established internet mass media (e.g., major online newspapers) have been effectively censored to limit criticism of the regime.[39] Still, social networks, online video platforms, secure messengers, and foreign-based internet mass media remain a great concern as Moscow has no control over information on these platforms. Cyberspace remains a domain only partly controlled by the authorities, enabling a relatively free flow of information. Therefore, to prevent possible Western efforts to destabilize Russia (as perceived by the Russian leadership) through IW in cyberspace, Moscow has taken the necessary precautions.[40]

Consequently, Russian authorities, through legislation and cyber regulation, strive to control Russian cyberspace to prevent or deter, as much as possible, the dissemination of information that may mar the positive representation of Vladimir Putin's regime, or any activity that may endanger the regime's stability.[41] Therefore, Russian authorities seek to take control over the content of the information circulating in Russian cyberspace. This is exemplified by our qualitative analysis—we use process tracing, legislation review, and analysis to exemplify and prove our findings and arguments.[42]

The authors analyzed actions and legislation taken by the Russian government since 2014 to gain more power and control over cyberspace. Since 2014 and the Russian intervention in Ukraine, the struggle between Russia and the West has intensified, specifically in the cyber domain. The authors have reviewed major official sources containing the previously mentioned legislation: the official internet portal of legal information of the Russian Federation, which contains all legislative acts and amendments accepted in Russia; official data considering legislative activities of the State Duma (the lower house of the Federal Assembly of the Russian Federation) provided by the Duma; and the official site of the president of Russia, which provides detailed information regarding the legislation approved by the president.[43] Furthermore, the authors reviewed legislation that has attracted significant attention by civil society, human rights organizations (Russian and international), and businesses, due to the potential of the laws to violate basic human rights. Finally, the authors reviewed operational expenses necessary for the legislation's implementation, which range from freedom of speech restrictions to data retention procedures. Eventually, the authors took into consideration only the most significant and prominent legislative acts and their amendments, which have had real (nonsymbolic) impacts on Russian society, and in fact have been implemented by the Russian authorities.

Generally, the most prominent Russian legislation directed at control over domestic cyberspace could be separated into the two major categories, which are also interconnected and represent one holistic perspective of information operations (offensive and defensive). This article defines these two categories

as legal-technological and legal-psychological, which considers their impact on Russia's cyberspace and population and aligns with Russia's vision of offensive cyber operations. Also, in Russian IW campaigns, digital-technological and cognitive-psychological components are interconnected.[44]

Through appropriate regulation, Russia's authorities strive to establish control over Russia's cyberspace from the informational-technological perspective. At the same time, through the appropriate legislation, Russia's authorities strive to discourage its own population from undesirable activity in cyberspace (sharing information, writing undesirable posts, articles etc.), which from the authorities' perspective may endanger the stability of the regime—this is the psychological element.

The most prominent recent legal-technological efforts by Russian authorities consist of the following measures: the Yarovaya law; Russia's "sovereign internet" law; the mandatory installation of SORM (System of Operational-Investigatory Measures); and a law that makes Russian applications mandatory on smartphones, computers, etc.[45] This legislation (with the exception of SORM's mandatory installation, which for the first time was accepted in its current form in the 2000s) has been accepted in the last several years.[46] At the same time, the legal-psychological efforts consist of the three major measures: the "disrespect law" (18 March 2019); the "fake news" law (18 March 2019); and the new "foreign agent" law (2 December 2019).The Yarovaya law, passed in 2016, requires the provision of encryption/decryption keys on request by distributors of information such as internet and telecom companies, messengers, email services, forums, and other platforms that allow the exchange information to Russian special services such as the Federal Security Service (FSB). The encryption/decryption keys are necessary for decoding received, transmitted, delivered and/or processed electronic messages and information.[47] Moreover, according to this law, big data attributed to activity in Russian's cyberspace must be stored in Russian territory, while the special services should have unrestricted access to this data.[48] In practice, this law allows Russian special services to access private and corporate information circulating in the Russian segment of cyberspace. For example, companies like Facebook or Google must store information concerning data and activities of their Russian users in Russian territory and provide unrestricted access to the Russian special services. At the same time, the Yarovaya law is implemented only partially due to the technological difficulties and unwillingness to further aggravate the deteriorated relations with the Western countries and the Western technological companies.[49]

Furthermore, the Decree of the Government of the Russian Federation from 13 April 2005 (number 214) with changes from 13 October 2008 regarding SORM requires telecommunication operators to install equipment provided by the FSB. This allows the FSB and other security services to monitor

unilaterally, without a warrant, users' communications metadata and content. This includes web browsing activity, emails, phone calls, messages, social media platforms, and so on. Moreover, the system has the capability of deep packet inspection—a filtering inspection point that filters transmitted data and weeds out noncompliant or unwanted material like spam, viruses or, in the context of this case, unwanted content and foreign websites. Thus, SORM is one of the major tools helping implement and regulate the Yarovaya law.[50]

Additionally, on 1 May 2019, President Putin signed and approved Russia's sovereign internet law, which allows the Russian internet to become independent and operate as an intranet, a stand-alone network outside of the World Wide Web. In practice, it allows Russia to operate an intranet, a restricted regional network such as what is used by large corporations or militaries. This network gives authorities the capacity to deny access to parts of the internet in Russia, potentially ranging from cutting access to particular internet service providers (ISPs) to cutting all internet access in Russia.[51]

Furthermore, on 2 December 2019, Russian president Putin signed a legislative bill requiring all computers, smartphones, and smart devices sold in Russia to be preinstalled with Russian software.[52] Later, the government announced a list of applications developed in Russia that would need to be installed on the above-mentioned categories of devices. This legislation was signed by President Putin on 8 December 2020, although its implementation and enforcement is delayed due to the COVID-19 global pandemic. In the near future, devices will be issued with government-issued serial numbers.[53] This will allow Moscow to tighten control over end users through regulation, monitoring, and surveillance. At the end of 2020, Russia's authorities continue preparations (including the legal and technological) for implementation of this legislation.

At the same time, the recent legal-psychological efforts consist of three major laws, as mentioned earlier, directed at prevention of distribution of facts and critiques directed at the government's activities and officials. For example, the law that regulates "disrespect" allows courts to fine and imprison people for online disrespect of the government, of Russian officials, of Russian human dignity, and public morality as the Russian Federation reserves the right to instruct citizens about proper public dignity and morality.[54] This law is very obscure—it allows the authorities the opportunity to interpret it as they wish. However, it is designed to prevent dissemination of information through informational-telecommunication networks only.[55]

An additional recent fake news law also outlaws the dissemination of what the government deems to be misinformative or misleading—any information undesirable by the government can be defined as "fake news."[56] Roskomnadzor (Federal Service for Supervision of Communications, Information Technology, and Mass Media), responsible for the Kremlin's censorship, is empowered by

the law to notify the editorial body (or author) of the online publication that certain information must be removed from its website.[57] Moreover, the law prescribes heavy fines for knowingly spreading mis/disinformation and forces ISPs to deny access to websites disseminating it in the pretrial order following the appropriate decisions issued by the Roskomnadzor.[58]

The recent foreign agent law applies to any individual who distributes information on the internet and is funded by foreign sources. Interestingly, YouTube channels can be also defined as such.[59] According to this law, Russian citizens and foreigners can be defined as foreign agents. Consequently, all materials (including posts in social media) published by individuals who receive funds from non-Russian sources must be labeled as foreign agents.[60] A commission of the Ministry of Justice and the Ministry of Foreign Affairs have the power to recognize individuals as foreign agents. Therefore, foreign agents will be obliged to create a legal entity and tag messages with a special mark. Furthermore, individual foreign agents are subject to the same requirements as nonprofit organizations recognized as foreign agents (the law regarding nonprofit organizations was adopted in 2012). According to the law, foreign agents will be obliged to provide data on expenditures and audits regarding their activities to the Ministry of Justice.[61] It should be noted that these administrative obligations are time consuming, complicated, and expensive—they are aimed at discouraging so-called foreign agents from their activities. Apparently, this legislation is directed against antigovernment activists, vloggers, bloggers, independent journalists, independent politicians, and human-rights activists.[62] Overall, the purpose of the legal-psychological efforts is to discourage the population from participation in any kind of anti-government activities in cyberspace.

At the same time, the disrespect law, fake news law, and the new foreign agent law are implemented to discriminate against particular individuals, organizations, and sporadically in indiscriminate manner against the general population to intimidate people and discourage them from critiquing the regime.[63]

Therefore, it can be argued that Russian IW outside its borders is inextricably linked with the authorities' efforts to control Russian domestic cyberspace, and together they constitute one holistic framework of information security. This enables Russia to achieve tactical superiority over the openly pluralistic democratic West, as Russia can be considered a nondemocratic country with the previously mentioned legislation as well as other oppressive laws. Russia conducts IW against Western countries and organizations, while it limits the potential of possible Western IW operations in Russian cyberspace.

Conclusion: Russia Has the Upper Hand

The question examined in this article is how Russia employs information warfare on other players in the international arena but protects itself from IW. The au-

thors' main argument is that while Russia executes influence operations and IW using cyberspace, it strives for uncompromising control over its domestic cyberspace. Russia restricts potential Western and undesirable domestic informational influence over its population. As discovered though the case studies of Russian intervention in the Scandinavian, Baltic, and East-Central European states, Moscow's bots and trolls affect Western democracies by effectively disrupting their democratic institutions. Russia undermines the democratic nature of its adversaries, dividing their societies between different ethnic groups and political persuasions, thus harming their governance. The targeted states are very limited in their responses as online regulation and moderation can potentially harm independent parties and voices, an essential part of democracy, as these efforts would risk mistaking legitimate narrative campaigns for Russian IW actions.

Many international players, including the West, use IW for their own advantage. However, in this case Russia has the upper hand. As discussed here, in the current state of affairs, Russia is winning in the cyber realm as it hits hard while blocking almost every major Western attempt of influence. Moscow influenced the United States, Britain, Europe, NATO, and many other countries and organizations, and it suffered only limited foreign interventions. Legislation such as the Yarovaya law or its sovereign internet law allows Russia to restrict the flow of undesirable information. For example, laws such as the foreign agent law discourage Russian citizens from regime criticism. Eventually, liberal democracies will need to strengthen their unique characteristics, revamp internet policies, and educate civilians in order to resist Russia's influence attempts. For democracy to prevail without the potential need to undermine their democratic nature, countries must enact efficient measures to contain hostile foreign propaganda.[64]

Endnotes

1. In this regard, China should also be mentioned as a unique case as it spreads information worldwide but vigorously restricts and protects its own cyber domain.
2. Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Foreign Affairs*, 16 November 2017.
3. Daria Litvinova, *Human Wrongs: How State-backed Media Helped the Kremlin Weaponise Social Conservatism*, Reuters Institute Fellowship Paper (Oxford, UK: University of Oxford, 2018).
4. Ronald Suny, *The Revenge of the Past: Nationalism, Revolution, and the Collapse of the Soviet Union* (Stanford, CA: Stanford University Press, 1993), 1–15.
5. Stephen G. Brooks and William C. Wohlforth, "Power, Globalization, and the End of the Cold War: Reevaluating a Landmark Case for Ideas," *International Security* 25, no. 3 (2001): 5–53.
6. Martin McCauley, *The Rise and Fall of the Soviet Union* (New York: Routledge, 2014), 437–52.
7. Ernest J. Wilson III, "Hard Power, Soft Power, Smart Power," *Annals of the American Academy of Political and Social Science* 616, no. 1 (March 2008): 110–24, https://doi

.org/10.1177/0002716207312618; and Joseph S. Nye Jr., "Get Smart: Combining Hard and Soft Power," *Foreign Affairs* 88, no. 4 (July/August 2009): 160–63.

8. Joseph S. Nye Jr., "Public Diplomacy and Soft Power," *Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 94–109, https://doi.org/10.1177/0002716207311699; and Patryk Babiracki, *Soviet Soft Power in Poland: Culture and the Making of Stalin's New Empire, 1943–1957* (Chapel Hill: University of North Carolina Press, 2015), 1–14.
9. An *influence operation* is the combined and synchronized application of diplomatic, informational, military, and economic abilities in times of peace or war that seek to influence decisions and behaviors or foreign targets. See Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica, CA: Rand, 2009), 3–6; and Bettina Renz, "Russia and 'Hybrid Warfare'," *Contemporary Politics* 22, no. 3 (2016): 283–300, https://doi.org/10.1080/13569775.2016.1201316.
10. Roger C. Molander, Andrew Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: Rand, 1996), https://doi.org/10.7249/MR661.
11. Timothy McCulloh and Richard Johnson, *Hybrid Warfare*, JSOU Report 13-4 (MacDill Air Force Base, FL: Joint Special Operations University, 2013).
12. Renz, "Russia and 'Hybrid Warfare'."
13. Nicholas J. Cull et al., *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It: An Analytic History, with Lessons for the Present* (London: London School of Economics and Political Science, 2017); and *Soviet Active Measures: Forgery, Disinformation, Political Operations*, Special Report No. 88 (Washington, DC: Bureau of Public Affairs, U.S. Department of State, 1981).
14. *GEC Special Report: Russia's Pillars of Disinformation and Propaganda* (Washington, DC: U.S. Department of State, 2020); and Richard Fletcher et al., *Measuring the Reach of "Fake News" and Online Disinformation in Europe* (Oxford, UK: Reuters Institute, University of Oxford, 2018).
15. Совет Федерации (Federation Council), "Концепция стратегии кибербезопасности Российской Федерации" (Concept of cybersecurity strategy of the Russian Federation) (n.d.).
16. Michael Connell and Sara Vogler, *Russia's Approach to Cyber Warfare* (Arlington, VA: CNA, 2016).
17. Jeffrey Hart, "Three Approaches to the Measurement of Power in International Relations," *International Organization* 30, no. 2 (Spring 1976): 289–305, https://doi.org/10.1017/S0020818300018282.
18. Connell and Vogler, *Russia's Approach to Cyber Warfare*.
19. Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear?: How New Is Russia's 'New Way of War'?," *Small Wars and Insurgencies* 27, no. 2 (2016): 282–301, https://doi.org/10.1080/09592318.2015.1129170; and Neil MacFarquhar, "A Powerful Russian Weapon: The Spread of False Stories," *New York Times*, 28 August 2016.
20. Matthew Chance, "Putin Has Relished US Political Chaos. He May Now Fear Trump's Impeachment," CNN, 12 November 2019.
21. Margarita Levin Jaitner and Kenneth Geers, "Russian Information Warfare: Lessons from Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO CCDCOE Publications, 2015).
22. A. Thomas Lane, "The Baltic States, the Enlargement of NATO and Russia," *Journal of Baltic Studies* 28, no. 4 (1997): 295–308, https://doi.org/10.1080/01629779700000111; and Nivedita Das Kundu, "Russia's Baltic Security Dilemma," *India Quarterly: A Journal of International Affairs* 59, nos. 1–2 (2003): 59–72, https://doi.org/10.1177/097492840305900104.
23. John R. Deni, "The Paradox at the Heart of NATO's Return to Article 5," *RUSI Newsbrief* 39, no. 10 (November/December 2019).
24. Here, we argue that Russia had in fact strengthened itself with its actions in South

Ossetia, Abkhazia (Georgia, 2008), and Crimea (Ukraine, 2014). Though the Russo-Georgian war as well as the annexation of Crimea were costly in terms of economic, diplomatic, and military costs, Russia had successfully managed to push countries within its backyard away from the West, away from joining NATO, and away from further integration in Western and Central Europe. With far greater economic and military power than Georgia or Ukraine, the Russian calculated cost-benefit analysis turned to be a sound investment. See Wojciech Konończuk, "Russia's Real Aims in Crimea," Carnegie Endowment for International Peace, 13 March 2014; Kakhaber Kemoklidze and Natia Seskuria, "Twelve Years Since the August War, Georgia Still Faces Russian Aggression," *RUSI Commentary*, 12 August 2020; and Ariel Cohen, "The Russo-Georgian War's Lesson: Russia Will Strike Again," *New Atlanticist* (blog), Atlantic Council, 10 August 2018.

25. Richard D. Hooker Jr., "Operation Baltic Fortress, 2016: NATO Defends the Baltic States," *RUSI Journal* 160, no. 3 (2015): 26–36, https://doi.org/10.1080/03071847.2015.1054731; and Stephen J. Flanagan et al., *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance* (Santa Monica, CA: Rand, 2019), https://doi.org/10.7249/RR2779.
26. James Kirchick, "Russia's Plot against the West," *Politico*, 17 March 2017.
27. Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: Rand, 2018), https://doi.org/10.7249/RR2237.
28. Henri Mikael Koponen, "Finland Remains Resistant to 'Fake News,' Disinformation," International Press Institute, 24 January 2018; and Corneliu Bjola and Krysianna Papadakis, "Digital Propaganda, Counterpublics and the Disruption of the Public Sphere: The Finnish Approach to Building Digital Resilience," *Cambridge Review of International Affairs* 33, no. 5 (2020): 638–66, https://doi.org/10.1080/09557571.2019.1704221.
29. Stefan Meister, "The 'Lisa Case': Germany as a Target of Russian Disinformation," *NATO Review*, 25 July 2016.
30. MacFarquhar, "A Powerful Russian Weapon."
31. Erik Brattberg and Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Washington, DC: Carnegie Endowment for International Peace, 2018).
32. Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019).
33. See Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, 2d ed. (Cambridge, UK: Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.
34. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.
35. Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (Oxford, UK: Oxford University Press, 2018), 4, https://doi.org/10.1093/oso/9780190923624.001.0001.
36. Eric Tucker, "FBI Director Warns of Ongoing Russian 'Information Warfare'," AP News, 5 February 2020.
37. Michael Birnbaum, "Sweden Is Taking on Russian Meddling Ahead of Fall Elections. The White House Might Take Note," *Washington Post*, 22 February 2018.
38. Президент России (President of Russia), "Военная доктрина Российской Федерации" (The Military Doctrine of the Russian Federation), 5 February 2010; and "Секретарь Совбеза Патрушев призвал защитить молодых интернет-пользователей от зарубежных спецслужб" (Secretary of the Security Council of Russia Patrushev Urged to Protect Young Internet Users from Foreign Intelligence Services), *Newsru*, 19 July 2019.
39. Lilia Shevtsova, "Forward to the Past in Russia," *Journal of Democracy* 26, no. 2 (April 2015): 24, 29, https://doi.org/10.1353/jod.2015.0028.

40. Президент России (President of Russia), "Об утверждении Доктрины информационной безопасности Российской Федерации" (On Approving the Doctrine of Information Security of the Russian Federation), 5 December 2016.
41. Президент России (President of Russia), "Об утверждении Доктрины информационной безопасности Российской Федерации."
42. *Process tracing* is a qualitative methodology used to understand whether and how a cause or a set of causes have influenced a set of changes in a given case study.
43. Official portal of legal information, http://pravo.gov.ru/; State Duma (Federal Assembly of the Russian Federation), http://duma.gov.ru/en/; and the Kremlin (Presidential Executive Office), http://en.kremlin.ru/.
44. Martin C. Libicki, "The Convergence of Information Warfare," *Strategic Studies Quarterly* 11, no 1 (Spring 2017).
45. Президент России (President of Russia), Федеральный закон от 06.07.2016 г. № 374-ФЗ (The Federal Law of 06.07.2019 No. 374-F3), 6 July 2016; "Joint Statement on Russia's 'Sovereign Internet Bill'," Human Rights Watch, 24 April 2019; Юлия Котова (Julia Kotova), "Госдума одобрила в основном чтении запрет на продажу смартфонов без российского софта" (The State Duma Approved a Ban on the Sale of Smartphones without Russian Software), *Forbes*, 19 November 2019; Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Ministry of Digital Development, Communications and Mass Media of the Russian Federation), Постановление Правительства РФ от 13 апреля 2005 г. N 214 (Decree of the Government of the Russian Federation of April 13, 2005 N 214), Об утверждении Правил организации и проведения работ по обязательному подтверждению соответствия средств связи (с изменениями от 13 октября 2008 г.) (On approval of the rules for organizing and carrying out work on the mandatory confirmation of the conformity of communication facilities, with changes from 13 October 2008); and Официальный интернет-портал Правовой информации (Official Internet Portal for Legal information), Федеральный закон от 02.12.2019 № 425-ФЗ (Federal Law of December 2, 2019 No. 425-F3), "О внесении изменения в статью 4 Закона Российской Федерации, О защите прав потребителей" (On amending article 4 of the law of the Russian Federation, about protection of consumer rights), 2 December 2019.
46. Nathalie Marechal, "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy," *Media and Communication* 5, no. 1 (2017): 29–41, https://doi.org/10.17645/mac.v5i1.808.
47. Президент России (President of Russia), Федеральный закон от 06.07.2016 г. № 374-ФЗ (The Federal Law of 06.07.2019 No. 374-F3—Yarovaya Law), 6 July 2016.
48. Metadata is stored for a period of one year and data (messages of internet users, voice information, images, sounds, video, etc.) for a period of six months.
49. Юлия Степанова (Yuliya Stepanova), Юлия Тишина (Yuliya Tishina), "Операторам не грозит хранение в особо крупных размерах" (Operators are not in danger of oversized storage), *Коммерсантъ (Kommersant)*, 27 April 2020; and Анна Балашова (Anna Balashova), Мария Кокорева (Maria Kokoreva), Юлия Старостина (Yuliya Starostina), "Facebook и Twitter не получили отсрочку на перенос серверов в Россию (Facebook and Twitter have not received a grace period to move servers to Russia)," RBC, 1 October 2020.
50. Министерство цифрового развития (Ministry of Digital Development), Постановление Правительства РФ от 13 апреля 2005 г. N 214 (Decree of the Government of the Russian Federation of April 13, 2005 N 214).
51. "Joint Statement on Russia's 'Sovereign Internet Bill' "; and Вячеслав Половинко (Vyacheslav Polovinko), Юлия Минеева (Yulia Mineeva), Дарья Козлова (Daria Kozlova), "Желейный занавес: Власть усиливает давление на Сеть, но «сувернет» выходит из-под контроля даже своих создателей" (Jelly Curtain: The Authorities Increases Pressure on the Web, but "Sovereign Internet" Gets Out of Control Even of Its Creators), *Но́вая газе́та*, 8 November 2019.
52. Петр Харатьян (Petr Kharatyan), "Предустановку российского софта Госдума

одобрила без обсуждения с бизнесом" (The State Duma Approved the Preinstallation of Russian Software without Discussion with Business), *Ведомости*, 5 November 2019.

53. Совет Федерации, "Информация о законопроектах, внесенных в Государственную Думу сенаторами Российской Федерации в порядке реализации права законодательной инициативы" (работа завершена в 2020 году) (по данным СОЗД на 5 февраля 2021 года) (Information on bills submitted to the State Duma by senators of the Russian Federation in order to exercise the right to legislative initiative (work completed in 2020) (according to the data of the Social Development Fund of the Russian Federation as of February 5, 2021), 5 February 2021; Официальный интернет-портал правовой информации (Official Internet Portal for Legal information), Федеральный закон от 02.12.2019 № 425-ФЗ (Federal Law of December 2, 2019 No. 425-F3), 2 December 2019; Anton Zverev, "Putin Signs Law Making Russian Apps Mandatory on Smartphones, Computers," NASDAQ, 2 December 2019; and Дмитрий Шестоперов (Dmitry Shestoperov), "Рунет берут на карандаш: В какое целое складываются части регулирования цифровой среды" (Runet Has Been Taken Under Control), *Коммерса́нтъ*, 27 December 2019.
54. Официальный интернет-портал правовой информации (Official Internet Portal for Legal information), Федеральный закон от 18.03.2019 № 30-ФЗ (Federal Law of March 18, 2019 No. 30-F3).
55. Varvara Percova and Aleksey Sivashenkov, "Со всем уважением. Чем обернется для Рунета закон об оскорблении власти" (With All Due Respect. What Will the Law on Insulting Authorities Bring to Runet?), *Forbes*, 18 March 2019.
56. Президент России (President of Russia), "Подписан закон, устанавливающий административную ответственность за распространение заведомо недостоверной общественно значимой информации" (Has Been Signed a Law Establishing Administrative Responsibility for the Deliberate Dissemination of False Socially Significant Information), 18 March 2019. False information is regarded as unreliable socially significant information distributed under the guise of reliable information that creates a threat to the life and health of citizens, property, and the threat of mass disturbance of public order and public safety.
57. "Russia: Russian President Signs Anti-fake News Laws," Library of Congress, 11 April 2019.
58. "Putin Signs 'Fake News,' 'Internet Insults' Bills into Law," *Moscow Times*, 18 March 2019.
59. 'Путин подписал поправки к закону «О СМИ» (Putin Signed Amendments to the «Media Law»), *Коммерса́нтъ*, 2 December 2019/
60. The definition of the term *foreign agents* is of great social significance for Russian natives due to Russia's authoritarian past.
61. Официальный интернет-портал правовой информации (Official Internet Portal for Legal information), Федеральный закон от 02.12.2019 № 426-ФЗ (Federal Law of 02.12.2019 No. 426-F3), "О внесении изменений в Закон Российской Федерации О средствах массовой информации" и Федеральный закон "Об информации, информационных технологиях и о защите информации."
62. Александр Воронов (Alexander Voronov), "В иностранные агенты могут записать блогеров, студентов и туристов" (Bloggers, students and tourists can be defined as foreign agents), *Коммерса́нтъ*, 25 November 2019.
63. "Freedom of the Net 2020: Russia," Freedom House, accessed 26 March 2021.
64. Kristina Hook, "Hybrid Warfare Is Here to Stay. Now What?," Political Violence at a Glance, 12 December 2018.