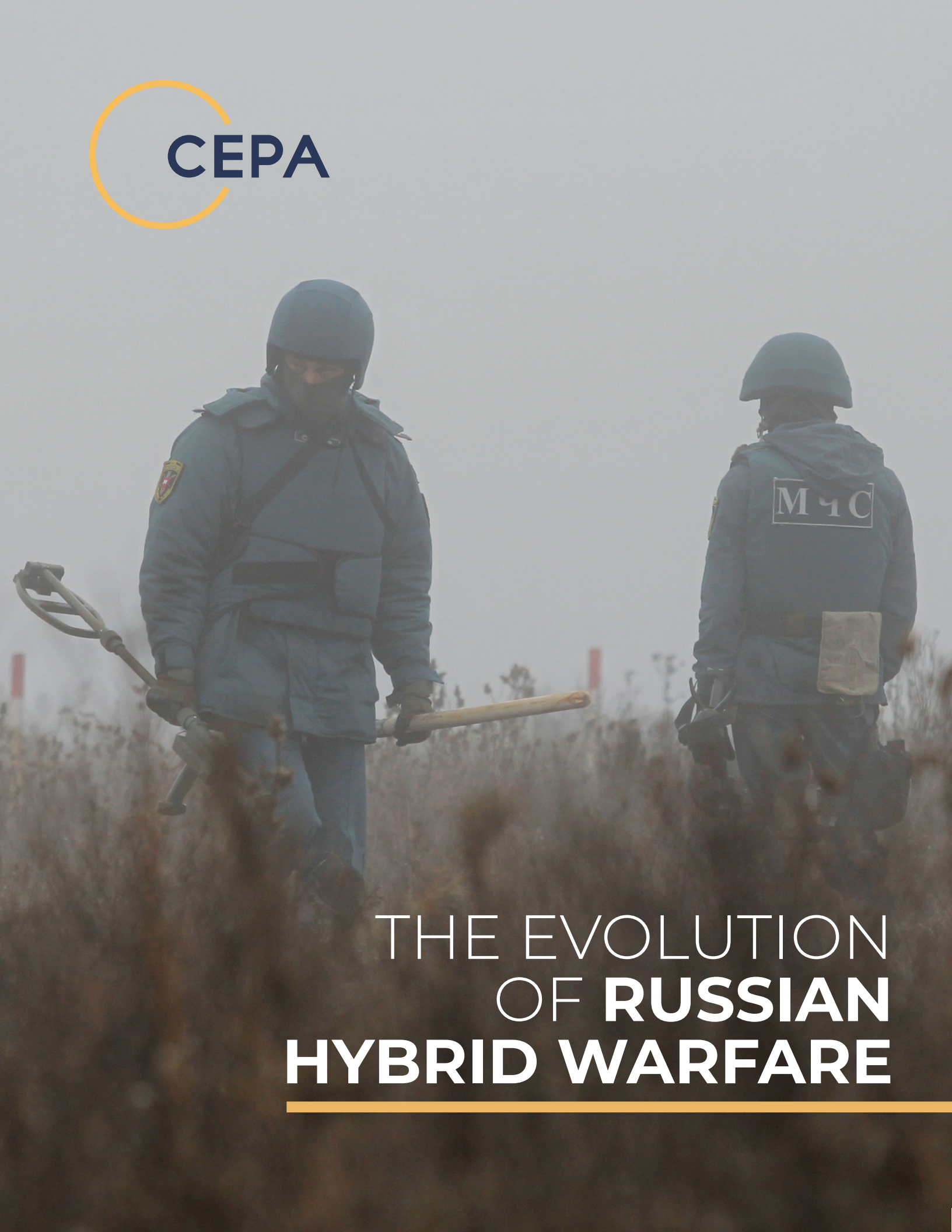
CEPA



THE EVOLUTION OF **RUSSIAN HYBRID WARFARE**

Contents

Introduction 2
Ukraine 7
Estonia 18
United Kingdom 27
EU/NATO 36
Conclusion 44
Endnotes 48

Acknowledgements

The authors are grateful for research assistance provided by U.S.-based journalist Iryna Solomko, as well as the communications and editorial team at the Center for European Policy Analysis (CEPA). The authors would also like to thank the external peer reviewers for their invaluable comments and suggestions, as well as Donald Jensen for his original framing of the research question. This report was made possible with generous support from the Smith Richardson Foundation.

About CEPA

The Center for European Analysis (CEPA) is a non-partisan think-tank dedicated to strengthening the transatlantic relationship. Headquartered in Washington, D.C. and led by seasoned transatlanticists and young leaders from both sides of the Atlantic, CEPA brings an innovative approach to the policy arena. Our cutting-edge analysis and timely debates galvanize communities of influence while investing in the next generation of leaders to understand and address present and future challenges to transatlantic values and principles.

Cover: Members of the Emergencies Ministry of the separatist Donetsk People's Republic demine the area at the militants' former positions on the contact line with the Ukrainian armed forces following troop withdrawals near the settlement of Petrivske (Petrovskoye) in Donetsk region, Ukraine November 19, 2019. REUTERS/ Alexander Ermochenko.

About the Authors

Alina Polyakova is the President and Chief Executive Officer of the Center for European Policy Analysis (CEPA). She serves on the board of the Free Russia Foundation and the Institute of Modern Russia and is professor of European studies at the Johns Hopkins School of Advanced International Studies (SAIS). Dr. Polyakova was the founding director for global democracy and emerging technology at the Brookings Institution.

Mathieu Boulègue is a research fellow at the Russia and Eurasia Programme at Chatham House, the Royal Institute of International Affairs, in London. Before joining Chatham House, Mathieu was a partner at the risk management and strategic research consultancy AESMA, where he worked as director of Eurasian affairs. In his research, Mathieu focuses particularly on Eurasian security and defence issues as well as on Russia's domestic and foreign policy.

Kateryna Zarembo, Associated Fellow, the New Europe Center. She teaches at the International Relations Department at the National University of Kyiv-Mohyla Academy. From 2010 to 2017 worked at the Institute of World Politics; she was a Deputy Director at the New Europe Center in 2017-2019. She got her Ph.D. from the National Institute for Strategic Studies (Kyiv, Ukraine), holds an MA in European Studies from the University College Dublin (Dublin, Ireland) and an MA in English and Italian Languages at the National Taras Shevchenko University (Kyiv, Ukraine).

Sergiy Solodkyy, First Deputy Director of the New Europe Center, is an expert in foreign policy, international relations, and security. Previously, he worked at the Institute of World Policy (2010-2017). Solodkyy graduated from the Westminster University majoring in International Relations and also from the Institute of Journalism of the Taras Shevchenko National University of Kyiv.

Kalev Stoicescu is a Research Fellow at the International Centre for Defence and Security (ICDS) in Estonia. Prior to joining ICDS in August 2014, Kalev was an Estonian Ministry of Foreign Affairs and Ministry of Defence official. Among other fields, he specializes in issues related to Russian foreign and domestic policy, as well as developments in the field of NATO's defence and security. He served at the Ministry of Foreign Affairs from 1991-2000, including as Ambassador to the OSCE and Ambassador to US and Canada. He was a member of the Estonian delegation in border negotiations with Russia and Latvia.

Precious N Chatterje-Doody is a Lecturer in Politics and International Studies at The Open University, UK. Her research focuses on Russian approaches to communication, memory and security, and she is the author (with Dr Ilya Yablokov, Leeds University) of Russia Today and Conspiracy Theories: People, Power and Politics on RT, forthcoming with Routledge in 2021.

Oscar Jonsson is academic director at the Center for the Governance of Change at IE University. He was earlier director of Stockholm Free World Forum, a subject-matter at Swedish Armed Forces Headquarters, and a visiting scholar at UC Berkeley. He holds a PhD from Department of War Studies, King's College London and is the author of The Russian Understanding of War (Georgetown University Press).

INTRODUCTION

Alina Polyakova and Mathieu Boulègue

In 2018, CEPA examined Russia's approach to nonlinear competition in its well-received report "Chaos as a Strategy: Putin's 'Promethean' Gamble."[1] The report's initial assessment was that Kremlin leaders were applying military and nonmilitary means as one in the same, that they were strategic in intention and opportunistic in their use of chaos, and that they were succeeding by effectively managing two of the most essential variables in their strategy: time and risk.

The result is a form of strategic competition whereby Russia sows chaos to achieve its agenda beyond its borders by deploying an array of hybrid warfare tools. This "chaos strategy" calculates that a relatively weakened Kremlin can avoid direct competition with the West to still successfully compete by splintering its opponents' alliances, dividing them internally, and undermining their political systems, and by doing so ensure long-term regime survival.[2]

From the Kremlin's perspective, hybrid warfare is a tactical application of the chaos strategy. It is full spectrum warfare that deploys a blend of conventional and nonconventional means aimed at affecting on the ground changes in target while seeking to avoid direct military confrontation with Western states. Hybrid warfare is employed in a tailored way to sow chaos in target countries. Such efforts generally include irregular warfare, active measures, and special operations.[3] Unable to compete in direct confrontation, the Kremlin's use of hybrid warfare is a means to compensate for its weaknesses vis-à-vis the United States and NATO.

But hybrid war is not static. Over time, Russia's views on the conduct and efficacy of its chaos strategy with the West has evolved based on experience, development of new tools, and assessment of the Western response. From the West's point of view, it is paramount to assess the *evolution* of Russia's hybrid warfare tactics to better understand likely developments in multi-vector warfare against Western interests, international institutions, and frontline states.

The West, however, is not united on how to confront the issue and define common solutions to the problem, especially because lessons learned from one case rarely apply to another. Given that Russia's strategic assumptions about the conduct of hybrid warfare appear to be changing, Western policymakers would benefit from a fresh examination of how Russia's strategists and military leaders are adapting hybrid warfare tools to increase chaos, and Western responses to it.

This report seeks to assess, understand, and respond to the evolution of Russia's vision of the chaos strategy through critical examples of Russia's use of hybrid warfare. It looks at the evolution and adaptations of Russian hybrid warfare against four target countries and institutions — Ukraine, a frontline state suffering the consequences of aggressive Russian military and sub-threshold action; Estonia, whose resilience against Russian cyberattacks has inspired major policy changes in Europe regarding information security; the United Kingdom, a unique and remarkable example of how Western countries are affected by subthreshold activities, especially in the informational realm; and, finally,

institutions like the European Union (EU) and NATO, which are seeing their internal cohesion put to the test by Russian non-linear operations.

Each case study examines the evolution of Russia's tailored toolkit of nonlinear means of action, the impact on respective countries and institutions, as well as policy responses to the challenge. However, the Russian toolkit of hybrid means is different in each case study because these represent diverse theaters of operation for the Russian regime. Different tools are, therefore, deployed to different degrees to obtain different results.

What ties these case studies together is the fact that they are all targets of the Kremlin's chaos strategy. A key takeaway for understanding differing effects is that chaos strategy works in concentric circles: the further a country is from Russia, the less exposed it becomes in terms of diversity and impact of hybrid tools employed against it. Responses must, therefore, be crafted to fit the specific national and institutional environments.

Russia's Worldview and the Birth of Chaos

The chaos strategy, and the tactical use of hybrid warfare, was borne out of the perception among the Russian leadership that Russia is locked in a form of great-power competition with the United States and Europe, as well as increasingly with China. The stakes are high: ultimately, it is about the survival of the current Russian regime.[4]

For decades since the end of the Cold War, Russian authorities have been feeding a sense of post-Cold War humiliation that Russia's security concerns were not sufficiently taken into consideration, if not downright ignored. This grievance narrative is reinforced by a "besieged fortress" mentality at home that is fueled by a fear of encirclement by NATO forces and exclusion from the European security architecture. This would have forced Russia to choose confrontation over cooperation with the West.

For Russia, the problem remains that it cannot compete in a direct contest of national power

The Russian leadership has the perception that there is a window of opportunity to take action and make foreign policy and security intentions a reality[5] — the war with Georgia in 2008 was a harbinger of Russia's reassertion. What followed were calculated steps aimed at doing away with an international order the Kremlin leadership feels cheated by and disappointed with.

For Russia, the problem remains that it cannot compete in a direct contest of national power — political or conventional military — with its peer and near-peer competitors. The Russian leadership fundamentally feels its conventional military is inferior to the West's, and especially NATO. Therefore, as Russia cannot compete symmetrically, it chooses to contest and disrupt asymmetrically.[6]

It follows that Russia has seeded chaos via asymmetrical means through disinformation, cyberattacks, political subversion, business ties, and economic warfare, among other tools. The approach has combined both old and new, drawing on lessons from the successful use of Soviet-era asymmetric strategies, but amplified with the power of modern technology and social media.

Nonmilitary hybrid tools, as those being pondered by Russian military planners, are part of warfare *per se*.[7] Such means represent a coordinated and tailored effort at the strategic level to reshape the internal course — be it political, economic, or societal — of target countries. Russia uses a synergetic and convergent toolkit

of military and nonmilitary tactics[8] in its protracted conflict with the West, honed by a willingness to alter, by force if necessary, the Western-led liberal international order. This effort also seeks to increase Russia's international standing in absolute and relative terms as well as advance Russian interests against the West.

Chaos 1.0: The Rise and Fall of the 'Gerasimov Doctrine'

While many voices feed the collective picture of Russia's military posture, Western analysis was swift to attribute the origins of Russia's current behavior to Chief of the Russian General Staff Gen. Valery Gerasimov. In February 2013, Gerasimov articulated his theory of modern warfare in a now-famous article for the Military-Industrial Kurier.[9] "Hybrid warfare" and the "Gerasimov doctrine" were consequently coined as umbrella terms[10] in the West to describe, often without context or erroneously, Russia's nonlinear approach to conflict. Indeed, the article was written in the context of Russia's response to the Arab Spring and fears of the spread of color revolutions against Kremlin-friendly regimes. Gerasimov fused methods from previous attempts to use nonlinear competitive strategies against more powerful rivals with updated technology and military concepts.

In this context, Russian operations must lead to information and psychological dominance of the enemy. Seeding chaos is, therefore, part of what Russian military strategists refer to as the "initial period of war" — taking after Soviet military theory but applied to modern warfare. These concepts eradicate the line between peace and war, placing politics and armed conflict in the same category.

In his text, Gerasimov described the way advanced military powers in the West engage in warfare, while outlining the importance of nonmilitary means to achieve military goals. He highlighted the primary threats to Russian sovereignty and suggested that the Kremlin's political leadership needed to be more open to innovative ideas on future security challenges.[11] Gerasimov drew from Russian military strategists like Vladimir Slipchenko, the former vice president of the Russian Academy of Military Science,[12] military writers Sergey Bogdanov and Sergey Chekinov,[13] and Chief of Main Directorate for Political-Military Affairs of the Russian Armed Forces Andrey Kartapolov.[14]

This is rather a tactical applications of how Russia understands modern warfare. It reflects a pragmatic acceptance of the need to take what opportunities arise. What makes this chaos strategy unique is the fact that the synergy between nonlinear and nonmilitary tactics is no longer auxiliary to the use of force, but rather the equivalent of force itself. Of course, Russian military thinkers did not exclude the use of conventional forces. On the contrary, they stressed Russia's need for innovation and the wider modernization of its armed forces. Russia's "soft power" (*miagkaia sila*) is only here to prepare the ground for hard power.

Based on Western responses to their behavior patterns thus far, Russian leaders could draw the conclusion that time is indeed on their side. Disorientation and distraction in the West produce more one-sided concessions, and, therefore, purchase more time for Russia than victory on any battlefield. Worse yet, the second lesson that Russian leaders could draw is that risk-taking works. CEPA's analysis of the "Chaos 1.0" strategy warned that an underlying danger for Russia was in executing the strategy over an extended period.[15]

Chaos 2.0: Understanding the Evolution of Hybrid War

Chaos is not entirely static. A significant event in the evolution of Russia's use of chaos to compete against the West occurred when Gerasimov delivered a keynote speech to the Russian Academy of Military Science in March 2019.[16] Gerasimov reported on evolutions of military strategy and military-scientific developments. The address was important in how it differed from his 2013 assessment on the use of nonlinear means to sow chaos.[17] While presenting operational lessons learned from recent deployments in Syria, Gerasimov insisted on the use of military power as well as political-military coercion.

Throughout his speech, Gerasimov insisted on two main "vectors" in the development of Russian military strategy: limited action and active defense. These developments will influence military thinking and, subsequently, military procurement in the coming years, as well as likely inform new iterations of the Russian military doctrine. All these represent, in a way, Gerasimov's personal military legacy.

The strategy of *limited action* outside Russia's borders seeks to counter existing threats to Russian national interests through limited out-of-area military intervention. This largely encompasses lessons learned from operations in Syria, and to an extent in eastern Ukraine. Accordingly, asymmetric and nonlinear methods of action are paramount, not least to obtain and keep informational superiority throughout the duration of military operations with an emphasis on surprise and decisiveness. While this does not offer a blueprint for persistent global power projection, which Russia cannot afford, limited action endorses the focused application of conventional military power as a tool of state power to achieve national aims.[18] This is a dangerous reminder for the West and its allies that the chaos strategy is indeed working. Instead of becoming subtler and more nuanced, Russia's ambitions for chaos are becoming bolder and more direct, as depicted in the case studies.

The strategy of *active defense* aims to preemptively neutralize threats through active measures. Accordingly, this would be a response to Western interference, depicted by Gerasimov as a "Trojan Horse." This reference to the West is more confrontational than before: it frames the United States as an "aggressor" and accuses it of developing interference strategies that combine fifth-column political warfare and color revolutions with high-tech global strike capabilities. This, too, is linked to the preparation of the operational environment through information superiority and the use of nonlinear tactics. Active defense employs the Soviet toolkit of deception (*maskirovka*) and places the onus on nonmilitary means of action.[19]

Entropy in a Changing World

Russia's military interventions in Syria, Venezuela, and, more recently, Libya raise the question whether the Kremlin is still being opportunistic or whether it has revised its military strategy to better project force around the globe based on a single playbook. These interventions have taken advantage of preexisting chaos and weakness that Russia did not directly cause. Together with its growing conventional power, Russia is now far more confident about using hard power in the hybrid mix.

The aforementioned changes in Russian military thinking reflect a reinvigorated confidence in the efficacy of chaos as a competitive strategy. If anything, the Kremlin leadership feels vindicated about the usefulness of hard power options, while categorizing nonmilitary means as a tool to prepare conflict environments and make the use of force more effective.[20] This

is best exemplified by Kalev Stoicescu's chapter on Estonia, where the threat of Russia's military action cannot be dissociated from hybrid tools aimed at testing the country's resolve below the threshold of Article V of NATO's founding treaty, which commits the Alliance to collective defense.

Among the drivers of change in Russian thinking, disappointment and unexpected outcomes have been some of the most powerful. As Kateryna Zarembo and Sergiy Solodkyy show, this is most notably the case with low-intensity military operations in Ukraine: difficulty in upholding a degree of "plausible deniability" of direct military intervention; war fatigue; issues with managing proxy groups and local militia; the failure of "Novorossiya" and other ideological products in Ukraine;[21] the absence of an exit strategy in the Donbas, etc. Russia has now altered its originally ambitious aim (to control Crimea *and* the Donbas) in favor of perpetuating a persistent, low-scale conflict that will impede Ukraine's integration into Western security structures.[22]

Further afield, in the United Kingdom, Precious Chatterje-Doody explores how Russian hybrid operations — mainly information operations — have been adapting in order to infiltrate networks, destabilize internal norms, and ultimately create an environment conducive to Russian interests. Oscar Jonsson outlines Russian tactical adaptations in the EU and NATO, where Russian hybrid tools are used to increase political polarization and challenge institutional cohesion.

Chaos strategy through hybrid, multi-vector warfare is here to stay. The consequences of this are many and unwanted, and notably include the potential for miscalculation with the West. To avoid such a situation, U.S. experts and leaders can learn much from the knowledge and experiences of allies and partner states in Europe — countries and institutions which have long been contending with the most aggressive forms of Russia's hybrid warfare.

UKRAINE

Kateryna Zarembo and Sergiy Solodkyy

Evolution of Russia's Hybrid Warfare: The Case of Ukraine

As a target of Russia's hybrid warfare, Ukraine is a unique case study. Not only does it offer valuable data for analysis and lessons learned, but it is also arguably one of the most vulnerable victims. Its geographical and historical proximity to Russia, as well as Russian ambitions to take control of Ukraine as a part of its own heritage, likely mean that the Kremlin has trained the full force of its hybrid warfare machinery on Ukraine.

With this in mind, the resilience Ukraine has demonstrated since independence, and especially after 2014, is remarkable and worthy of detailed analysis. In particular, assaults on Ukraine's politics, military, economy, social fabric, and information space have to be considered. This chapter offers an explanation of Ukraine's successes, address its challenges, and concludes with lessons learned from its experience.

Russia's Hybrid Tools of Aggression against Ukraine

Russia has used *conventional military means* against Ukraine, but it has added a few twists to further frustrate and exhaust its victim. Russian troops, who even during the most sweeping of military operations against Ukraine in 2014-2015 were dressed in Russian military green uniforms without insignia and chevrons, were labeled "green men."[23] But there was no official declaration of war or even an admission by the Russian government that it had sent soldiers to Ukraine. Russian President Vladimir Putin acknowledged that his country's troops had occupied Crimea only after the special operation was over.[24]

Meanwhile, the Russian leadership has never acknowledged the presence of Russian troops in eastern Ukraine, although the evidence shows that Russia has sent modern arms and troops to the fight. The Kremlin has played word games to whitewash its violations of international law, claiming, for instance, that Russian soldiers "got lost" and found themselves in the war zone.[25] Another time, when members of Russian special forces were captured in Ukraine, Putin averred that Russia "has never said that there were no people who are engaged in solving certain issues, including in the military sphere."[26]

As for the presence of their weapons in Ukraine's occupied territories, Russian officials have said that perhaps fighters had seized them from the Ukrainian army or had somehow acquired them on their own. In another example of hybridity, mercenaries from the so-called Wagner Group — a Russian paramilitary formation that has fought in global conflicts, including in Syria and probably in Sudan and the Central African Republic — have turned up in Ukraine.[27]

Just as energetically, and despite the international inquiry, Russia denies that its troops shot down a Malaysia Airlines passenger plane over Ukraine in July 2014. One of Russia's arguments is that Ukraine was obliged to close the airspace in the war zone. Russia has also blocked efforts

The primary goal of Russia's military operations at this stage is to keep Ukrainians demoralized and stressed from the ever-present threat of ramped-up aggression.

to set up an international tribunal and ignored major requests from investigators in the Netherlands, undermining and slowing the probe. Russia is trying to shift responsibility from itself to Ukraine, even when the evidence unequivocally proves Russia's guilt.

The primary goal of Russia's military operations at this stage is to keep Ukrainians demoralized and stressed from the ever-present threat of ramped-up aggression. By keeping the war on a steady simmer, Russia feeds the frustration and resentment that it hopes Ukrainians will gradually direct at their own politicians. That anger gives rise to suspicions that, for example, Ukrainian politicians are not interested in ending the war, possibly profit from it, or are using it to antagonize pro-Russia voters.[28] In this way, the prolonged conflict sows chaos in Ukraine's politics and gives a boost to movements that seemed either marginal or even hostile to Ukraine five years ago.

Political tactics are among the most significant weapons in the hybrid warfare arsenal. Russia's most obvious use of them in Ukraine is its support for the leaders of the Opposition Platform – For Life (Opozytsiyna platforma – Za zhyttia, OPZZh) party, who call for closer relations between Ukraine and Russia. Party leader Viktor Medvedchuk has never hidden his friendly ties with Putin, who is the godfather of his daughter.[29] One of Ukraine's richest politicians, with assets estimated at $133 million,[30] Medvedchuk headed the presidential office of then-Ukrainian President Leonid Kuchma in the early 2000s, when Ukraine's relations with the West were strained over persecution of the political opposition and independent media. Medvedchuk held no position in the governments of Presidents Viktor Yushchenko (2005-2010), Viktor Yanukovych (2010-2014), or Petro Poroshenko (2014-2019), but he was still considered a prime mover behind the scenes and nicknamed the Gray Cardinal.[31]

When Russia began its incursions into Ukraine in early 2014, Medvedchuk took on the role of negotiator with representatives of Russia-controlled members of militarized groups in the Donbas. According to a report from Espresso TV, German Chancellor Angela Merkel, after reportedly being asked by Putin, appealed to Poroshenko to involve Medvedchuk in the talks.[32] Medvedchuk turned out to be a key player in negotiations for the release of Ukrainian hostages held captive in Russia or in prisons in Russia-controlled Crimea and eastern Ukraine.

Political tools currently play a key role in influencing the situation in Ukraine. The presidential and parliamentary elections in 2019 showed considerable public support for politicians who could find peaceful solutions with Russia.[33] However, Ukrainians were still not ready to massively support those politicians who are extremely pro-Russia. Medvedchuk enjoys little popularity in Ukraine, and his party's support is purely regional. Pro-Russia forces would have had much more opportunity to influence the political agenda had Russia not occupied territories most loyal to such politicians.

The *economic dimension* of hybrid warfare is equally relevant to this discussion. Ukraine suffered economic blows on several fronts, including lost industries in Crimea and the east, direct costs of the war, lost trade with Russia, and Russia-imposed punitive measures from import bans to economic sanctions against individuals. As a result,

after 2014 trade between Russia and Ukraine dropped by 75% and, according to Ukrainian economists, has fallen back to its early-2000s level. All of these problems helped shrink Ukraine's economy, with GDP dropping from $183 billion in 2013 to $91 billion in 2015, reaching $153 billion in 2019.[34]

Energy trade is a major component of economic warfare. Russia has worked to undermine Ukraine's reliability as an energy transit country, most notably by shutting off the flow of gas to Central and Eastern Europe in the winter of 2009 over a pricing dispute with Ukraine. It has also pushed forward with work on the Nord Stream 2 undersea pipeline to Germany, which would bypass Ukraine and weaken the country's leverage as an energy transit partner in dealings with Russia.

Attacks on Ukraine's *social fabric and information space* are closely linked. The Institute for the Study of War's Mason Clark has written that Russian strategists consider information operations "the most important sphere of military operations, as both an independent battlefield and an enabler of successful kinetic actions."[35] Clark also writes that "the Russian military views this new relationship between information and kinetic operations as a two-way street: kinetic operations are now inherently subordinate to the information campaign of a hybrid war; no kinetic operation can succeed unless it is nested in and enabled by the overall information campaign."[36] This strategy translates into a hybrid war in which society is as much a target as the central government or military. Depending on the circumstances, Russia employs the tools that seem most appropriate for the purpose and timing: different phases of Russian hybrid warfare are characterized by different instruments.

In Ukraine, information warfare in traditional media is waged less through Russian networks, which reach only 9% of the population,[37] than through local channels. For example, the NewsOne, 112 Ukraine, and Zik television channels belong to Taras Kozak, a former member of parliament from the Opposition Bloc who is said to be a close Medvedchuk ally.[38] And, of course, the Kremlin makes liberal use of trolls and bots on social media in Ukraine, as it does around the globe.

The aim of Russia's information strategy is not so much to make Ukrainians look kindly on Russia as to sow distrust and instability within the country, to delegitimize the government, and to drive wedges between the people and the authorities, and between various groups in society and politics. There are several examples of Russia's hybrid warfare in Ukraine — such as support for attacks on minorities to instigate interethnic violence or accusations against Poroshenko of profiting from his chocolate factory in the Russian city of Lipetsk while the then-president's company insisted that profits from the plant actually went for taxes and charities in Ukraine.[39] Some Ukrainians fear that if civil unrest were to break out, Russia would use it as a pretext for military intervention as a "peacekeeper," which would eventually lead to a total loss of sovereignty. These fears have been voiced for years since Russian aggression against Ukraine started in 2014.[40]

But sometimes Russia's strategy is self-defeating. One effect of its hybrid warfare in Ukraine has been to build domestic support for Ukraine joining the European Union (EU) and NATO. Prior to Russia's seizure of Crimea and military actions in eastern Ukraine, the country had been split on the question of accession to either organization. Russia's belligerence has so outraged Ukrainians that now almost half support membership in NATO, a record high, and almost 60% favor joining the EU (26.9% oppose joining the EU and 32.8% oppose joining NATO, according to the poll conducted by SOCIS and Razumkov Center in July 2020).[41] Russia has unwittingly helped clarify some thinking in Ukraine and eased a long-standing source of disagreement.

An armed serviceman looks out from a Russian army vehicle outside a Ukrainian border guard post in the Crimean town of Balaclava March 1, 2014. REUTERS/Baz Ratner.

The Phases of Russia's Hybrid Warfare against Ukraine

A constant in Ukraine and Russia's frequently turbulent relationship has been Russia's view of its neighbor as an extension of itself that was never meant to be independent. There have long been politicians in Moscow who speak of Ukraine as a territory of Moscow's "privileged interest," and Russia's top leadership has sincerely regretted the collapse of the Soviet Union.[42]

Russian elite make great efforts to thwart Ukraine's development as a full-fledged state. For example, Russia ratified the "Big Treaty" (the Treaty on Friendship, Cooperation, and Partnership), which provides for the inviolability of Ukraine's borders, in December 1998, nearly a year after Ukraine had done so. Russian diplomats also repeatedly delayed negotiations on delimiting the countries' shared borders so that an agreement was not signed until 2010, almost 20 years after Ukraine gained independence. The two countries still have not been able to agree on the division of the maritime space, and the Russian occupation of Crimea ensures that they will not do so any time soon.

Looking over the past three decades, we can discern at least four stages of Russia's political influence on Ukraine. First came the preparatory phase, which covers the period from the collapse of the Soviet Union to the beginning of the military operation against Ukraine that Russia launched in February 2014. The second stage was the failed blitzkrieg, when Russia moved to take control of Ukraine's south and east, including Crimea. This stage, which lasted until early 2015, was a turning

point because it saw the most intensive involvement of Russian armed forces.

The third stage began in February 2015, after the signing of the so-called Minsk II agreements, when Russia stepped up its use of political, economic, social, and information campaigns as it dialed back military operations. We are now witnessing the fourth phase of this hybrid war, which began in the spring of 2019 and is waged primarily through agents of influence in Ukraine. This period has seen growing support for political forces that promote concessions to Russia.

Clearly, Russian policy toward Ukraine has changed little since 1991. The Kremlin has never accepted the notion of an independent Ukraine, free to join the EU or NATO, which it is convinced would undermine its traditional influence in this part of the world. What has changed in the last three decades is how much the Kremlin relies on various means of influence to keep Ukraine under its thumb, culminating in Russia's 2014 military attack on Ukraine.

2.1 Phase 1: preparation

To analyze the evolution of Russia's hybrid war, it is important to consider the preparatory period, before the use of military force against Ukraine, because it allowed the Kremlin to test certain methods of coercion first. Thus, Moscow was aware of the Ukrainian army and security services' weaknesses, especially in Crimea, where 90% of members of the Security Service of Ukraine (SBU) switched to the Russian side after the occupation.[43] Russia also understood how to work in the information sphere. Russian television, which was especially popular in eastern and southern Ukraine, spread stories during the 2014 protests about a coup d'état in Kyiv by right-wing radicals who posed a threat to Russian-speaking citizens. In this way, the Russian government worked in advance to tamp down resistance among a frightened population to its coming incursions.

Moreover, Russia already had experience conducting special operations in Crimea, in particular during a dispute over tiny Tuzla island in the Kerch Strait in 2003 when Russia tried to connect the Ukrainian island with its Taman Peninsula, and the campaign of Yuri Meshkov, who was elected president of Crimea in 1994 after calling for the peninsula's accession to Russia.

The Tuzla operation set the precedent for some special operations tactics in the framework of a hybrid war. For example, the Russian government dissociated itself from the construction of a dam to Tuzla that had precipitated the dispute, pointing the finger instead at local authorities. Despite diplomatic notes and harsh public statements, Russia remained silent. Only Ukraine's coordinated position forced Russia to stop the dam construction right at the Soviet-era administrative border.[44]

Meshkov's increasingly bold pro-Russia agitation, which ended with special forces invading his residence, and the Tuzla crisis are two of the better-known conflicts between Ukraine and Russia before the 2014 hybrid war, although there were many others, including "gas wars" over pricing, and Russia's interference in Ukraine's 2003 presidential election.

These episodes taught Moscow several important lessons:

Special operations are best launched when the central government is particularly weak and vulnerable. The hybrid war in 2014 had early success as a power vacuum had formed in Kyiv after Yanukovych, who was president at the time, fled the capital.

Support among local leaders, who can be disorganized and disruptive, for a special operation plays a secondary role. The Russian government must play a crucial, albeit covert, role in special operations.

Trust between the Ukrainian authorities and its Western allies must be undermined. For instance, Ukraine successfully appealed to international partners during the Tuzla crisis in 2003. Statements by Western governments likely influenced the actions of Russia, which at the time seemed to value cooperation with international institutions. In 1993, the issue of ownership of Crimea was even discussed in the United Nations Security Council where Russian diplomats — who were allied with then-Russian President Boris Yeltsin against a revanchist parliament — supported Ukraine's position.

Crucially, do not accept responsibility for a hybrid, unconventional attack. Moscow declares its non-involvement in the action and thus avoids responsibility under international law. Hybrid provocation is also cheaper than a large, overt campaign.

2.2 Phase 2 (2014-2015): failed blitzkrieg

The hybrid war just after Russia's annexation of Crimea in March of 2014 included clear and coordinated Russian actions inside Ukraine, along with efforts to discredit the new government abroad. Russia aimed to carry out a kind of blitzkrieg, so things moved fast in Crimea and southern and eastern Ukraine.

But if Crimea was captured without a single shot fired, the rest of Ukraine began to resist the "Russkaya Vesna" (Russian Spring, a militarized allusion to the Arab Spring), which aimed at the secession of Ukraine's regions. Ukraine's government had been slow to react to developments in Crimea because it did not know if its army and special forces were ready to defend the country's sovereignty, and because foreign allies urged Ukraine "to resolve the conflict peacefully" and not to "take hasty steps."[45]

After the seizure of office buildings in eastern and southern Ukraine, Kyiv decided to use its military. Russia likely (and wrongly) had envisioned a bloodless operation in which part of Ukraine would be taken over by pro-Russia or Russian representatives. It did not expect this level of military reaction and massive public resistance, which forced the leadership to change its initial plans.

2.3 Phase 3 (2015-2019): low-intensity conflict and other means

After the Minsk agreements in February 2015, Russia pivoted to a low-intensity military conflict in the east combined with hybrid attacks on the rest of Ukraine. Its moves served primarily to destabilize Ukraine and discredit Ukraine's leaders in the eyes of their people and their Western partners. Russia's policy changed due to the introduction of EU and U.S. sanctions as well as the signing of the Minsk agreements. Russia was interested in their implementation, as they would effectively allow Ukraine's federalization and legitimization of Russia's "stooges" among the local elite. In addition, maintaining a low-intensity hybrid conflict is militarily cheaper than a full-scale one.

To begin with, the GRU, Russia's military intelligence service, and the FSB, Russia's domestic intelligence agency, have carried out dozens of special operations in Ukraine, which have been meticulously documented by researchers.[46] These include attacks on critical infrastructure and armament depots, and assassinations of members of Ukraine's security services, soldiers, and Russian dissidents who had fled to Ukraine.[47] There have also been more subtle information attacks, such as a phone call between the Ukrainian and Russian presidents Petro Poroshenko and Vladimir Putin that the Russians leaked in order to stir up distrust of the Ukrainian head of state.[48] As for "conventional" espionage, there was the Russian spy Stanislav Yezhov who served as an interpreter to the Ukrainian prime minister.[49]

In addition, the Ukrainian security service has said Russian agents were behind attacks on ethnic minorities in Ukraine, including Roma, Jews, Hungarians, and Rusyns, with the goal of instigating interethnic tensions and violence.[50]

Cyberattacks have also been central to Russian hybrid warfare. In 2018 alone, the SBU reported some 360 known cyberattacks against Ukraine, and in 2019, the number approached 500.[51] In the lead-up to the presidential election in 2019, Ukraine braced for more cyberattacks, especially against its Central Election Committee. While the election took place without major disruptions, some Ukrainian officials counted as many as one cyberattack every 40 minutes against certain Ukrainian institutions. NATO specialists trained their Ukrainian partners to counter cyberattacks ahead of the country's local elections in 2020.[52]

Fakes and disinformation have also become integral to Russia's hybrid warfare. As just one instance, an analysis by Internews Ukraine of the Ukrainian segment of the Russian social network VKontakte ahead of the 2019 presidential election found a largely negative portrayal of both the presidential candidates and Ukraine as a dysfunctional state.[53]

All the while, Ukrainians have lived under the constant threat of further military aggression. From 2015 to 2019, Russia violated the cease-fire negotiated by the Minsk Trilateral Contact Group more than 20 times,[54] including in the first hours after it was proclaimed. Russia also regularly holds military exercises close to Ukrainian territory and amasses its military units along the Ukrainian border and in occupied Crimea, combining hybrid means of aggression with psychological pressure.[55]

One lesson the Kremlin has repeatedly drawn from its warfare against Ukraine is to avoid open aggression, which does not allow it to deny responsibility

Fakes and disinformation have become integral to Russia's hybrid warfare.

for the armed conflict and mobilizes Ukrainian public opinion against Russia as well as Western support for Ukraine. For example, it was only after the open aggression in 2014 that support for the union with Russia among Ukrainians dropped radically: from 30% in May 2013 to 21.4% in May 2014 to 7.8% in June 2017 (according to a poll conducted by the Ilko Kucheriv Democratic Initiatives Foundation).[56] As for Western support, a relevant example relates to Russia's November 2018 attack on and seizure of three Ukrainian navy vessels in the Kerch Strait. This incident prompted the EU to open a field office of its advisory mission (EUAM) in Mariupol, a step that EU countries had strongly opposed earlier as too sensitive for EU policy regarding the conflict in the east.[57]

2.4 Phase 4 (2019-present): is Russian soft power back?

A change in Ukraine's leadership in 2019 might have presented Russia an opportunity to change its approach to its neighbor. Instead, while Ukraine's new president, Volodymyr Zelenskyy, adopted some different policies toward Russia, the Kremlin kept to relatively the same tactics. The only noteworthy difference is that conditions in Ukraine have provided more opportunities for hybrid influence.

In the first place, pro-Russia political forces have gained ground in Ukraine, as over time ties to Russia have become less disqualifying in the country's politics. For example, the Opposition Platform – For Life party won 43 seats in parliament in 2019, up from 29 seats in 2014, even after two of its members, Medvedchuk and pro-Russia oligarch and energy tycoon Yuriy Boyko, met with then-Russian

Prime Minister Dmitriy Medvedev four months earlier. In fact, it was in 2019 that Medvedchuk made a comeback in Ukraine's national politics, running on the Opposition Platform party list and becoming a member of parliament.

Since the election, the initial trust that Ukrainians had placed in Zelenskyy's victorious Servant of the People party has dwindled, while the Opposition Platform has gained support. A recent opinion poll found that if parliamentary elections were held in November 2020, the Opposition Platform and European Solidarity parties would have shared second place, each with roughly 16% of the vote, an unimaginable result back in 2014.[58] Even some notorious pro-separatist politicians in eastern Ukraine — for instance, Nelia Shtepa, a former mayor of the city of Sloviansk who was arrested in 2014 on charges of violating Ukraine's territorial integrity but later released without trial — fared decently in the 2020 local elections, coming third with 16.6% of the vote.

The Kremlin's tactics, though, aim not so much to install a pro-Russia government in Kyiv as to destabilize Ukraine until it becomes the failed state that Russian propaganda has long claimed it to be. The most recent example of such an approach appeared in October 2020 when the Constitutional Court, acting on the Opposition Platform's appeal, ruled e-declarations by public officials to be unconstitutional. Not only was the introduction of e-declarations for public officials considered to be the one of the key post-Maidan anti-corruption measures, the court's ruling threw Ukraine in a constitutional crisis. Indeed, any action against the ruling or the court itself could undermine the separation of powers and start a spiral of illegality, not to mention jeopardize Ukraine's relations with its Western partners. One can only hypothesize whether the idea was concocted in the Kremlin given that the appeal was submitted by the chief pro-Russia party. Be that as it may, the outcome serves Russian interests well.

In the armed conflict, the most notable recent change has been the replacement of Vladislav Surkov, a former aide to Putin and the Kremlin's informal chief of propaganda, by Dmitriy Kozak as the stage manager of Russia's involvement in Ukraine. Kozak is best known as the champion of a failed Russian plan for Moldova in 2003 that would have made concessions to separatists in the country's Transnistria region but would have reunited both sides in a federation (and which Moldova's then-President Vladimir Voronin pulled out of right before the expected signature).[59]

The change of personalities in Moscow has not translated into a change in policy as yet. The Kremlin has so far manipulated the conflict-settlement process to its own advantage, winning back some crucial figures captured by the Ukrainian security services in prisoner exchanges, including Vladimir Tsemakh, suspected of downing the Malaysia Airlines plane in 2014.

Some Ukrainian journalists have alleged Zelenskyy's office and the SBU sabotaged some special operations, including the capture of Russian mercenaries from the Wagner Group who are reportedly fighting in eastern Ukraine.[60] While these allegations have not been proven, they feed suspicion and distrust toward the authorities.

Some analysts predict that the Kremlin will try to destabilize Ukraine through regional referendums. Zelenskyy is trying to change Ukrainian law to permit such referendums.[61] This idea is consistent with the Kremlin's strategy in Ukraine.

Ukraine's President Volodymyr Zelenskiy and servicemen walk in a trench near the frontline with Russian-backed separatists in Krasnohorivka in Donetsk Region, Ukraine August 7, 2020. REUTERS/ Gleb Garanich.

Ukraine's Recipe for Resilience

3.1 What has worked ...

Ukraine's success in countering Russia's hybrid war is difficult to assess. The Kremlin continues efforts to shape Ukraine's domestic and foreign policy agendas in a conflict intended to exhaust Ukrainian resources and cause enough economic or societal havoc that Kyiv will be forced to make concessions.

It is impossible to know how the conflict would have developed had the West not supported Ukraine, or how Russia would have acted and how Ukraine would have fared had the government in Kyiv not sent the army to meet Russian aggression in the Donbas in 2014. Still, we can draw certain lessons from Ukraine's experience.

Reforms are key to Ukraine's ability to withstand Russia's hybrid warfare. Ukraine's desire to join the EU and NATO adds fuel to the country's efforts to root out corruption and strengthen the rule of law, while hybrid wars are more effective in countries where institutions are weak and elite corrupt. Thus the Ukrainian government has set a course to reform those areas that can counter Russian aggression directly, such as defense, and those that affect its security and resilience more generally (fight against corruption, rule of law, decentralization, etc.). It has faced an extraordinary challenge due to a shortage of honest politicians and funds.

As many have noted, Ukraine is forced to wage two wars simultaneously: one on its eastern front to stop Russian attacks and the other at the national level to push through reforms opposed by an old guard of bureaucrats and oligarchs.[62] Independent

assessments have credited Ukraine with making significant improvements in its defense capabilities. The Ukrainian army has come a long way toward reaching interoperability with the armies of NATO countries, and it has gained valuable experience in its conflict with Russia.[63]

Contacts between Ukrainian and Western officials have played an important role in deterring further Russian aggression. Keeping its Western partners (above all, Germany, France, and the United States) involved in mediation and holding Russia accountable has been one of Ukraine's biggest achievements in dealing with the conflict. It has been crucial that Germany and France have led negotiations with Russia under the Normandy Format. They have supported Ukraine on key matters, such as insisting that eastern Ukraine be demilitarized before any new political arrangements, or "special status," for the embattled regions can be made. Another important point is that EU and U.S. sanctions against Russia clearly signal who the aggressor is, even if the aggressor itself denies its involvement.

Another less publicized but important backstop has been support for Ukraine in international tribunals, including the International Court of Justice (ICJ) and the International Tribunal for the Law of the Sea. An interim success for Ukraine came in November 2019 when the ICJ ruled that its claims against Russia are proper and within the court's jurisdiction.[64] Ukraine filed its case back in 2017, accusing Russia of violating international agreements against racial discrimination and financing terrorism. It took the Ukrainian side three years to prepare 29 volumes and more than 17,500 pages of evidence against Russia.

Also contributing to Ukraine's resilience is its civil society. Groups such as Come Back Alive, which provides equipment, medical supplies, and training to the army, and StopFake, the Ukraine Crisis Media Center, and Internews Ukraine, all of which work to reveal and counter Russia's information warfare, are a trump card for Ukraine that the Kremlin failed to anticipate. Promisingly, Ukraine's civil society has become a recruiting ground for the country's political class.

3.2 … and what hasn't

Despite the abovementioned achievements, Ukraine's track record on reform is mixed. This per se doesn't belittle Ukraine's achievements in countering Russian hybrid aggression. However, every incomplete reform or weak spot in its institutions is something that the adversary can capitalize on, especially in such spheres as security and defense. The reform efforts, which are crucial for the country's resilience, are sometimes seen as one step forward and one step back.[65]

For example, in an attempt to eradicate bribery, the Ukrainian authorities have created an anti-corruption infrastructure that includes the High Anti-Corruption Court, the National Anti-Corruption Bureau of Ukraine (NABU), the Specialized Anti-Corruption Prosecutor's Office, and the National Agency for the Prevention of Corruption. However, until now there have been no "big" cases involving the prosecution and punishment of corrupt officials. In addition, some interinstitutional controversies remain, for example, the willingness of both Poroshenko and Zelenskyy to retain their control over NABU.[66] The abovementioned constitutional crisis, which dealt a blow to both anti-corruption infrastructure and the judiciary, is another case in point.

The long-overdue reform of the SBU is still a work in progress, despite ambitious legislation, significant public pressure, and unprecedented Western support.[67] Meanwhile, while the Ukrainian army of 2020 compared with that of 2014 is indeed like a phoenix reborn from the ashes, some of its standards should still be improved. In 2018-2020, 77,000 contract officers, almost one-third of Ukraine's armed forces,

left the army.[68] Ukrainian authorities must make more of an effort to make Ukraine's armed forces a genuinely elite, mission-driven institution.

In addition, Ukrainian officials have not always managed the delicate balance between democratic freedoms and security, or communicated their intentions clearly. For example, Ukraine's security-motivated 2017 ban of the Russian social networks VKontakte and Odnoklassniki (prolonged in 2020 until 2023)[69] caught unawares some of its Western partners, who later criticized the move as an infringement on the freedom of speech.

All these missteps are certainly explainable. No state-building process can run perfectly, especially in a country which is a victim of hybrid aggression. However, it is important to bear in mind that any mistake made by officials could not only hurt the country, but also be exploited by the adversary. This, as well other chapters of Ukraine's experience, lay the productive ground for lessons to learn and examples to emulate.

ESTONIA

Kalev Stoicescu

Russia's non-conventional hybrid warfare against Estonia

Russia's use of hybrid war against Estonia has evolved in recent months and years, not least because these efforts differ from other theaters of operation, but because Estonia is a member of NATO and the European Union. Unlike in Ukraine, using force against Estonia would mean conflict between Russia and NATO. So the Kremlin would naturally wish to keep its moves against Estonia and other Baltic states under the threshold of NATO's Article V, unless Russia were already in open and direct military conflict with NATO or the United States elsewhere.

Estonia is not a weak state that Russia can relatively easily destabilize and manipulate. It is governed by the rule of law, the level of corruption and criminality are low, and it has no relevant pro-Kremlin political parties, politicians, and movements. Nor is it in a gray zone, as it is strongly anchored in the Western community and institutions. Again unlike some other countries in the neighborhood, Estonia's economy, including its energy industry, does not depend on Russia. The electric power grids of the Baltic states are in the process of separating from the Russian and Belarusian system,[70] and although Russia is Estonia's main supplier of natural gas, that is not unusual in the European Union.[71]

Besides, Europe's gas supply will diversify, and since Estonia pays the market price for its deliveries, Russia has little incentive to use one of its preferred methods, such as cutting off gas flows, to punish a lucrative customer. Russia tried only once to punish Estonia by switching off the gas in the early 1990s, but it realized quickly that the first to suffer were Russian-speaking people and households in North-East Estonia - exactly those the Kremlin arguably defended.

All of which means that Russia uses considerably different weapons in its hybrid war against Estonia than against Ukraine or Belarus. The Kremlin's efforts against Estonia are focused primarily on the country's less-integrated Russian speakers and Estonia's highly digitalized society. Russia backs these up with a steady military buildup and show of force in its Western Military District, which includes the Kaliningrad exclave to the west and borders Estonia to the east. Other tactics, such as massive money laundering through Nordic banks based in Estonia, are part of a much wider Russian pattern of using the West's weaknesses to its own advantage.[72] Massive flows of Russian money to European and off-shore banks - most of which are likely laundered considering the obscurity of the schemes and actors - serve not only the purpose of fulfilling the financial and personal interests of Russia's leaders and oligarchs, but also of feeding corruption and manipulating Western countries.[73]

Russia's non-conventional actions against Estonia have a long history, stretching back at least as far as a failed coup d'état attempt in Tallinn organized by the Soviet Union on December 1, 1924. Fifteen years later, the Soviet occupation and annexation of the Baltic countries in 1939-1940 finds echoes in Russia's seizure of Crimea in 2014.

Estonian soldiers get ready for the commemoration of the centennial of the War of Independence ceasefire near the border crossing point with Russia in Narva, Estonia January 3, 2020. REUTERS/Ints Kalnins.

The restoration of Estonia's independence in August 1991 began a new battle in the Kremlin's hybrid warfare against the country. Despite then-Russian President Boris Yeltsin's generally democratic sympathies, Russia tried mightily to thwart the Baltics' natural ambition to reunite with Europe and the trans-Atlantic community. The Kremlin repeatedly and falsely accused Estonia, since the early 1990s, on totally false grounds, of ethnic cleansing, "apartheid in white gloves" and the glorification of fascism.[74]

It became obvious in the 1990s that Russia was determined to discredit Estonia and attempted to prevent it from joining the EU and NATO, most notably by refusing to sign and enforce a border treaty negotiated and agreed by November 1996. Moscow also attempted to exploit friction between the country's titular ethnic group and its non-Estonian, mainly Russian-speaking, minorities and to use political, economic and military leverage to that end. Although the Kremlin did not manage to keep Estonia and the other Baltic states in its orbit, Vladimir Putin's rise and the consolidation of his autocratic rule signaled that relations between Russia and the West would sour and the hybrid warfare would not only continue, but would intensify.

Estonia is clearly an attractive target, even if not strategically important, for hybrid attacks as it is home to a community of Russian speakers, most of whom settled there during the Soviet years. However, the Russian speaking community is not homogeneous in terms of integration in Estonian society. Only a minority is made up of Russian-speakers who are not Estonian citizens and those who do not speak Estonian and are poorly integrated in

the society. This in turn decreases Russia's ability to influence the entire community.

Furthermore, the countries' official histories of Estonia's incorporation into the Soviet Union are still irreconcilably opposed. Moscow's hybrid attacks on Estonia and the other Baltic countries are also meant to show that these countries are liabilities to NATO and the European Union.

The military factor

Russia's aspirations to great-power status and "special rights" in its backyard rely primarily on its military might rather than the promise of prosperity, given that its economy is smaller, less dynamic, and less diversified than those of the United States, Europe, or China. That matters especially in the Nordic-Baltic region, where all of Russia's neighbors are members of NATO and/or the EU, and are economically more advanced.

While Russia is bulking up its military muscle on all fronts, its Western Military District has once again become, as in the Cold War, a clear priority. Russia's Kaliningrad exclave is increasingly militarized, including weapons of blackmail such as Iskander missile systems and likely tactical nuclear weapons, meant to put its unfriendly neighbors on notice. The Baltic states are virtually doubly covered by Russian A2/AD (Anti-Access and Area Denial) protective domes from Kaliningrad, as well as the Leningrad and Pskov oblasts. The Russian navy (Baltic fleet) and air force are very active in or above the Baltic Sea, often violating the maritime boundaries and air space of other countries, including Estonia, and bedeviling ships and aircraft of NATO countries.

Russia has recently conducted large snap exercises to gauge its combat readiness close to NATO territory. It also holds regular strategic-level exercises in its western reaches, including some with Belarus. The next large exercise will be Zapad 2021, probably in September.

As opposition protests continue in Belarus, formally an ally of Russia, President Aliaksandr Lukashenka may soon have no choice but to submit to certain demands from the Kremlin in order to maintain his grip on power, even including deployment of Russian forces to and use of air bases in Belarus. That would set alarm bells ringing for NATO and the Baltics, because the roughly 65-mile (105-kilometer) distance from southeastern Kaliningrad to northwestern Belarus happens to be the Lithuanian-Polish border across the Suwalki Gap.

With Russian troops at both ends, they would need only to cover a small stretch to meet in the middle and cut the Baltics off from their NATO and EU neighbors. Far from de-escalating, the Kremlin considers such military threats an effective political and psychological weapon against the West. The logic of a possible Russian aggression against the Baltic states is not necessarily, if at all, linked to them or the security situation in the Baltic and Nordic regions. It is about Russia willing to weaken and undermine NATO, and eventually use the opportunity to attack the weakest point in the Alliance's posture.

Lessons from the events of 2007

The history is a major subject of discord between Russia and Estonia. Estonia restored its independence in August 1991 under the principle of legal continuity with the prewar Republic of Estonia, which had been occupied and annexed by the Soviet Union in 1939-1940. Russia, however, still maintains that Estonia voluntarily joined the USSR.

That conflict, along with Russia's willingness to sow strife among Estonia's ethnic and linguistic groups, helps explain the Estonian government's decision in 2007

to move a "liberator" statue of a Red Army soldier from the city center of Tallinn to a nearby cemetery. It also helps explain the protests, riots, and Russian cyberattacks that followed the decision.

The events of the spring of 2007 revealed some truths about Estonian society, including that its Russian speakers were far from integrated into society, that official Russian propaganda could influence Estonia's Russian minority, and that Russia would not hesitate to meddle in Estonia's internal affairs given a chance.

Recent analyses, including by the International Centre for Defence and Security (ICDS) think tank in Tallinn, conclude that Russia prepared well in advance of the events, as the statue's removal was debated publicly for some time, and Moscow's moves were not at all spontaneous. Putin gave clear indications in his annual address to Russia's Federal Assembly in May 2006 (the course to militarization), and particularly in his speech at the Munich Security Conference in February 2007.[75]

Russia's likely first goal was to amplify the riots in Tallinn and provoke interethnic bloodshed, but the riots stopped after two nights of vandalism in the city center. Some smaller protests formed in other towns but were quickly dispersed. Russia did not achieve anything, considering that it likely expected international condemnation against Estonia.[76] A young Russian man was killed in the first night of riots, and although the police identified suspects in his beating, they never charged anyone in his stabbing death.[77] The Kremlin tried to use his death for its own purposes and to treat him like a martyr to Russophobia, to no real avail.

Potentially more damaging than the riots were Russian cyberattacks on Estonian state institutions, political parties, banks, and other organizations. The most important aspect of the April 2007 events were Russia's cyberattacks, as the Kremlin tried desperately to punish Estonia and put it on its knees. Hackers with the skills, coordination, and resources that suggested a state-sponsored campaign launched DDoS and defacement attacks over several weeks. Russian hackers, undoubtedly supported directly by the Russian state, considering the resources and coordination necessary for such massive cyberattacks, targeted web pages, and services of Estonian state institutions, political parties, commercial banks, and other entities (defacing and/or saturation/DDoS attacks).

Russia did not achieve, once again, its desired goals, in spite of prolonged cyberattacks during several weeks.[78] The result was shows of support from Estonia's allies and the international community while Russia refused to cooperate in the investigation and denied vehemently any state-level involvement. This practice of 'plausible deniability' is by now very well established – Russia continues to deny its direct role in e.g. the Ukrainian Donbas.

The Russian government pretended that it retaliated against Estonia by severely cutting the oil and other goods it sent through Estonian ports, mainly Muuga and Tallinn, ostensibly in retaliation for moving the soldier memorial. Later, it became clear that the redirection of much of Russia's maritime exports to the Russian ports of Ust-Luga and Primorsk, in the Gulf of Finland, was related not to the "Bronze Soldier" but to the business interests of members of President Putin's inner circle.[79]

The spring 2007 cyberattacks were a kind of turning point. Russia showed that it was willing and able to wage hybrid warfare, while Estonia became the first country to mount a successful cyber defense despite facing a massive, surprise attack and lacking much experience in the field. Estonia soon became home to NATO's Cooperative Cyber Defence Centre of Excellence (CCD CoE), which had been planned before the 2007 attacks but gained some urgency because of them.

Those attacks were also the center's first subject of analysis and research, and they provided lessons in strengthening cyber defenses. Apart from helping to prepare allied countries to counter even large, complex cyberattacks (in terms of offering know-how and training opportunities, including large and complex cyber exercises), the CoE also developed guidelines for applying international law in cases of cyberattack, which became known as the Tallinn Manual.[80]

Russia's principal tools of hybrid warfare against Estonia are undoubtedly its state-owned and specialized propaganda and disinformation channels.

In response, Estonia also strengthened its own national cyber defense and security capabilities, including the Information System Authority that was created in 2011 on the basis of efforts made since 2007. It entails strengthened coordination between ministries and state agencies through the Government's Office/Chancellery as well as provides substantially more resources for cyber security and defense and increased cooperation with the private sector). The country's volunteer Defence League formed a cyber unit to support government agencies and civilian organizations during cyberattacks and to raise general awareness about cyber security. The unit includes IT specialists, mostly from the private sector, who stand ready to mobilize quickly in support of civilian and military structures.[81]

Estonia, its allies, and Russia learned certain lessons from the events in April and May 2007. NATO and EU countries, particularly Estonia, took cyber defense more seriously. It became a top priority for civilian and military organizations. On the other hand, Russia probably learned that it is difficult to provoke widespread and violent ethnic conflict in Estonia, even when poking at sensitive issues. The ultimately unsuccessful Russian cyberattacks against Estonia showed that small states that might be vulnerable in conventional defense can punch above their weight in cyber defense.

Russian propaganda and disinformation in Estonia

Russia's principal tools of hybrid warfare against Estonia are undoubtedly its state-owned and specialized propaganda and disinformation channels. These include, as in the case of most other Western countries, the RT (formerly Russia Today) TV channel and the Sputnik news agency, news website, and radio broadcast (formerly Voice of Russia and RIA Novosti). These two Kremlin "news" brands, with nearly global reach and budgets that exceed the BBC's, are Russia's inverted versions of CNN and Voice of America/Radio Liberty. Just as the Moscow-led Eurasian Economic Union and the Collective Security Treaty Organization pretend to be analogs of and responses to the European Union and NATO.

Estonia has a fairly large non-ethnic Estonian, mainly Russian-speaking minority, who make up about 27% of the population. That, together with its history and its border with Russia, makes Estonia an attractive target especially for other Russian state-owned TV channels, including PBK (Pervyi Baltyiski Kanal – First Baltic Channel), NTV-Mir, RTR-Planeta and RenTV Estonia. PBK is the Baltic version of Russia's First Channel (Pervyi Kanal) where propaganda 'stars' like pro-Kremlin flame-thrower Dmitry Kiselyov and Vladimir Solovyov are almost as visible to Russian-speaking viewers in Estonia as to the Russian domestic public.

The Russian TV channels are usually part of large packages, including channels in Estonian, English and other languages, offered by Estonia's main internet and TV providers (e.g. Telia, Elisa, STV and others) in cooperation with intermediary companies (like the Latvian registered Baltijas Mediju Alianse and the Estonian Balti Autorite Levi Liit – Broadcast Union of Baltic Authors). In this way, Russian propaganda channels are part of almost every customer's TV package in Estonia. In 2018, they earned about €6 million from license fees (paid by all customers) and publicity/advertising.[82]

The other Russian channels, such as RTR Planeta and NTV Mir, in addition to the Baltic version of Pervyi Kanal, are influential among the Russian-speaking audience in Estonia. These major Russian networks will probably remain on Estonian cable TV as long as the service providers are not forced to drop them, and no political party in parliament, particularly the Centrists, is willing to discuss specific regulations and restrictions. Internet and cable-TV service providers claim that they are guided only by market economy and preferences of customers. The vast majority of Russian speakers in Estonia wish to watch television in their own language, but ETV+ *(see below)* cannot compete with Russia's TV channels in terms of resources and quality of programs.

ETV+

Estonian Public Broadcasting (ERR) launched a Russian-language television channel (ETV+) in September 2015 aimed at the country's Russian-speaking minority and airing news and entertainment.[83] ETV+ is not intended to compete with entertainment programs on Russian TV, but rather to provide local news that at least theoretically should be of interest to Russian speakers.

The channel's annual budget of about €5 million, staffing and productions are meager compared with those of the Russian channels. ETV+'s audience has grown during the COVID-19 pandemic to about 5 percent of Russian speakers, but, paradoxically, it is more popular with Estonian-language viewers who want to see how news is presented to the Russian-language public.[84] It remains to be seen whether ETV+ will be able to hold on to its newer Russian-speaking viewers.

RT and PBK

The government of Estonia has so far not followed Latvia and Lithuania in banning RT.[85] Those countries argued that RT is controlled through its parent company, Rossija Segodnya, by Kiselyov, who is on an EU sanctions list. For their unwillingness to act, Estonian officials cite the country's high ranking on Reporters Without Borders' World Press Freedom Index, even though RT, with its diet of pro-Kremlin agitprop and misinformation, hardly stands alongside mainstream journalism.[86]

Another reason might lie in the country's politics. Estonia's Centrist Party holds the offices of prime minister (Jüri Ratas) and Tallinn mayor (Mikhail Kõlvart), and it is probably loath to do anything that would lose it Russian-speaking (or any) voters. In any event, having been kicked out of neighboring countries, it could make sense for RT to tread lightly in Estonia, lest it leave a reluctant Tallinn no choice but to ban it.

Tallinn's City Council sponsored for many years a marginal channel called Tallinn TV that aired mostly the political platform of the Centrist Party under the guise of local news. The channel, with an annual budget of about €30 million, was 'restructured' recently for the official purpose of saving local taxpayers' money.[87] Undoubtedly also because the Centrist Party came out of the wilderness to lead the government in 2016 and continued as the leading party in a new coalition following parliamentary elections in March 2019.

However, the government of Estonia and Tallinn's City Council looked for alternatives to continue the transmission of Tallinn TV news in Russian through other channels to Russian speakers. Tallinn's mayor announced in April 2020 that the city had chosen PBK, although a plurality of Russian-speaking viewers had recently told pollsters they trust the public, Russian-language ETV+ channel more.[88]

The closure of Sputnik's office in Estonia

Sputnik's Tallinn office employed 35 people until it closed at the end of 2019.[89] The channel could no longer fund its operations because EU sanctions prevented Estonian banks from doing business with it. Like RT, Sputnik is part of Rossija Segodnya. Estonian banks did not accept operating Sputnik's accounts any longer, and the Russian propaganda channel could not pay salaries of employees or the rental space anymore.

Estonia's foreign minister, Urmas Reinsalu, said Sputnik's fate was down to sanctions and not its content.[90] The Russian government, however, called Estonia's action "political harassment" and vowed to retaliate.[91] Blogger Erkki Bahovski, a foreign policy expert at the ICDS, wrote that Sputnik's closure had "generated a little spat between Estonia and Russia as the latter accused Estonia of oppressing the press and violating the freedom of speech."[92] But Sputnik's status as "press" is a matter of debate.[93] Sputnik did not air views that dissented from its pro-Kremlin line, that its amateurish reports were anonymous, and that the channel had been exposed as running several Estonian-language Facebook pages under pseudonyms.

There is no direct and clear information about Russia's threatened retaliation, which most likely would have been the expulsion of Estonian journalists from Russia - but no Estonian journalists have worked in Russia since March 2020. Former correspondents for Estonian Broadcaster ERR and Postimees, a leading newspaper, have had trouble getting necessary visas or accreditations to work in Russia.

Sputnik's website in Estonia, which continues to operate, is an outlier among Russia's propaganda outlets in also offering content in the host country's language. Its popularity among Estonians is, however, questionable at best.

Propastop

In reaction to Russia's aggression against Ukraine in 2014 and the rising tide of Russian propaganda and disinformation, members of Estonia's volunteer Defence League launched the Propastop blog aimed at "cleansing Estonia of propaganda, false information and media lies," and shoring up the security of Estonia's information space.[94]

The blog spots and then marshals facts to refute false information about Estonia. In addition to helping the Estonian public better understand the Kremlin's techniques and motives, Propastop offers a comprehensive list of articles containing Russian propaganda and disinformation. It also appears in Russian, English, and German.

Russia has likely learned that many of Estonia's less-integrated Russian speakers, as well as some ethnic Estonians, regularly watch Russian state-owned TV channels. The Kremlin's tactic is probably to seek long-term gradual influence, filling the glass drop by drop instead of all at once and risking a reaction.

Russia's propaganda and disinformation find little purchase as long as Estonia's media remain free and its government and citizens are vigilant. The older Estonian population, with the experience of living in the former Soviet Union, well understands Russia's propaganda and its motives. Russia seeks to sow doubt among

A woman looks at the screens during the Locked Shields, cyber defence exercise organized by NATO Cooperative Cyber Defence Centre of Exellence (CCDCOE) in Tallinn, Estonia April 10, 2019. REUTERS/ Ints Kalnins.

Estonians about their government, liberal democracy, and the rule of law. As long as the country's people maintain some trust in their institutions and one another, that will be a losing battle.

Lessons learned from Estonia

At the moment, Estonia is not a primary target of Russian hybrid warfare. The Kremlin is preoccupied with other issues, including the continuing protests in Khabarovsk over the arrest of the governor there, the future of Belarus, the conflict in Nagorno-Karabakh, and Russia's proxy wars with Turkey in Syria and Libya. But the possibility always remains that Moscow could find it useful some time to stir the pot in the Baltics.

Russia can quickly re-train its propaganda and disinformation on Estonia or other Baltic states at any time, and if it did so, that would likely be a harbinger of some aggression against the region. For that reason, the Kremlin's official statements as well as its broadcasting bear permanent monitoring for signs of change, such as increased bellicosity, over the usual background noise of persistent and "normal" propaganda and disinformation.

And because the threat of military action is an inseparable part of Russia's hybrid warfare — and the possibility of fruitful dialogue with the Kremlin is remote — Estonia and its allies must continue to strengthen their deterrence and defense. But Russia's main weapons in its hybrid war against Estonia, as well as other NATO and EU countries, are propaganda and disinformation, as well as the use of cyberspace.

Estonia should take further steps against Russian state-owned channels that do not meet any professional definition of journalism and free media. Preferably, NATO and EU allies and partners could agree on broadcasting standards and steps to limit the spread of Russian propaganda and disinformation in the trans-Atlantic region. This is about defending common values and concerns as well as fighting Russian misuse of social media for politically subversive aims.

Cyber defense is a key aspect of Estonia's security. Russia has not launched a major cyberattack against Estonia since the events of 2007, but there is no reason to believe it won't again. Estonia's approach is to expose and attribute Russia's malicious activities not only in cyberspace, but also in espionage and other areas. Estonia's Western allies should follow its example, even at the risk of riling the Kremlin. Other Estonian examples worth following are the volunteer-run Defence League's cyber unit,[95] created to support state-run cyber defense and security organizations, and Propastop for countering Russian propaganda and disinformation.

The fight against Russian hybrid warfare, including propaganda and disinformation, is inherently asymmetric because Western governments cannot adopt Russia's behavior and tactics, and the openness of Western democratic societies makes them more hospitable to bad-faith actors and more vulnerable to misinformation than Russia's controlled information space. Western countries have to help their citizens become more aware of Russia's aims and hybrid tools, including its subversive propaganda and disinformation.

Finally, Russia's money laundering and export of corruption undermine Western countries and societies. It makes little sense or impact to counter only Russia's efforts in cyberspace and the media, or to try to limit European dependence on Russian energy without rooting out Russian money laundering and corruption.

UNITED KINGDOM

Precious Chatterje-Doody

The Evolution of Russia's Influence Attempts in the UK

Russia's strategic priorities for established international centers of power differ significantly from those that apply in countries within its cultural, geographic, or linguistic influence. What is more, different "permission sets" apply[96] — targeted military force cannot be used to back up psychological operations, for instance. In the United Kingdom, then, it is counterproductive to militarize Russia's specific activities as forms of hybrid or informational "warfare." This suits Russian interests by overplaying the state's capabilities[97] and exaggerating the coherence and control underlying processes and outcomes.[98] Successful policy responses, by contrast, must address a fundamentally messier reality.

Russia's main strategic priority for the U.K. can be summarized as cultivating an atmosphere conducive to increasing Russia's influence there — whether in absolute or relative terms. The main pillars of the strategy for achieving this objective are: infiltrating networks of social, economic, and political influence; promoting the destabilization of norm and value hierarchies, including in ways that create sympathy for Russian alternatives; and ensuring targeted informational and narrative support for specific Russian foreign policy priorities. In pursuing these "influence attempts" in the U.K., Russian state actors have used both targeted tactics and opportunistic interventions, while independent actors pursuing their own interests have also produced incidental benefits for the Russian state.

Russia's Political Influence Attempts in the UK

Throughout Russian President Vladimir Putin's leadership, Russia's approach to its activities in the U.K. has evolved in line with a broader strategic evolution combining foreign, military, and security policy; diplomacy; and informational/technical capabilities. From the promotion of positive representations of Russia to counter what was perceived as the West's information manipulation,[99] effective representation of Russia evolved into a national security concern.[100] A more confrontational approach ultimately emerged, of conceptually and practically undermining key institutions, mirroring what Russian political and military elites perceived "competitor" states in the West to be doing.[101] The practical implementation of such approaches also became more flexible and delegative.

Despite being strategically pragmatic, this flexibility and delegation mean that Russia's influence attempts in the U.K. suffer from an element of unpredictability due to a lack of direct control. These factors must be accounted for within policy responses to the three main forms of influence attempt: infiltrating networks of social, economic, and political influence; promoting the ongoing destabilization of norm and value hierarchies, including in ways that create sympathy for Russian alternatives; and providing targeted informational and narrative support for Russian foreign policy priorities.

1.1 Network infiltration

The Kremlin's strategy increasingly reflects the belief that efforts in the spheres of information, culture, and finance must be combined to successfully pursue foreign policy goals.[102] The U.K. offers many potential avenues for such combined efforts because its economic, cultural, political, and infrastructural networks have all been substantially infiltrated either by Russian state actors directly, or indirectly by self-interested actors who nonetheless may have informal or unofficial relationships with the Russian state.

Evidence from across Europe has shown the Russian state's support for anti-European Union (EU) and nationalist political parties.

Economic networks

Since the 1990s, the number of internationally mobile wealthy residents of Russian extraction with bases in London has grown steeply due to an investor visa scheme, favorable market and regulatory conditions, and the reputation of the U.K.'s judicial system.[103] Numerous business people with links to the Russian state have subsequently taken on the kind of cultural and media assets within the U.K. that can help to consolidate personal power and respectability,[104] including ownership stakes in Premier League soccer clubs and local and national media organizations.[105]

The links between Russian business, intelligence, and organized crime[106] have prompted concern within the British political establishment over whether state-linked Russian expatriates might wield nefarious influence across the U.K.'s political, media, and business sectors.[107] The factors that make London attractive to wealthy expatriates also enable illicit finance to be "recycled through what has been referred to as the London 'laundromat.'"[108] Interconnected industries of lawyers, accountants, estate agents, and PR agencies have developed around London's wealthy Russian diaspora, and the boundaries between legitimate, illegitimate, and state-linked business activities are not always clear. Companies that have fulfilled lobbying contracts for the Kremlin and for Kremlin-linked individuals wanted internationally on criminal charges have also made substantial donations to the U.K.'s ruling Conservative Party.[109]

Political networks

The unclear economic connections are concerning because the U.K. honors system enables economic and cultural assets to be easily converted into resources at the center of British political power, such as through appointments to the House of Lords. Numerous members of the U.K.'s House of Lords have business links to Russia, including positions on the boards of companies linked to the Russian state.[110]

Evidence from across Europe has also shown the Russian state's support for anti-European Union (EU) and nationalist political parties.[111] Central figures in the U.K.'s Leave.EU campaign met multiple times with the Russian ambassador to the U.K., denied receiving financial benefits,[112] but were investigated by the National Crime Agency due to unclarity over the sources of campaign finance.[113] Donors linked to Russia's Ministries of Defence and Finance, and energy industry (though acting in the capacity of private individuals) have also gifted millions of pounds to the Conservative Party, securing access to top politicians.[114]

Infrastructural networks

Russia benefits from well-developed cyber capabilities, which have been applied as part of a long-term program to accrue competitive advantage and shape opponents' decision architecture. This

includes infiltrating the networks that support Critical National Infrastructure (CNI), whether for espionage purposes or as a prelude to future attacks.[115] Several sectors of the U.K.'s CNI have been subject to such cyber intrusion.[116] Furthermore, during the investigation into the 2018 poisoning of former Russian-British double agent Sergei Skripal and his daughter in Salisbury, both the Foreign and Commonwealth Office (FCO) and the Defence Science and Technology Laboratory (DSTL) were targeted by phishing attempts orchestrated by the GRU, Russia's military intelligence service.[117] Cyberattacks are not necessarily conducted directly, sometimes involving collaboration between the Russian state and organized crime.[118]

However, while information on the efficacy of such activities in the U.K. is classified, cyber operations do not deliver outcomes in isolation. Since around 2016, Russian state actors have increasingly employed cyberattacks not to disrupt CNI, but to promote destabilization of democratic norms and values — mirroring what they see as the hostile practices of Western states.[119]

1.2 Norm and value destabilization

Western states have witnessed declining consensus around norm and value hierarchies since at least the 1990s,[120] and Russian state actors have actively supported this destabilization in the U.K. Founded in 2005, Russia's culturally focused international broadcaster, Russia Today, was transformed after the August 2008 Russo-Georgian war to produce more combative outputs that fulfilled the Kremlin's (2008) stated security objective of effective overseas representation, including through reporting Russian domestic state television's most extreme claim of an attempted "genocide" in Georgia.[121] The network's 2009 rebrand as RT encouraged viewers to "question more" what they were being told about world events.

Bolstered in the aftermath of the annexation of Crimea with the 2014 establishment of London-based RTUK and by Edinburgh and London branches of the new Sputnik international newswire and multimedia broadcaster, RT has provided enthusiastic support for Eurosceptic and nationalist movements in the U.K. Much of its content alleges the inequities and inadequacies of the European project;[122] the former Scottish National Party leader, Alex Salmond, fronts his own TV show; the U.K.'s highest-profile Eurosceptic, Nigel Farage, has been a frequent speaker; and rising support for Eurosceptic parties was emphasized prior to the 2019 European Parliament elections.

Cyber operations have also been employed to this end, including in the publication of thousands of Brexit-related tweets by several hundred (later suspended) accounts linked to the St. Petersburg, Russia-based troll farm, Internet Research Agency (IRA).[123] RT has also promoted extreme libertarian takes on the U.K.'s coronavirus response, challenging calls for collective action.[124]

The increased use of so-called hack-and-leak operations during international election campaigns has been a significant development over the past five or six years. These involve obtaining information and documentation sensitive to political parties via unsanctioned access, then leaking and amplifying them online.[125] The U.K. government concluded that Russia-linked actors almost certainly attempted to interfere in the U.K.'s 2019 general election in this way, but their impact (if any) remains unclear pending an ongoing criminal investigation.[126] Leaked content generally undermines both social values and the legitimacy of establishment institutions, which may be exacerbated by the strategic insertion of counterfeit documents.

Members of the military wear protective clothing as work continues on the home of former Russian spy Sergei Skripal in Salisbury, Wiltshire. The property is to be dismantled, with the roof completely removed by military teams in the wake of the Novichok attack as decontamination work continues. AP-Images via REUTERS.

As in the case of the 2016 U.S. presidential election, the amplification of hacked content tends to take place via complex networks. Some of these (e.g., partisan online message boards) may have no connection to the Russian state and be pursuing their own interests in amplifying such stories. Others (e.g., bot and troll activity) may be the subject of clandestine state coordination, but be limited in their effectiveness by financially motivated mutual amplification.[127] Some actors, like RT and Sputnik, have direct and open links to the Russian state. Their activities have been described in a general sense as "sowing doubt in Western media reporting (including information available to policy-makers)."[128] The amplification of hacked content is one means to attempt this.

A recent U.K. example concerns a 2018 cyberattack on the Integrity Initiative counter-disinformation program of the U.K.-based Institute for Statecraft. Funding and participant data (genuine and falsified) were released, then reported on by political bloggers, including some regularly featured on Russia's international broadcasters.[129] RT and Sputnik presented the initiative as a U.K. government-funded "anti-Russia crusade"[130] and an "information warfare effort run by British military intelligence specialists."[131] The hacked data were used to weave a story representing the U.K. government as the hypocritical perpetrator of exactly the kind of influence attempts of which it accuses Russia. This is consistent with both outlets' tendency to question dominant Western narratives about issues of international contestation, the sources and evidence upon which they are based, and the broader scope of purported Western norms and values.

1.3 Informational and narrative support for specific foreign policy priorities

Norm destabilization is a general approach to forging influence abroad, but specific foreign policy priorities also receive targeted support as they arise. The recalibration of Russia's international messaging (via RT's rebrand) prompted by the 2008 Russo-Georgian war was echoed following the 2014 military operations in the Donbas and Crimea, with RTUK and Sputnik launched the same year. Sputnik's slogan, "telling the untold," is coherent with Russia's intention for RT, of breaking "the Anglo-Saxon monopoly on ... global information streams."[132] Both outlets amplified the Russian political elite's contradictory narratives and denials around Crimea and the Donbas.

The aftermath of the 2018 Skripal poisonings shows how specific foreign policy priorities have been supported in the U.K. Both RT and Sputnik reported the case by quoting a range of Russian and British official sources, including mainstream media outlets, police, healthcare responders, and politicians.[133] This reporting charted real-world developments, but the interpretation of these developments relied heavily upon alternative commentators and analysts who did not routinely feature elsewhere, and whose expertise may not be widely acknowledged.

This "parallel commentariat" articulated "competing and often contradictory" narratives of the case,[134] which served Russia's strategic interests by calling into question the reliability of Western political and media institutions and Russia's culpability. This approach capitalized on low public trust in established political and media institutions, and the inherent uncertainties around the classified investigation.[135]

Previous assessments of RT by the U.K. media regulator, Ofcom, revealed that the network's broadcasting compliance is comparable to similar broadcasters, but that breaches (including significant ones) are mostly associated with programming about Russia's foreign policy.[136] Correspondingly, the post-Skripal poisonings period saw Ofcom announce multiple investigations into problematic programming, after which RT immediately moderated its reporting.[137] Ofcom ultimately ruled that seven of RT's programs had not maintained due impartiality or an adequate range of perspectives on this controversial matter and issued a substantial fine.[138]

A more engaged practice than this kind of selective representation, disinformation refers to the deliberate propagation of "false, incomplete, or misleading" information which is intended to "fuel confusion" and undermine the basis for rational debate.[139] The most egregious recent cases of its relevance in the U.K. also relate to the Salisbury poisonings. As this fast-moving and controversial news story developed, Russian politicians, ministries, and embassy social media accounts made many provocative claims. They were swiftly reported by U.K. mainstream media as well as by Sputnik and RT due to their inherent newsworthiness.

However, some statements were lies — as with Putin's claim that the suspects named in the Salisbury attack had been found and identified in Russia as private citizens. RT, Sputnik, and their counterparts in the British mainstream media[140] reported his claim, contributing — even inadvertently — to the spread of Russia's strategic disinformation, despite meeting expected standards of journalistic integrity. As with "hack-and-leak," disinformation amplification relies on circulation and interaction among multiple sources, within an overall environment of rapid-access information overload.

UK's Responses

The U.K.'s 2010 National Security Strategy was written in a context in which non-state threats appeared to have taken over as the primary security concerns, and so identified "no major state threat"[141] despite citing cyberattacks in the top tier of priority risks.[142] By the revision of the document in 2015, however, the resurgence of state-based threats was clear. The document included a small section dedicated to Russia, which had "become more aggressive, authoritarian and nationalist, increasingly defining itself in opposition to the West."[143] The strategy stressed the importance of international cooperation, with an understandable focus on the role of NATO in mitigating overseas military threats, including through a Readiness Action Plan, and investment, joint task forces, and air policing missions intended as deterrence measures.

While the "hybrid tactics and media manipulation" of the Crimea annexation were explicitly referenced,[144] Russia was not given any substantive attention in the discussion of overseas influence attempts in the U.K. Here the key focus was on cyber activities generally. A five-year, £1.9-billion program was announced to improve the U.K.'s cybersecurity capabilities commitment by increasing the U.K.'s defensive capability, deterring potential attacks, developing cyber defense technologies, and collaborating internationally.[145]

The collaborative focus was placed on the EU (as well as the United States) for the establishment of effective coordinated sanctions regimes for both financial and cyber transgressions, with a push for intelligence sharing and collaborative preemption in these areas. Beyond this, the government's lack of strategic foresight on the political extent of Russian influence attempts has been reflected in somewhat patchy responses across the target areas outlined below, and was subsequently criticized.[146]

2.1 Network infiltration

Economic networks

The national security threat posed by the potential for Kremlin-connected individuals to base corrupt assets in London was outlined by the Foreign Affairs Select Committee of the House of Commons in 2018, following which a Serious and Organised Crime (SOC) Group was set up within the Home Office. The committee advocated expanding sanctions to regime-connected individuals, while clearly linking sanctions relief to specific actions,[147] and sanctions expansion was subsequently facilitated in several ways. The Sanctions and Anti-Money Laundering Act (2018) allows for sanctions in the interest of national and international peace and security, and to further the U.K. government's foreign policy objectives. Unexplained Wealth Orders (UWOs) were introduced in 2018 to compel targets to reveal the sources of their wealth and are usually combined with asset freezes.

In 2020, the U.K. government announced a sanctions regime for human rights abuses (a U.K. Magnitsky Act).[148] There have been proposals to strengthen the powers of Companies House, the U.K.'s registrar of companies, and the law governing Limited Partnerships, while various registers have been created to record the overseas political interests of those entering the U.K. corporate, property, or government procurement arenas.[149] Despite the potential of this rapid succession of measures, their effectiveness is limited to safeguarding against future infiltration of economic networks. They will barely impact individuals with long-established financial interests in the U.K., of which even those of dubious origin now appear entirely legitimate.

Political networks

The publication in July 2020 of the *Russia* report by the U.K. Parliament's Intelligence and Security Committee raised concerns about how far Russian expatriates' economic infiltration could develop into political infiltration. The report advocates legislative measures to mitigate this threat.[150] The committee proposed stricter measures for declaring financial payments within the House of Lords (akin to those in force in the House of Commons), but the government's response referred to the Lords' existing Code of Conduct, passing responsibility to their Conduct Committee.[151]

The *Russia* report also proposed establishing a Foreign Agents Registration Act, similar to that in place in the United States. Such a register might be one viable means to record where those with longstanding financial interests in the U.K. are politically compromised, and research is currently underway into comparable registration schemes to identify whether and how such a system could be put in place in the U.K.[152]

In 2019, the Defending Democracy program was established to combine expertise from various government departments, security and intelligence agencies, and civil society in order to protect the U.K.'s democratic processes from interference, strengthen the integrity of elections, encourage and facilitate democratic participation, and promote fact-based discourse.[153] It produced proposals for a digital imprints scheme to ensure transparency around the producers of election materials.[154]

These measures are, however, compromised by a reluctance to learn from the past. Despite the Intelligence and Security Committee (2020) and the Department of Digital Culture, Media and Sport (DCMS) (2019) recommending an investigation into potential Russian influence on the EU referendum (Brexit), the government responded that "a retrospective assessment ... is not necessary"[155] because no evidence has been seen of "successful interference in the EU Referendum."[156] A cross-party group of members of Parliament is suing the government over its inaction, arguing that no evidence of interference has been found because "the government appeared not to have sought evidence."[157]

Infrastructural networks

Following the defense-and-deterrence approach and collaborative activity championed in the U.K.'s 2016 Cyber Security Strategy, a new National Cyber Security Centre (NCSC) was established to link up existing operations across GCHQ's information security arm, Communications-Electronic Security Group (CESG); the Centre for the Protection of National Infrastructure (CPNI); CERT-U.K. (Computer Emergency Response Team); and the Centre for Cyber Assessment (CCA).[158]

The U.K. and its allies have collaboratively named and shamed the GRU for various recent cyber activities, including those of hacker group APT28 (2018), the NotPetya attack (2018), and an attack on Georgia (2020).[159] Deterrence capabilities were further boosted with the introduction in 2019 of a new cyber sanctions regime in the U.K. and EU,[160] though it is too early to reliably ascertain its impact. Finally, the Law Commission is currently reviewing the Official Secrets Act with a view to better legislating for unsanctioned cyber access.[161]

2.2 Norm and value destabilization

The detection, deterrence, and defense components of the new cyber defense strategy are likely also to work well to combat hack-and-leak operations. As previously noted, however, it is the amplification of such information that gives it the power to destabilize societal norms and values by drawing into question

the legitimacy of key social institutions, the ideals they are based upon, and the extent to which they truly reflect such ideals. Multiple departments and agencies have, therefore, worked to counter the spread of harmful content in the on- and offline media environment. Initiatives specifically aimed toward biased narratives and disinformation are discussed in the subsequent section, but there are several that aim generally to mitigate the features of this environment that facilitate norm destabilization.

Following extensive investigations into the potential harms of the online environment, DCMS stated that it could not "stress highly enough the importance of greater public understanding of digital information—its use, scale, importance and influence."[162] The department pushed for digital literacy to be incorporated as a pillar of primary education, to be funded by a levy on social media companies.

Targeted action has been taken to combat state-backed disinformation in the U.K.

The current U.K. system already supports digital literacy objectives, which are one of the statutory duties of the media regulator, Ofcom,[163] and form part of the roles of the Information Commissioner's Office, the Electoral Commission, and the Advertising Standards Authority. While all four regulators have written separately about their roles in this arena, DCMS has recommended that the government ensure greater collaboration between them.[164]

Steps set out in proposals for an Online Harms framework (see further details below) included the publication of a media literacy strategy that facilitates critical engagement with online content.[165] Media literacy alone is unlikely to solve this problem, however, since it privileges individual responsibilities over structural safeguards.[166]

It is, therefore, notable that the government further committed that recommendations made in 2019 by the independent Cairncross Review[167] into the sustainability of high-quality journalism in the U.K. would inform its wider work on digital regulation. This included working toward new codes of conduct that redefine the relationships between news publishers and online platforms.[168]

2.3 Informational and narrative support for specific foreign policy priorities

Given Ofcom's relative success at regulating misleading or unduly partial media coverage,[169] the main concern around RT comes in the norm destabilization category. Despite concerns about the viral spread of some of its more biased content, there are questions over whether (and how) it can change news consumers' perceptions,[170] while the network skillfully spins criticisms into a selling point. This makes the continued transparent application of regulatory measures more strategically advisable than overtly political special treatment.

Further, targeted action has been taken to combat state-backed disinformation in the U.K., given disparities between different social networks' actions to stem state-led influence efforts. Stressing that social media companies had a "responsibility to comply with the law and not to facilitate illegal activity,"[171] DCMS noted a disjuncture between Facebook's ostensible commitment to transparency and its financial disincentives to effectively audit the sources of its advertising revenue.[172] It advocated increased government pressure, backed by financial penalties, to bring all platforms into line.[173]

These recommendations fed into the proposed regulations of the Online Harms

framework (under Ofcom's remit). In its December 2020 full response to the consultation on these proposals, the U.K. government set out the guiding principles for an Online Safety Bill, due to be ready later in 2021, which will impose on social media companies a duty of care regarding their users, while promoting a process-based, rather than content-focused, approach to addressing online harms.[174] DCMS also established a cross-Whitehall Counter-Disinformation Unit (CDU), connecting the counter-disinformation activities of DCMS, the Home Office, the FCO, and the Cabinet Office.[175] An assessment of these measures' efficacy can, however, only come in the fullness of time.

Conclusion

Russia's "influence attempts" in the U.K. are primarily aimed at creating favorable conditions to increase its influence thereby infiltrating networks of social, economic, and political influence; undermining dominant norm and value hierarchies (opening space for Russian alternatives); and providing targeted informational and narrative support for Russian foreign policy priorities.

Russia's approach to such activities has become increasingly flexible, capitalizing opportunistically on evolving social divisions and institutional failings. It has also become increasingly delegative, with the Russian state accruing incidental benefits from self-motivated independent actors not under its control.

This messy reality is hugely challenging for the U.K. to counter, but has only recently been reflected in U.K. policy responses. Despite the U.K. government acknowledging the "enduring and significant threat posed by Russia to the U.K. and its allies, including conventional military capabilities, disinformation, illicit finance, influence operations, and cyber-attacks,"[176] key response areas have suffered from a lack of strategic foresight: economic sanctions, money laundering, and unexplained wealth regimes have been implemented only very recently, and while welcome going forward, cannot combat preexisting network infiltration.

There has been a political reticence to investigate interference in the EU referendum, or to impose stricter regulation of political donations and interests. While cyber safeguards are moving in a promising direction despite constant technological developments, media safeguards are still being worked out through the U.K.'s legislative processes: foreign agent registration, amendments to the Official Secrets Act, and an Online Safety Bill remain pending. Russia's "influence attempts" will continue to take advantage of such opportunities.

EU/NATO

Oscar Jonsson

From Eastern Ukraine to Western Elections: Russian Operations against the EU and NATO

While Russian influence operations have a history that goes far beyond the concept of hybrid warfare, they have seldom gotten such attention. This chapter investigates the evolution of Russian hybrid means and the ends to which they are applied. The Russian leadership's best bet against the collective West is currently in these operations. The core of countering them lies in changing the Russian cost-benefit analysis that suggests, so far, that conducting these operations holds great rewards and carries fairly small risks.

Russian Goals and the Limits of Russian Power

At their foundations, the European Union (EU) and NATO are based on a political agreement that acknowledges mutual interests, security, and support. This is the focus of the conflict between Russia and the West (here shorthand for the EU and NATO). Russia stands little chance of prevailing in this conflict in the face of a committed and united West. Conversely, it has a great opportunity to succeed against a divided West. Unfortunately, many divisions exist that can be exploited. Fragmenting the West's political unity lies at the core of Russia's strategy as it seeks to promote economic ties with some European states — Germany and France — while isolating and provoking others. This paper focuses on Russian influence operations against both the EU and NATO as well as individual member states.

The Russian leadership's ability to achieve its goals — regime security and great power status through weakening the EU and NATO — comes from its power of destruction rather than its power of attraction. Russia has few true allies in the world. Even China, which shares an increasingly close relationship with Russia, cannot be considered an ally.[177]

The United States and Europe have seen increasing political polarization and decreasing trust in democracy over the past few decades.[178] Russia has sought to exploit this fact through its support for filliberal extremist actors and movements that are united in their opposition to the EU, NATO, or simply "the establishment."[179] This enables Russia to have a destructive influence over processes that are already contentious.

Elections and referenda, which, in essence, are processes to settle political contention, are particularly vulnerable. The core idea of popular votes is that even if one's own side does not win, one will accept the outcome as the process was free and fair. There is, therefore, an incentive for Russia to influence the outcome of these processes to sow doubt and create instability.[180] The European Parliament accurately summarized the goal of Russian cyber operations targeting the EU as: "distorting truths, provoking doubt, dividing Member States, engineering a strategic split between the European Union and its North American partners and paralyzing the decision-making process, discrediting the EU institutions and transatlantic partnerships ... undermining

and eroding the European narrative based on democratic values, human rights and the rule of law."[181]

Hammers: Russia's Hybrid Tools

While hybrid warfare is naturally a wide effort, the Russian way goes beyond a Western all-of-government approach to include organized crime, cyber privateers, and intelligence services with a global reach and impressive coordination. According to one estimate, there are at least six presidential administration departments and a series of presidential councils in Russia that are involved in the active measures campaign.[182] This shows both the variety of Russia's hybrid warfare and its impressive machinery for exercising control. It poses a particular challenge for the EU and NATO, which are carefully bound by their respective mandates divided into different domains. Moreover, different sectors within the EU and NATO have a hard time cooperating even in the best of circumstances, not to mention against an actor that uses everything from licit and illicit finance, hackers, media outlets, and intelligence services.

The information domain is the most important venue for hybrid warfare. The revolution in information and communications technology has been one of the most profound societal changes in a long time. Today, a large part of how we understand the world, power, and legitimacy is mediated through social media.[183] Therefore, "the process of collecting and organizing information is now a tremendous source of economic, political and cultural power."[184] This shift is, naturally, no secret to Russian strategists who have done their utmost to update their disinformation toolbox.

Russia's vulnerabilities in the information domain have been exposed on several occasions in the past. For example, Chechen separatists successfully used the internet in a propaganda war with the Russians during the Second Chechen War, Russia's image took a beating in the global media when it invaded Georgia in August 2008, and the Russian leadership was caught unaware by the pro-democracy Arab Spring in the Middle East and North Africa and the massive anti-government protests these uprisings inspired following the Russian elections in 2011. However, each failure was followed by adaptation and innovation: after the Chechen wars, Russia increased internet restrictions and surveillance; after the Georgian war, Russia's state-controlled television network, RT, extended its global reach to include Arabic, Spanish, and French audiences; and, after the Arab Spring, Russia expanded censorship of social media[185] (such as a new treason law that targets human rights activists and limits freedom on the internet).[186]

Russia's countermeasures were not limited to defense. Its offensive toolbox was enhanced as well. Following the Arab Spring and the concomitant protests in Russia, the first reports referring to the Internet Research Agency (IRA), the St. Petersburg-based troll farm, emerged.[187] The Russian leadership used the IRA to conduct an offensive against its domestic opponents (e.g., Russian opposition leader Alexei Navalny as early as 2013), but also international opponents (e.g., the United States' 2016 presidential election).[188]

While targeting the United States, Russia's strategy included running fake social media accounts pretending to be everything from alt-right voices to Black Lives Matter activists. The goal was to increase polarization and violence. Evidence of Russian meddling in the 2020 U.S. elections is now also emerging. A number of reports have described the use of fake Instagram accounts to discredit then U.S. presidential candidate Joseph R. Biden, Jr.[189] Moreover, the Russian disinformation machinery has sought to amplify the voices of QAnon, a conspiracy

Joint press statements by NATO Secretary General Jens Stoltenberg and the President of European Commission, Ursula von der Leyen ahead of a meeting with the College of Commissioners. December 15, 2020. Credit: NATO.

theory collective that believes that former U.S. President Donald J. Trump is the guardian against a coup and that Hillary Clinton and her allies are running sex-trafficking rings.[190]

The Russian disinformation machine often maintains a high degree of coherence across channels and regions in terms of key messages, but not always in delivery. This is to a large degree the result of coordination from the top by Dmitry Peskov, Russian President Vladimir Putin's press secretary. Peskov's weekly meetings with representatives of pro-Kremlin media outlets are combined with guidelines for social media farms and foreign embassies.[191] This is what allows for a high degree of coherence (although never flawless) between the different arms of the Kremlin machinery.

Another less noticed, but no less effective, way of pushing Russian narratives against the EU and NATO is evident in the Western Balkans. The Western Balkans are today at the front line between the EU and NATO on the one hand and Russia on the other. The states of the Western Balkans are on a steady, but slow, path to integration with the EU and NATO. Up until 2014, the Russian leadership did not seem to care too much about this, but after Russia invaded Ukraine that year its ambitions grew in the region. Montenegro, in particular, concluded association negotiations with NATO in May 2016 and joined the Alliance in June 2017. Coincidentally, Montenegro experienced an increase in cyberattacks both in terms of sophistication, but also in numbers, from 22 in 2012 to more than 400 in 2017.[192]

Russian leaders wanted to make an example of Montenegro for states pondering NATO membership. Around the time of the Montenegrin parliamentary elections on October 16, 2016, pro-NATO and pro-EU political parties as well as civil society groups and electoral monitors were targeted by large-scale distributed denial-of-service (DDoS) attacks. The cyberattacks were traced to APT28, also known as Fancy Bear, a hacking group with ties to Russia's military intelligence service, GRU.[193] There was also a coup attempt ahead of the elections that sought to topple the government and assassinate then-Prime Minister Milo Đukanović. The coup plotters were identified as GRU officers Eduard Shirokov (nom de guerre Shishmakov) and Vladimir Popov.[194] They were indicted in 2017 along with 12 other people with Russian, Serbian, and Montenegrin citizenship.[195]

The cyberattacks, intelligence operations, and subversion in Montenegro should be seen in conjunction with Russia's larger information offensive against the Western Balkans. A key instrument in that offensive has been Sputnik Serbia (*Srbija*), which has focused on providing pro-Russian, anti-EU, and anti-NATO narratives. Sputnik has been successful as it allows for free reproduction of its articles, which results in these articles being widely published by outlets with few resources.[196] In other words, Russian disinformation is successful not so much because of illegal methods, but rather because it exploits opportunities presented by the structural transformation, or crisis, in the media.

It is hard to assess the aggregated impact of this disinformation in the international domain, but some examples can be illustrating. For example, 42% of Serbians see Russia as their best partner and 14% the EU. This is the case even while Russian trade and aid to Serbia is just a fraction of that of the EU.[197]

The case of Montenegro provides a vivid example of the combination of offline and online tools used by Russia, and the Russian leadership's broader desire to undermine NATO and EU membership. By themselves, the cyberattacks or the information efforts might seem like minor nuisances, but the combination of these different tools is what makes them potent and gives them synergies.

As social media companies and governments get better at handling the crudest form of information influence, the Russian tactics have evolved. In Sweden, Sputnik published in 2015 a Swedish edition, but gave up after nine months because of low readership and influence.[198] That did not, however, stop the information offensive, but rather Russia updated its methods and targeted existing Swedish media. One example is how the Nordic's largest newspaper, Aftonbladet, published a story targeting a Swedish researcher as a member of British intelligence. The story was created from a (seemingly) GRU hack of the British Institute for Statecraft and then reported by Sputnik, RIA Novosti, and RT, after which Aftonbladet picked it up.[199] The story was clearly false and has been reprehended by the Swedish Press Ethical Committee. Influence operations through local and national media give a strong air of legitimacy that a Sputnik publication cannot have. Local and national media are, unfortunately, a fairly easy target.

Another shift is Russia's increasing use of fake portals in the information domain. In 2020, the IRA set up a fake left-wing news publication, PeaceData, staffed it with fake editors, and hired unwitting but legitimate freelance journalists. The angle of the reporting was "anti-war" and "abuse of power," and it focused on "appealing to left-wing voters and steering them away from the campaign of Democratic presidential candidate Joe Biden."[200] PeaceData contributors were asked to recruit more writers from among their contacts, thus increasing the perceived legitimacy of the operation. The scheme was exposed before it could

build a significant following (only 14,000 followers on Twitter), but it is a good example of innovation and adaptation. This example also underlines how "the old Soviet technique of infiltrating authentic social groups is being updated for the 21st century, obscuring the difference between real debate and external manipulation."[201]

Russia took a similar approach in France where two online portals — OneWorld.Press and ObservateurContinental.fr — spread disinformation surrounding the Covid-19 pandemic. The latter, for instance, alleged that NATO's Defender-Europe 20 exercises were to blame for the outbreak of Covid-19 in Europe. Both the portals had connections to InfoRos, which has ties to the GRU and, among other things, is physically located in the Russkiy Mir Foundation, a Russian-government funded instrument of soft power.[202]

The Russian operation in France mirrored a larger pattern of using the pandemic to spread disinformation about NATO. The pandemic created an urgent need for rapid information, which provided a fertile ground for disinformation campaigns. NATO detailed how it had detected coordinated disinformation campaigns against the presence of its troops in Latvia, Lithuania, and Poland. These campaigns included a fake letter, purportedly from NATO Secretary General Jens Stoltenberg to Lithuanian Defense Minister Raimundas Karoblis, stating that NATO was withdrawing its troops from Lithuania, and a fake interview that claimed Canadian troops had brought Covid-19 to Latvia.[203] NATO said Russian state-controlled media — Sputnik and RT — were instrumental in spreading this disinformation. Sputnik alleged that the coronavirus was being developed in U.S./NATO labs.[204] In each of the campaigns, NATO identified common techniques: forgeries, fake personas, falsehoods, amplification in fringe pro-Russian websites, and "language leap," where fabricated content leaps from its original source to English-language media.[205]

The cyber domain is another area which holds a lot of promise for a revisionist power like Russia to offset a more prosperous and superior West. Russia is skilled at combining the use of different domains of influence. It is a sophisticated cyber actor that has the "full range of capabilities for undertaking actions in cyberspace .... It implements a very advanced offensive program."[206] These capabilities were shown in Russia's interference in the 2016 U.S. presidential election and are a reminder that the most significant impact of its operations was not through fake social media accounts, but the hack-and-leak operation against the Democratic National Committee (DNC), which started with a cyber intrusion.[207] U.S. intelligence agencies concluded that the DNC hack sought "to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump."[208]

Following the exposure of its meddling, including by the Mueller report, Russia improved its modus operandi with increased operational security and more stealthy operations.[209] This included "a partly successful attempt to interfere, via hack-and-leak, in the French presidential elections of 2017 and almost certainly in the United Kingdom in 2019."[210]

Impact of Russian Influence Operations

The conduct of modern conflict is constantly developing with organizational and technological innovation, and through interactions with the participants. Russia's leadership has notably had a more difficult task as the world has become more aware of its nonmilitary influence since the 2016 U.S. presidential election. The

big technology companies — Facebook, Twitter, and Google — also seem to have woken up to the fact that they are key arenas for the information conflict, and have started to take countermeasures. On the other hand, hybrid warfare still favors the attacker as few costs are imposed. Moreover, the conditions for such warfare were particularly favorable during the Trump presidency and the higher demand for information in the pandemic.

It is critical to put Russian influence operations in perspective. It is incorrect to dismiss them as unsuccessful simply because both NATO and the EU are intact, or because many of the posts coming from the IRA have low viewership and low levels of interaction. In fact, Russia, starting from a limited power position, is attempting to impact the world's most powerful political union, the EU, and the world's most powerful military alliance, NATO, by using relatively cheap means.

Moreover, the aggregate impact of flooding the media with fake news is often bigger and more important than interactions with individual pieces of content. This can be seen in a study of the media landscape in Michigan in the lead up to the 2016 U.S. presidential election. It found that sensational and conspiratorial material as well as fake news was shared a lot more on social media than well-researched news, the proportion of well-researched news being shared was the lowest ever the day before the election, and that Trump-related hashtags by far surpassed Clinton-related ones.[211]

That being said, Russian disinformation attempts can hardly be so effective as Trump himself stating that it would be the most fraudulent election ever.[212] Nonetheless, it is lazy analysis to simply state that Trump was more harmful than foreign meddling as that is a false dichotomy. More correctly, the most effective influence operations have always been about exploiting existing divisions and local actors. For example, Trump

Russia is attempting to impact the world's most powerful political union, the EU, and the world's most powerful military alliance, NATO, by using relatively cheap means.

described Montenegro as "very aggressive" and said that defending it would lead to World War III.[213] The question is, where did those views originate? It is hard to believe that they originated from U.S. intelligence briefs. That narrative was only being pushed by the Russian disinformation machinery. This illustrates the fact that the impact of disinformation cannot merely be measured through Facebook interactions, it can also be seen in a president's comments that draw either directly from Russian sources or, more likely, from sources that are susceptible to Russian disinformation.

Even if Russian influence operations in 2016 did not sway a single voter, they sharpened the polarization in U.S. politics and society. This was manifested in the country being tied up for years in debates on the extent of collusion by the Trump campaign with the Russians and impeachment procedures.

The threat from Russian influence operations remains real, even though they are, by their very nature, unlikely to have an immediate or obvious impact. The EU and NATO are dependent on political support from their member states. In these states, there is some opposition to both institutions that can be amplified and exploited by malign Russian actors.

Lessons for the EU and NATO

Even before Election Day in the United States in 2016 it was clear to the Obama administration that Russia was trying to meddle in the outcome. When then-U.S. President Barack Obama met Putin he told him to "cut it out," but the Russian leadership did not.[214] In other words, U.S. deterrence failed. Obama was unsuccessful in conveying a credible "or else" to Putin. Similarly, French President Emmanuel Macron called Sputnik and RT "propaganda machines" to Putin's face at Versailles in 2017, but that, too, did little to stop Russian disinformation operations.

There has been much discussion about the ambiguity of disinformation operations. Much of it is exaggerated. Attribution is possible, albeit not immediate. U.S. sanctions that followed Russian election interference and other operations have targeted individual and low-level GRU operators, with their activities and duties clearly outlined.[215] This goes to show that attribution is not a major challenge. In fact, U.S. intelligence agencies have a good sense of who is doing what, but they have failed when it comes to deterrence.

The most immediate lesson for Western governments from the U.S. elections in 2016 was not to be quiet about Russian influence operations. The biggest benefit of exposing Russian operations is increasing public awareness of the threat and the determination to devote sufficient time and resources to countering it, which will in the long run change the cost-benefit calculus.[216] Moreover, Bellingcat's investigative journalism has served to expose Russian intelligence operations and has become a headache and source of embarrassment for the Russian leadership.

Nonetheless, "naming and shaming" should not be seen as sufficient for deterring Russian operations. After the U.S. elections in 2016, the poisoning of former Russian-British double agent Sergei Skripal in the United Kingdom in 2018, and the poisoning of Navalny in August 2020, it has become clear that the Russian leadership is not too worried about some of its high-profile operations becoming known to the public. On the contrary, the Skripal poisoning was intended to send a signal to other intelligence officers in Russia and also to the West. As "Putin and his inner circle appear to believe that they are in nothing less than a political war, [naming and shaming] will at best influence tactics, not strategy."[217]

With the Russian leadership committed to the idea that it is in a political war against the EU and NATO, more is needed than simply exposing its malign behaviors. So far, the Western approach has been to primarily rely on sanctions in lieu of stronger policy measures. Sanctions are an alternative to escalation. They satisfy the urge to "do something" rather than fix the underlying problem.[218] Moreover, inflicting economic pain is only effective to the extent that economic development is a priority for the Russian leadership. Nonetheless, it is demonstrably subordinate to regime security and great-power status.

The EU is responsible for the political response to the challenge from Russia, including sanctions, and has since 2014 taken a wide range of measures to increase preparedness against hybrid threats. These include creating sectoral strategies, establishing expert bodies (Hybrid Fusion Cell, Center of Excellence for Hybrid Threats), creating information-sharing mechanisms, conducting exercises and simulations, partnering with NATO, and increasing investments in cyber defense.[219] Most notably, the EU adopted an Action Plan against Disinformation[220] and set up an EU versus Disinformation initiative in 2015. In July 2020, the EU also imposed its first-ever sanctions (asset freeze and travel ban) in response to cyberattacks on

individual GRU officers and the responsible center at the GRU.[221]

These are all important steps to improve the infrastructure, but the core problem for the EU and NATO is still political and about unity. Both the EU and NATO have viewed Russian hybrid warfare as more of a nuisance than a fundamental challenge. NATO is primarily responsible for the military instrument, but also has a key role maintaining political unity. The lack thereof was evident when Macron called for a rapprochement with Russia in 2019 while failing to grasp the fact that Russian aggression is premised on the predictability of the West to always return to the negotiating table even though the fundamental problem has not been addressed.

Indeed, between Russia's invasion of Ukraine and Macron's call for better relations, Russia had not only impacted the U.S. and French elections, it had also used chemical weapons on NATO soil to try and assassinate Skripal, an attempt that resulted in the death of a British citizen.[222] Western actions have underlined that the West is unwilling to accept economic pain for geopolitical gain, in a failure to invest more into military and nonmilitary capabilities or impose tougher sanctions.

Governments alone cannot solve the problem of Russian influence operations. Big technology companies provide an important arena for these operations. These firms have come a long way since their 2016 laissez-faire approach to beefing up their defenses. Facebook is now more aggressive about taking down coordinated inauthentic behavior, Twitter has banned all political advertising, and Google, Facebook, and Twitter have signed onto the EU's Code of Practice, which sets a wide range of commitments, including transparency in political advertising and the closure of fake accounts. However, as methods for exposing disinformation are disclosed, Russian strategists will seek to circumvent them.[223] The task for the EU and NATO is Sisyphean.

Just days before the 2020 U.S. elections, the New York Post ran a story based on leaked (or fake) information against Biden. Twitter was quick to block the story, and Facebook posted warning labels next to it.[224] Regardless of the wisdom of those actions, it does show the increased awareness of the big social media companies that staying away from acting is not a strategy.

Russia is constantly adapting its hybrid warfare in response to its adversaries' actions and technological change. As automated bots and hack-and-leak operations are exposed, Russian operations have changed to create more organic-looking means of influence that blend international and domestic issues.

The key lesson for Russian strategists so far has been that their operations carry low costs and have potentially very high rewards. As long as this calculus remains in place, these operations will continue. The political unity of the West is fragile and already under great domestic strain — a reality that Russia seeks to amplify and exploit. The fundamental challenge for the West is maintaining political unity to counter Russian operations and successfully deter the most significant ones, including election meddling or the use of chemical weapons on NATO territory.

Many other operations, however, such as run-of-the-mill disinformation, cannot reasonably be deterred given the Russian leadership's conviction that it is in a political war with the West. Such operations will need to be countered with hardened defenses, public-private cooperation, and dedication.

CONCLUSION

Alina Polyakova and Mathieu Boulègue

The current Russian leadership has no incentive to dial back its efforts to undermine Western cohesion, especially since the assessment in Moscow is that these are largely succeeding. The West should, therefore, expect more, not less, tactical exploitation of the logics of chaos for the foreseeable future. Despite individual countries becoming more resilient to Russia's evolving hybrid warfare, as seen in the cyber arena in Estonia and to some extent, the United Kingdom, the problem remains that the broader Western alliance as a whole is still underprepared to cope with and respond effectively to Russian destabilization.

As a result, miscalculation and overreach by both sides in crisis scenarios are increasingly more likely and outcomes more unpredictable. Geopolitical competition will look less like a cold war and more like a constant barrage of violent episodes, low-threshold probes of Western readiness, and strategic deception and obfuscation of targets and intentions. Russia's resolve to engender global chaos could unintentionally lead to an escalatory cycle. This danger will be compounded by Russia's relentless effort to probe NATO's coherence and ability to defend its member states.

Without equal assessment and adaptation to Russia's evolving tactics of hybrid war, Western policies will become less effective over the long run. Despite growing sophistication in certain domains, such as cyber, Russian influence attempts are often messy and opportunistic, taking advantage of weaknesses within target states' systems.

Moscow has also shown itself to be effective at identifying and filling, with minimal resources, power vacuums left behind by Western, and in particular U.S., disengagement. Comprehensive measures to address these vulnerabilities should necessarily also restrict the potential entry points for Russian influence attempts.

A strategic policy approach should systematically consider the following three pillars of response.

Internal resilience

Societal resilience

Russia's destabilization efforts rely on highlighting inadequacies, inconsistencies, and hypocrisies in democratic societies. Chaos at home serves Russia's strategic interests that have long sought to equate democracies with chaos and authoritarianism with stability.

Combatting Russian hybrid warfare should start by taking the focus *off* Russia. As with addressing any state-based nefarious activities, building resilience starts at home by supporting wider societal resilience. The United States should lead the global community of democracies to champion democratic values and principles, and that starts with setting an example of democratic governance.

The United States, as home to some of the world's largest social media platforms, should lead the regulatory agenda to ensure that Russia and other malicious foreign states cannot exploit the public discourse of open societies. Russia pioneered state-sponsored information influence operations, but the problem is now far broader than Russia.

Russia's President Vladimir Putin, Defence Minister Sergei Shoigu and Chief of the General Staff of Russian Armed Forces Valery Gerasimov visit the firing range Donguz to oversee the military exercises known as «Centre-2019» in Orenburg Region, Russia September 20, 2019. Sputnik/Alexei Nikolsky/Kremlin via REUTERS.

To confront this reality, the United States should work closely with Europe to craft a regulatory agenda that prioritizes democratic values and principles when it comes to online content moderation, personal data use, and algorithmic transparency.

Furthermore, more stringent U.S. regulations need to be implemented in the financial system. Russian President Vladimir Putin's regime maintains control at home and wreaks havoc abroad by exploiting the international financial system to hide illicitly acquired funds. Reforming beneficial ownership regulation and closing other loopholes in financial systems is critical for blocking pathways that enable corruption.

Cyber resilience

The United States should invest more capabilities and training in cybersecurity threat mitigation. Russia's cyber capabilities have evolved to become increasingly sophisticated and far-reaching. The United States, and other Western allies, are not immune to cyberattacks — rather, Western countries are quickly becoming prime targets for Russian cyber operations. The 2020 SolarWinds hack, attributed to Russia, infiltrated more than 250 U.S. federal agencies as well as hundreds of U.S. companies.[225]

The 2018 U.S. cyber strategy opened the door for the United States to pursue offensive cyber capabilities.[226] U.S. Cyber Command (USCYBERCOM) should fully explore and carefully deploy these

capabilities to deter future cyberattacks by Russia.

In the longer term, the United States and Europe will need to work together to develop a cyber deterrence strategy vis-à-vis Russia and other state actors that seek to use cyber tools to attack critical infrastructure systems, steal sensitive national security data, and breach intellectual property rights. Such a strategy should set out clear parameters for engaging with adversarial states in the cyber domain, which should include an elaborate response framework that works to de-escalate confrontation between cyber superpowers.

Cognitive resilience

The fight against information manipulation — Russian or otherwise — and must continue through all demographics. It is of the utmost importance to offer future generations of information consumers the proper tools to decipher the informational environment. Comprehensive media literacy education is indispensable for a long-term defense against norm destabilization and disinformation. It provides a safety net as media practices evolve and should be woven into national curricula from an early stage.

In this regard, there are lessons that Western countries can learn from frontline states, such as Ukraine and Estonia, that have been targets of Russian information warfare for decades. Developing a critical lens for misleading or manipulative information as part of a broader civics education should be a priority in secondary education curricula.

Unity of endeavor

Reassess the nature of the 'Russia challenge'

After the end of the Cold War and the West's declaration of "victory" over the Soviet Union, Russia studies were quickly relegated to an unwanted dark art. Meanwhile, Russian military planners never stopped red teaming the West.

It is time to pay more attention to Russia studies. There is an urgent need for a better policy understanding of the evolution of Russian strategic thinking and its tactical applications. The U.S. government should increase support to public institutions, agencies, research centers, and think tanks working on Russia studies. This must be done by taking into consideration the diversity of national approaches to Russia, and the need to better coordinate expertise and policy in the United States and beyond.

Through more coordinated and calibrated policy, the goal should be to achieve a sense of unity in the West as regards the nature of the "Russia challenge." This could be achieved in the United States through increased engagement with European partners, fostered by the Biden administration. While it may be hard to achieve a common understanding, greater policy coherence with Western partners should be pursued.

In parallel, it is vital that the new U.S. administration does not relegate Russia affairs to the back burner or deprioritize them. The "Russia challenge" is here to stay and should not be overlooked as a consequence of the overarching necessity to address all things China.

Cooperation and support for allies

The United States cannot push back against Russia alone. It should spearhead more comprehensive links with partners and allies in order to calibrate not only policies but also effects.

Sharing best practices is critical in that regard, alongside increased coordination and support in countries targeted by Russian hybrid warfare. This could take the form of increased intelligence sharing,

return of experience, and lessons learned from successfully pushing back against Russian hybrid attacks, as well as specific cooperation programs between NATO allies — an effort the United States could lead.

Such an endeavor should also include coordination between responses that fall within the jurisdiction of crime-fighting agencies, intelligence and security services, and the relevant regulatory bodies. When a country is under the stress of Russian aggression, the international community should increase its level of direct support and solidarity.

Gray zone deterrence

Expose, attribute, and discredit Russian hybrid warfare operations

The Russian leadership hates surprises: there is space to explore asymmetric policy options that push back more actively against Russian hybrid operations. A priority for the United States should be to systematically and comprehensively expose, attribute, and discredit Russian operations — especially information manipulation operations and cyber operations — and even more so when they are unsuccessful.

The United States and its Western partners should agree on practical standards and steps directed at limiting the spread of Russian propaganda and disinformation. This is about defending our common values and concerns as well as fighting against Russian misuse of the information sphere for politically and socially subversive aims.

Move deterrence to the gray zone

Traditional frameworks of response to Russia's "chaos strategy" do not apply in the gray zone or against hybrid operations. It is, therefore, vital to invest more time and effort in pursuing asymmetric responses by using unconventional capabilities.

Russia should not be allowed to avoid responsibility for using nonlinear, ambiguous means. Quicker reaction times against Russian hybrid operations should be achieved by adapting legal and normative frameworks to gray zone deterrence in the United States. Asymmetric pushbacks should be encouraged without sacrificing values and ethical standards of operation.

For instance, the United States should use the full scope of sanctions authorities to target relevant entities, organizations, and individuals involved in the implementation of hybrid attacks aimed at destabilization and violation of sovereignty and territorial integrity of the United States and its Western allies.

Ultimately, the U.S. and Western response to Russia should have a desired end state in mind — namely, agree on what a "properly" behaving Russia would look like. While changing the strategic intent of the current Russian leadership is a useless endeavor, it might be possible to alter its cost-benefit calculus in the gray zone and force it to reconsider using hybrid tactics against the West.

Imposing costs for hostile action is necessary, but testing Russia's proverbial pain threshold should be done keeping in mind the potential for tactical errors and miscalculation.

Endnotes

1 Jensen, Donald N., and Doran, Peter B. 2018. "Chaos as a Strategy: Putin's "Promethean" Gamble." *Center for European Policy Analysis*, November, 2018, https://cepa.org/chaos-as-a-strategy/.

2 Inkster, Nigel. 2016. "Information Warfare and the US Presidential Election." *Survival*, 58 (5): 23-32, https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1231527.

3 "Lexicon for Russian Influence Efforts." *National Intelligence Council*, June, 16, 2017, and Giles, Keir. 2016. "Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power." *The Royal Institute of International Affairs, Chatham House*, March, 2016, https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power

4 Jensen, Donald N., and Doran, Peter B. 2018. "Chaos as a Strategy: Putin's "Promethean" Gamble." *Center for European Policy Analysis*, November, 2018, https://cepa.org/chaos-as-a-strategy/.

5 Gorenburg, Dmitry. 2019. "Circumstances Have Changed Since 1991, but Russia's Core Foreign Policy Goals Have Not." *PONARS Eurasia*, January, 2019, https://www.ponarseurasia.org/memo/circumstances-have-changed-russias-core-foreign-policy-goals-have-not.

6 Polyakova, Alina. 2018. "Weapons of the weak: Russia and AI-driven asymmetric warfare." *The Brookings Institution*, November, 15, 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

7 Jonsson, Oscar. 2019. *The Russian Understanding of War: Blurring the Lines between War and Peace*. Washington DC: Georgetown University Press, November, 2019.

8 Giles, Keir. 2016. "Russia's "New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power." *The Royal Institute of International Affairs, Chatham House*, March, 2016, https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power.

9 Gerasimov, Valery. 2013. "Noviye vyzovy trebuyut pereosmysleniya form i sposobov vedeniya boevykh deistviy. (New challenges require rethinking of the forms and methods of warfare)." *Voenno-promyshlenniy kur'er*, February 26,, 2013, https://www.vpk-news.ru/articles/14632

10 Galeotti, Mark. 2018. "I'm Sorry for Creating the "Gerasimov Doctrine"." *Foreign policy*, March, 5, 2018, https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

11 Renz, Bettina. 2016. "Russia and "hybrid warfare"." *Contemporary Politics*, 22 (2016): 283-30, DOI: 10.1080/13569775.2016.1201316, https://www.tandfonline.com/doi/abs/10.1080/13569775.2016.1201316.

12 Slipchenko, Vladimir. 2013. "Information Resource and Information Confrontation: their Evolution, Role, and Place in Future War." *Armeyskiy Sbornik (Army Journal)*, No. 10 (2013).

13 Chekinov, Sergey, and Bogdanov, Sergey. 2015. "A Forecast of Future Wars: Meditation on What They Will Look Like." *Voennaya Mysl' (Military Thought)*, No. 10 (2015), and Chekinov, Sergey, and Bogdanov, Sergey. 2014. "Military Futurology: Its Origin, Development, Role, and Place within Military Science." *Voennaya Mysl' (Military Thought)*, No. 8 (2014).

14 Kartapolov, Andrey. 2015 "Lessons of Military Conflicts and Prospects for the Development of Means and Methods of Conducting Them, Direct and Indirect Actions in Contemporary International Conflicts." *Vestnik Akademii Voennykh Nauk (Bulletin of the Academy of Military Science)*, No. 2 (2015).

15 Jensen, Donald N., and Doran, Peter B. 2018. "Chaos as a Strategy: Putin's "Promethean" Gamble." *Center for European Policy Analysis*, November, 2018, https://cepa.org/chaos-as-a-strategy/.

16 "Vektory razvitiya voyennoy strategii (Vectors of military strategy`s development)." *Krasnaya Zvezda*, March, 4, 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/.

17 Felgenhauer, Pavel. 2019. "A New Version of the "Gerasimov Doctrine"?" Jamestown Foundation, Eurasia Daily Monitor, vol. 16, no. 32, March, 7, 2019, https://jamestown.org/program/a-new-version-of-the-gerasimov-doctrine/.

18 Frolov, Vladimir. 2019. "Why Moscow Sent Its Military Personnel to Venezuela." *The Moscow Times*, April, 2, 2019, https://www.themoscowtimes.com/2019/04/02/why-moscow-sent-its-military-personnel-to-venezuela-a65052.

19 Polyakova, Alina. 2018. "Weapons of the weak: Russia and AI-driven asymmetric warfare." *The Brookings Institution*, November, 15, 2018, https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

20 Renz, Bettina, and Smith, Hanna. 2016. "Russia and Hybrid Warfare – Going Beyond the Label." *Aleksanteri Papers*, 1/2016. https://www.stratcomcoe.org/bettina-renz-and-hanna-smith-russia-and-hybrid-warfare-going-beyond-label.

21 Igor 'Strelkov' Girkin also admitted that the Novorossiya project was nothing more than propaganda and that the true goal was a Crimea-like takeover and not the establishment of an independent state.. See Chekalkin, Dmitry. 2014. "How Russia invaded Ukraine as told by FSB colonel Girkin." *Euromaidan Press*, December 7, 2014, http://euromaidanpress.com/2014/12/07/fsb-colonelgirkin-tells-details-of-how-russia-invaded-ukraine-in-twice-censored-interview/.

22 Jensen, Donald N. 2017. "Moscow in the Donbas: Command, Control, Crime and the Minsk Peace Process." NATO Defense College Research Report, March 1/17, 2017, https://www.ndc.nato.int/news/news.php?icode=1029.

23 "The occupation of Crimea: No markings, no names and hiding behind civilians." *Ukrainian Helsinki Human Rights Union*, 2019, https://helsinki.org.ua/en/publications/analytical-report-in-english-on-the-use-of-prohibited-methods-of-warfare-during-kremlin-s-occupation-of-crimea-in-february-march-2014-is-now-available/.

24 "Putin: Krym prisoyedinili, chtoby nye brosat' natsionalistam (Crimea was annexed so as not to abandon to nationalists)." *BBC Russian Service*, March, 9, 2015, https://www.bbc.com/russian/international/2015/03/150309_putin_crimea_annexion_film.

25 "Moskva: desantniki "sluchayno" pereshli granitsu Ukrainy (Moscow: paratroopers "accidentally" crossed the border of Ukraine)." *BBC-Russian Service*, August, 26, 2014, https://www.bbc.com/russian/international/2014/08/140826_russian_paratroopers_ukraine_reaction.

26 "Rebels without a Cause: Russia's Proxies in Eastern Ukraine." *International Crisis Group*, July, 16, 2019, https://www.crisisgroup.org/europe-central-asia/eastern-europe/ukraine/254-rebels-without-cause-russias-proxies-eastern-ukraine.

27 "SBU vylozhila dokazatelstva uchastiya "vagnerovtsov" v voyennyh prestupleniyah na Donbasse (SBU posted evidences of the participation of "Wagnerians" in war crimes in Donbas)." *Ukrinform*, May, 19, 2018, https://www.ukrinform.ru/rubric-ato/2463702-sbu-vylozila-dokazatelstva-ucastia-vagnerovcev-v-voennyh-prestupleniah-na-donbasse.html.

28 Both Ukrainian and Russian opinion leaders expressed those ideas. For example, one may read these messages in the following texts: Russia-sponsored portal *Ukraina.ru* about Poroshenko's interest in the war: "Ob`yavit` voynu, ne nachinaya: Rezhim Poroshenko podvel Ukrainu k opasnoy cherte (Declare war without starting: Poroshenko's regime has brought Ukraine to a dangerous line)." *Ukraina.ru*, December, 18, 2018, https://ukraina.ru/exclusive/20181218/1022111946.html; Ukrainian politician Vadim Novinskiy about the interest of the Government not to end the war: "Ni voyny, ni mira": Minskie soglasheniya chetyre goda spustya ("No war, no peace": Minsk agreements four years later)." *Segodnya*, February, 14 2019, https://politics.segodnya.ua/politics/ni-voyny-ni-mira-minskie-soglasheniya-chetyre-goda-spustya-1221510.html.

29 "Putin's friend emerges from shadows in Ukraine." *Financial Times*, April, 25, 2017, https://www.ft.com/content/0972792c-1e96-11e7-a454-ab04428977f9.

30 "Zolota sotnia: TOP-100 naybagatshih ukraintsiv (The Golden hundred: Top 100 the richest Ukrainians)." *NV Business*, October, 31, 2019, https://nv.ua/ukr/biz/markets/top-100-naybagatshih-ukrajinciv-reyting-nv-i-dragon-capital-novini-ukrajini-50050784.html.

31 Miller, Christopher. 2016. "Behind The Scenes In Ukraine, Ties To Putin Help Power Broker Pull Strings." Radio Free Europe, August, 24, 2016, https://www.rferl.org/a/ukraine-medvedchuk-putin-prince-darkness-gray-cardinal/27943679.html.

32 "Putin zaluchyv Medvedchuka do Minskogo protsesu cherez Merkel (Putin involved Medvedchuk in the Minsk process through Merkel)." *Espreso.TV*, July, 13, 2019, https://espreso.tv/news/2019/07/13/putin_zaluchyv_medvedchuka_do_minskogo_procesu_cherez_merkel_novyy_predstavnyk_ukrayiny_v_tkg_bezsmertnyy.

33 Mochan, Veronika. 2020. "Khto zainiav mistse Rosii: iak zminylasia zovnishnia torhivlia Ukrainy u 2019 rotsi (Who took Russia's place: how did Ukraine's foreign trade change in 2019?)." *Yevropeiska Pravda*, February, 3, 2020, https://www.eurointegration.com.ua/rus/articles/2020/02/3/7105833/.

34 Ukraine: the data. *World Bank*, https://data.worldbank.org/country/ukraine?view=chart.

35 Clark, Mason. 2020. "Russian Hybrid Warfare: Military Learning and The Future of War Series." *Institute for the Study of War*, September, 2020: 21, http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf.

36 Clark, Mason. 2020. "Russian Hybrid Warfare: Military Learning and The Future of War Series." *Institute for the Study of War*, September, 2020: 22, http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf.

37 "Riven doviry do sotsialnykh instytutiv i politykiv (Level of trust for the social institutions and politicians)." *Razumkov Center*, February, 2020, https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-diialnosti-vlady-riven-doviry-do-sotsialnykh-instytutiv-ta-politykiv-elektoralni-oriientatsii-gromadian-liutyi-2020r.

38 "Vlasnyk Newsone i 112 kupyv ische i telekanal ZIK (The owner of 112 and NewsOne also bought the Zik TV channel)." *Ukrinform*, June, 14, 2019, https://www.ukrinform.ua/rubric-society/2721693-vlasnik-112-ukraina-ta-newsone-kupiv-ise-j-telekanal-zik.html.

39 Solodkyy, Sergiy, 2016. "Ukraine's Foreign Policy Audit." *TRUMAN Agency, Institute of World Policy, INDEX OF RELATIONS, no. 2 (*October – December, 2016), https://truman.ua/sites/default/files/2018-02/Index%20of%20Relations%20%23%202.pdf.

40 Shtekel`, Myhaylo. 2017. "Pro "tretiy maidan" postiyno hovoriat v Rosii (About "third Maydan" is constantly talking in Russia)." *Radio Svoboda*, February, 17, 2017, https://www.radiosvoboda.org/a/28315050.html.

41 "Poll: nearly 60% of Ukrainians support EU accession, almost 50% – joining NATO." *UNIAN*, August, 13, 2020, https://www.unian.info/politics/ukraine-s-euro-atlantic-integration-poll-reveals-support-for-eu-nato-accession-11111945.html?_ga=2.234657950.1832883217.1611012326-1375065352.1611012326.

42 "Vladimir Putin's speech at the NATO summit (Bucharest, April 4, 2008)." *UNIAN*, April, 18, 2008, https://www.unian.net/politics/110868-vyistuplenie-vladimira-putina-na-sammite-nato-buharest-4-aprelya-2008-goda.html.

43 Veselova, Victoriya. 2016. "Iz SBU v FSB: kak slozhilis' sud'by krymskikh predateley (From the SBU to the FSB: how the fates of the Crimean traitors developed)." *Krym.Realii*, March, 23, 2016, https://ru.krymr.com/a/27631589.html.

44 "Probna viyna. 15 rokiv tomu Rosiya sprobuvala zakhopyty ukrayins" kyy ostriv Tuzla (The trial war. Fifteen years ago, Russia tried to capture the Ukrainian island Tuzla)." NV.ua, September, 29, 2018, https://nv.ua/ukr/ukraine/events/probna-vijna-15-rokiv-tomu-rosija-sprobuvala-zakhopiti-ukrajinskij-ostriv-tuzla-2496372.html.

45 "Why Crimea was not saved: transcript of the National Security and Defense Council of Ukraine." *Radio Svoboda*, February, 28, 2014, https://www.radiosvoboda.org/a/29794488.html.

46 E.g. Cătălin Alin Costea. 2019. "Russia's hybrid war in Ukraine (2014-2018)." *Foundation for Political, Economic and Social Research (SETA)*, 2019: 21-30.

47 Ibid.

48 Solodkyy, Sergiy, 2016. "Ukraine's Foreign Policy Audit." *TRUMAN Agency, Institute of World Policy, INDEX OF RELATIONS, no. 2 (*October – December, 2016), https://truman.ua/sites/default/files/2018-02/Index%20of%20Relations%20%23%202.pdf.

49 "Zatrymannia rosiiskoho shpyhuna v Kabmini: vsi podrobytsi (Detention of a "Russian spy" in the Cabinet: all the details)." *NV.ua*, December, 22, 2017, https://nv.ua/ukr/ukraine/events/zatrimannja-rosijskogo-shpiguna-v-kabmini-vsi-podrobitsi-2410148.html.

50 Interview of the authors at the Security Service of Ukraine. May, 2018.

51 "SBU: v 2019 rotsi neitralizovano pivtysiachi kiberatak na derzhavni orhany i krytychnu infrastrukturu (SBU: in 2019, half a thousand cyberattacks on government agencies and critical infrastructure were neutralized)." *Security Service of Ukraine*, January, 25, 2020, https://ssu.gov.ua/novyny/7030.

52 Solodkyy, Sergiy, 2019. "Ukraine-Russia relations." *TRUMAN Index*, no. 6 (January - March 2019), https://truman.ua/sites/default/files/2019-05/TRUMAN%20Index%20%236%2810%29.pdf.

53 "Russkiy mir" ta vybory v Ukraini: pro shcho hovoriat v Vkontakte ("Russian World" and Elections in Ukraine: What are they alking About in Vkontakt)." *Internews Ukraine*, November, 2018 – February, 2019, https://internews.ua/opportunity/vk-and-elections?fbclid=IwAR2ZHuFDZ8r0-UEvizELldZRjGILYJvvLNQo5JFw14SoOEBu3VSfm9nY5aM.

54 Solodkyy, Sergiy, 2019. "Ukraine-Russia relations." *TRUMAN Index*, no. 8 (July – September, 2019): 27, http://neweurope.org.ua/en/analytics/truman-index-12-ostanni-trendy-v-zovnishnij-politytsi/.

55 Kushnir, Mar`ian. 2018 "Rosiia kontsentruie viiska na kordoni z Ukrainou: iak davno? (Russia is concentrating troops on the border with Ukraine: for how long?)." *Radio Svoboda*, December, 10, 2018, https://www.radiosvoboda.org/a/text-rosia-koncentruie-viiska/29648121.html.

56 "Bezviz dlia Ukrainy - hromadska dumka (Visa-free regime for Ukraine - a public opinion)." *Ilko Kucheriv Democratic Initiatives Foundation*, June, 21, 2017, https://dif.org.ua/article/bezviz-dlya-ukraini-gromadska-dumka.

57 Remarks of the EUAM representative at the public event "The Eastern Partnership and Ukraine: looking back, thinking ahead", organized by the New Europe Center and the EU Institute for Security Studies on 25 February 2020 in Kyiv. For background reference: the EUAM was launched in 2014 in Kyiv as a response to the Russian aggression. However, its mandate only covered the civilian security institutions and back in 2014, field offices in the sensitive territories of Ukraine's East and South were out of the question.

58 "Z`iavyvsia svizhyi reitynh partii: konkurenty nazdohaniaiut sluh (A fresh poll has appeared: competitors are catching up with "servants")." *Ukrainska Pravda*, November, 12, 2020, https://www.pravda.com.ua/news/2020/11/12/7273288/.

59 "Povertav" Moldovi Prydnistrov'ia. Chym vidomyi Dmytro Kozak, yakyi teper vidpovidaie v Kremli za "ukrainskyi napriamok" ("Was returning" Transnistria to Moldova. What is known about Dmytro Kozak, who is now responsible in the Kremlin for the "Ukrainian direction")." *NV.ua*, February, 11, 2020, https://nv.ua/ukr/world/geopolitics/dmitro-kozak-zaminiv-surkova-na-donbasi-biografiya-novini-ukrajini-50069508.html?utm_content=set_lang&utm_medium=in_article&utm_campaign=langanalitics.

60 Butusov, Yuriy. 2020. "Zrada na samomu verkhu (Betrayal at the top)." *Censor.net*, August, 18, 2020, https://censor.net/ua/resonance/3214128/zrada_na_samomu_verhu_prezydent_zelenskyyi_zvilnyv_nachalnyka_gur_mo_burbu_za_vymogu_rozsliduvaty_proval.

61 Honchar, Mykhailo, Horbach, Volodymyr, and Savchenko, Serhiy. "Osin hibrydnoho nastupu. Operatsiia "cherez naradovladdia do federalizatsii" (Autumn of hybrid offensive. Operation "through the democracy to the federalization")." *Dzerkalo Tyzhnia*, October, 06, 2020, https://zn.ua/internal/osen-hibridnoho-nastuplenija-operatsija-cherez-narodovlastie-k-federalizatsii.html.

62 Kvien, Kristina. 2020. "Russian proxies and oligarchs block Ukraine's European integration." *Ukrainska Pravda*, November, 20, 2020, https://www.pravda.com.ua/eng/columns/2020/11/20/7274243/.

63 "NATO upgrades Ukraine." *Atlantic Council*, *UkraineAlert*, June, 16, 2020, https://www.atlanticcouncil.org/blogs/ukrainealert/nato-upgrades-ukraine/.

64 "Hague: Ukraina dovela pryinitanist spravy pro porushennia prav krymskykh tatar i ukraintsiv Rosiieu (Hague: Ukraine has proved the admissibility of the case of violation of the rights of Crimean Tatars and Ukrainians by Russia)." *Yevropeiska Pravda*, November, 8, 2019, https://www.eurointegration.com.ua/news/2019/11/8/7102823/.

65 Litra, Leonid, and Getmanchuk, Alyona. 2020. "One Year of Zelensky's Presidency: One Step Forward, One Step Back." *French institute of international relations*, October, 9, 2020, https://www.ifri.org/en/publications/etudes-de-lifri/russieneireports/one-year-zelenskys-presidency-one-step-forward-one.

66 "Poroshenko, Zelenskyi i NABU: mistse pid Sytnykom "zaminuvaly" sche do yoho pryznachennia (Poroshenko, Zelensky and NABU: the place under Sytnyk was "mined" even before his appointment)." *Deutsche Welle*, September, 9, 2020, https://www.dw.com/uk/poroshenko-zelenskyi-i-nabu-mistse-pid-sytnykom-zaminuvaly-shche-do-yoho-pryznachennia/a-54805259.

67 Bezuhla, Mar'iana. 2020. "Reforma popry opir: iak ta vsuperech chomu maie zminytysia Sluzhba Bezpeky Ukrainy (Reform despite resistance: how and in spite of why the Security Service of Ukraine should change)." *Yevropeiska Pravda*, December, 16, 2020, https://www.eurointegration.com.ua/articles/2020/12/16/7117688/.

68 Korba, Halyna. 2020. "Armiia na pauzi". Chy zalyshytsia ukrainske viisko bez izhi, zbroi i reform ("Army on Pause." Will the Ukrainian army be left without food, weapons and reforms?)." *BBC Ukraine*, October, 21, 2020, https://www.bbc.com/ukrainian/features-54485115.

69 Antoniuk, Daryna. "Ukraine prolongs ban on Russian websites VKontakte, Odnoklassniki until 2023." *KyivPost*, May, 16, 2020, https://www.kyivpost.com/technology/ukraine-prolongs-ban-on-russian-websites-vkontakte-odnoklassniki-until-2023.html?cn-reloaded=1.

70 "Lithuania's risk assessments different from those of Estonia and Latvia - Elering CEO." *The Baltic Times*, June, 30, 2020. https://www.baltictimes.com/lithuania_s_risk_assessments_different_from_those_of_estonia_and_latvia_-_elering_ceo/.

71 "Desynchronisation of Baltic power grids from Russia postponed." *ERR*, February, 5, 2019. https://news.err.ee/907644/desynchronisation-of-baltic-power-grids-from-russia-postponed.

72 Coppola, Frances. 2018. "The Banks That Helped Danske Bank Estonia Launder Russian Money." *Forbes*, September, 30, 2018. https://www.forbes.com/sites/francescoppola/2018/09/30/the-banks-that-helped-danske-bank-estonia-launder-russian-money/?sh=fd9ed6973197.

73 "London is not the place to launder Russian money, British minister says." *Reuters*, July, 22, 2020. https://www.reuters.com/article/us-britain-russia-moneylaundering-idUSKCN24N0OZ.

74 Barber, Tony. 1993. "Estonians accused of anti-Russian 'apartheid'." *Independent*, June, 24, 1993. https://www.independent.co.uk/news/world/europe/estonians-accused-of-antirussian-apartheid-1493666.html.

75 Putin, Vladimir. 2007. "Speech and the Following Discussion at the Munich Conference on Security Policy." *President of Russia*, February, 10, 2007. http://en.kremlin.ru/events/president/transcripts/24034.

76 Juurvee, Ivo, and Mattiisen, Anna-Mariita. 2020. "The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict." *International Centre for Defence and Security*, August, 21, 2020. https://icds.ee/en/the-bronze-soldier-crisis-of-2007/.

77 Cavegn, Dario. 2017. "Bronze Night's only death still unsolved." *ERR*, April, 26, 2017. https://news.err.ee/592217/bronze-night-s-only-death-still-unsolved.

78 "Cyber attacks against Estonia (2007)." *Cyber Law Toolkit*. https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007).

79 Ibid.

80 "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." *The NATO Cooperative Cyber Defence Centre of Excellence*, 2017. https://ccdcoe.org/research/tallinn-manual/.

81 "Estonian Defence League's Cyber Unit." *Estonian Defence League*. https://www.kaitseliit.ee/en/cyber-unit.

82 Ruussaar, Ainar. 2018. "Eesti vaataja maksab Kremli kanalitele ligi kolm miljonit aastas." *Postimees*, October, 21, 2018. https://www.postimees.ee/6434613/eesti-vaataja-maksab-kremli-kanalitele-ligi-kolm-miljonit-aastas.

83 "Estonia launches own Russian-language TV channel." *Deutsche Welle*, September, 28, 2015. https://www.dw.com/en/estonia-launches-own-russian-language-tv-channel/a-18747088.

84 Helme, Kristi. 2020. "ETV+ kahekordistas sel kevadel vaatajate arvu." *Eesti Päevaleht*, June, 4, 2020. https://epl.delfi.ee/artikkel/90069767/etv-kahekordistas-sel-kevadel-vaatajate-arvu.

85 Chadwick, Lauren. 2020. "Lithuania follows Latvia in banning Russian broadcaster RT." *Euronews*, July, 9, 2020. https://services.euronews.com/2020/07/09/lithuania-follows-latvia-in-banning-russian-broadcaster-rt.

86 "2020 World Press Freedom Index." *Reporters without borders*, 2020. https://rsf.org/en/ranking.

87 Pärnapuu, Priit. 2019. "KAART | Tallinn võidab TTV sulgemisega vähe." *Delfi*, September, 30, 2019. https://www.delfi.ee/news/paevauudised/eesti/kaart-tallinn-voidab-ttv-sulgemisega-vahe?id=87589749.

88 "Tallinn TV to broadcast news on Russian-language PBK." *ERR*, April, 1, 2020. https://news.err.ee/1071276/tallinn-tv-to-broadcast-news-on-russian-language-pbk.

89 "Sputnik ends operations in Estonia." *ERR*, January, 1, 2020. https://news.err.ee/1019231/sputnik-ends-operations-in-estonia.

90 "Reinsalu: Russia wants to use Sputnik to undermine EU unity." *ERR*, December, 27, 2019. https://news.err.ee/1018244/reinsalu-russia-wants-to-use-sputnik-to-undermine-eu-unity.

91 "Estonia claims 'foreign pressure' won't impact its push against Russian outlet Sputnik amid Moscow's complaints." *RT*, December, 27, 2019. https://www.rt.com/news/476946-sputnik-estonia-foreign-minister/.

92 Bahovski, Erkki. 2020. "Was Sputnik Eesti a trap?" *International Centre for Defence and Security*, January, 10, 2020. https://icds.ee/en/was-sputnik-eesti-a-trap/.

93 Ibid.

94 *Propastop*. https://www.propastop.org/eng/.

95 "Estonian Defence League's Cyber Unit." *Estonian Defence League*. https://www.kaitseliit.ee/en/cyber-unit.

96 Seely, Robert. 2017. "Defining Contemporary Russian Warfare." *The RUSI Journal*, vol. 162, no. 1: 50-59.

97 Renz, Bettina. 2016. "Russia and "hybrid warfare"." *Contemporary Politics*, vol. 22, no. 3: 283-300.

98 Szostek, Joanna. 2020. "What Happens to Public Diplomacy During Information War? Critical Reflections on the Conceptual Framing of International Communication." *International Journal of Communication*, vol. 14: 2728-2748, https://ijoc.org/index.php/ijoc/article/view/13439/0.

99 "National Security Concept of the Russian Federation." *Ministry of Foreign Affairs*, January, 10, 2000,https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768.

100 "Foreign Policy Concept of the Russian Federation." *President of Russia*, January, 12, 2008, http://en.kremlin.ru/supplement/4116.

101 Gerasimov, Valery. 2013. "Tsennost' nauki v predvidenii (The value of science in foresight)." *Voyenn -promishleny kurier*, February, 26, 2013, https://www.vpk-news.ru/articles/14632.

102 Pomerantsev, Peter, and Weiss, Michael. 2014. "The Menace of Unreality: How the Kremlin Weaponizes Information,

Culture and Money." *The Institute of Modern Russia*, *The Interpreter*, 2014, https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf.

103 Groskop, Viv. 2014. "How the Ukraine crisis is affecting Russians in Moscow-on-Thames." *The Guardian*, April, 6, 2014, https://www.theguardian.com/world/2014/apr/06/among-the-russians-in-london.

104 Schimpfossl, Elisabeth. *Rich Russians: From Oligarchs to Bourgeoisie*. Oxford University Press, 2018.

105 Foxall, Andrew. 2015. "The Kremlin's sleight of hand: Russia's soft power offensive in the UK." *Henry Jackson Society, Policy paper*, no. 3, https://henryjacksonsociety.org/wp-content/uploads/2019/01/HJS-The-Kremlins-Sleight-of-Hand-Report-NEW-web.pdf

106 Galeotti, Mark. *The Vory: Russia's Super Mafia*. Yale University Press, 2018.

107 "Russia." *Intelligence and Security Committee of Parliament*, 2020, https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl.

108 Ibid.

109 Thevoz, Seth, and Geoghegan, Peter. 2019. "Revealed: Russian donors have stepped up Tory funding." *openDemocracy*, November, 5, 2019, https://www.opendemocracy.net/en/dark-money-investigations/revealed-russian-donors-have-stepped-tory-funding/.

110 "Russia." *Intelligence and Security Committee of Parliament*, 2020: 16, https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl.

111 Hellman, Maria, and Wagnsson, Charlotte. 2017. "How can European States Respond to Russian information Warfare?" *European Security*, vol. 26, no. 2: 153-170, https://www.tandfonline.com/doi/abs/10.1080/09662839.2017.1294162 and Shekhovtsov, Anton. *Russia and the Western Far Right: Tango Noir*. Abingdon, Routledge, 2017.

112 "Leave.EU donor Arron Banks "must explain Russia link"." *BBC*, June, 10, 2018, https://www.bbc.co.uk/news/uk-politics-44428115.

113 "Disinformation and "fake news": Final Report." *House of Commons*, *The Digital*, *Culture*, *Media and Sport Committee*, February, 14, 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

114 Thevoz, Seth, and Geoghegan, Peter. 2019. "Revealed: Russian donors have stepped up Tory funding." *openDemocracy*, November, 5, 2019, https://www.opendemocracy.net/en/dark-money-investigations/revealed-russian-donors-have-stepped-tory-funding/.

115 Jensen, Benjamin, Valeriano, Brandon, and Maness, Ryan. "Fancy bears and digital trolls: Cyber strategy with a Russian twist." *Journal of Strategic Studies*, vol. 42, no. 2: 212-234, https://www.tandfonline.com/doi/abs/10.1080/01402390.2018.1559152?journalCode=fjss20.

116 "National Cyber Security Strategy 2016-2021." *HM Government*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

117 "Russia" *Intelligence and Security Committee of Parliament*, 2020: 16, https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl.

118 Ibid.

119 "Doktrina informatsiaonnoi bezopasnosti Rossiskoi Federatstii (The Doctrine of Information Security of the Russian Federation)." *The Ministry of Foreign Affairs of the Russian Federation*, December, 5, 2016, https://www.mid.ru/documents/10180/2563110/Ukaz_Prezidenta_Rossiiskoi_Federatsii_ot_05122016.pdf/b579d736-cb99-46ac-b4f7-a0b6bc102ed1.

120 Levitsky, Steven, and Ziblatt, Daniel. *How democracies die: What history tells us about our future*. Viking, 2018.

121 "We have evidence of genocide – Russian investigators." *RT*, August, 26, 2008, https://www.rt.com/news/we-have-evidence-of-genocide-russian-investigators/.

122 Chatterje-Doody, Precious N, and Crilley, Rhys. 2019. "Populism and contemporary global media: Populist communication logics and the co-construction of transnational identities." In *Populism and World Politics: Exploring Inter- and Transnational Dimensions*, edited by Stengel, Frank A., MacDonald, David B., and Nabers, Dirk. Palgrave Macmillan. 2019 and Crilley, Rhys, and Chatterje-Doody, Precious N. 2019. "Did Russia make Brexit promoter Nigel Farage a "YouTube star"?" *Washington Post*, March, 27, 2019, https://www.washingtonpost.com/politics/2019/03/27/did-russias-rt-make-nigel-farage-brexit-promoter-youtube-star/.

123 Chen, Adrian. 2015. "The Agency." *New York Times*, June, 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html and Llewellyn, Clare, Cram, Laura, Favero, Adrian, and Hill, Robin L. 2018. "Russian Troll Hunting in a Brexit Twitter Archive." *18th ACM/IEEE Joint Conference on Digital Libraries, Proceedings Association for Computing Machinery*, New York, NY, USA, 361–362, https://dl.acm.org/doi/10.1145/3197026.3203876

124 Hall, Natalie-Anne. 2020. "RT takes libertarian anti-lockdown stance." *Reframing Russia*, May, 19, 2020, https://reframingrussia.com/2020/05/19/rt-takes-libertarian-anti-lockdown-stance-guest-blog/.

125 Jamieson, Kathleen Hall. *How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know.* Oxford University Press, 2018.

126 "Russia." *Intelligence and Security Committee of Parliament*, 2020, https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl.

127 Keller, Franziska B., Schoch, David, Stier, Sebastian, and Yang, JungHwan. "Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign." *Political Communication*, vol. 37, no. 2: 256-280.

128 Giles, Keir. 2015. "Russia's Toolkit." In *The Russian Challenge*, *Chatham House report*, June, 2015: 57-64, https://www.chathamhouse.org/sites/default/files/field/field_document/20150605RussianChallengeGilesHansonLyneNixeySherrWoodUpdate.pdf.

129 Murray, Craig. 2018. "British Security Service Infiltration, the Integrity Initiative and the Institute for Statecraft." *Craig Murray*, December, 13, 2018, https://www.craigmurray.org.uk/archives/2018/12/british-security-service-infiltration-the-integrity-initiative-and-the-institute-for-statecraft/.

130 "Integrity Initiative: 'Anti-Russia crusade' funded by UK govt revealed." *RT*, December, 19, 2018, https://www.youtube.com/watch?v=T4X-cCZBWRc.

131 Klarenberg, Kit. 2018. "Integrity Initiative: Foreign Office Funded, Staffed by Spies, Housed by MI5?" *Sputnik*, December, 13, 2018, https://sputniknews.com/military/201812131070655802-integrity-initiative-intelligence-disinformation/.

132 "Visit to Russia Today television channel." President of Russia, June, 11, 2013, http://en.kremlin.ru/events/president/news/18319.

133 Tolz, Vera, Hutchings, Stephen, Chatterje-Doody, Precious N, and Crilley, Rhys. 2020. "Mediatization and journalistic agency: Russian television coverage of the Skripal poisonings." *Journalism*, July, 16, 2020. https://journals.sagepub.com/doi/10.1177/1464884920941967.

134 Ramsay, Gordon, and Robertshaw, Sam. 2018. "Weaponising news: RT, Sputnik and targeted disinformation." *King's College London*, *Centre for the Study of Media*, *Communication & Power*, March, 10, 2018, https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf.

135 Birge, Lucy, and Chatterje-Doody, Precious N. "Russian Public Diplomacy: Questioning Certainties in Uncertain Times." In *Public Diplomacy and the politics of uncertainty*, edited by Surowiec, Pawel, and Manor, Ilan. Palgrave Macmillan, 2021.

136 "Update on the RT service – new broadcasting investigations and approach to fit & proper." *Ofcom*, April, 12, 2018, https://www.ofcom.org.uk/__data/assets/pdf_file/0012/113043/rt-investigations.pdf.

137 Hutchings, Stephen, Chatterje-Doody, Precious N, and Crilley, Rhys. 2018. "Ofcom's Latest Ruling On RT Is More Significant Than You Might Think." *Huffington Post*, December, 21, 2018, https://www.huffingtonpost.co.uk/entry/ofcom-rt-bbc-latest_uk_5c1ce1b8e4b08aaf7a87c17c.

138 "Ofcom broadcast and on demand bulletin." Ofcom, no. 369 (December, 20, 2018), https://www.ofcom.org.uk/__data/assets/pdf_file/0020/131159/Issue-369-Broadcast-and-On-Demand-Bulletin.pdf.

139 Hellman, Maria, and Wagnsson, Charlotte. 2017. "How can European States Respond to Russian information Warfare?" *European Security*, vol. 26, no. 2: 153-170, https://www.tandfonline.com/doi/abs/10.1080/09662839.2017.1294162 and Shekhovtsov, Anton. *Russia and the Western Far Right: Tango Noir*. Abingdon, Routledge, 2017.

140 "Skripal poisoning: Putin says suspects "civilians, not criminals." *BBC*, September, 12, 2018, https://www.bbc.co.uk/news/world-europe-45494627 and Roth, Andrew, and Sabbagh, Dan. 2018. "Skripal poisoning: suspects are civilians, not criminals, says Putin." *The Guardian*, September, 12, 2008, https://www.theguardian.com/uk-news/2018/sep/12/skripal-poisoning-suspects-are-civilians-not-criminals-says-putin-novichok.

141 "A strong Britain in an Age of Uncertainty: The National Security Strategy." *HM Government*, October, 2010: 14-15, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf.

142 Ibid.

143 "National Security Strategy and Strategic Defence and Security Review 2015: A secure and prosperous United Kingdom." *HM Government*, November, 2015: 18, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf.

144 Ibid.

145 Ibid.

146 "Russia." *Intelligence and Security Committee of Parliament*, 2020, https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl.

147 "Moscow's Gold: Russian Corruption in the UK: Government response to the Committee's Eighth Report (HC 932)." HM Government, May, 21, 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/1488/148802.htm.

148 "The Global Human Rights Sanctions Regulations 2020." *HM Government*, *UK Statutory Instruments No. 680*, 2020, https://www.legislation.gov.uk/uksi/2020/680/contents/made.

149 "Russia." *Intelligence and Security Committee of Parliament*, 2020, https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl and "Moscow's Gold: Russian Corruption in the UK: Government response to the Committee's Eighth Report (HC 932)." *HM Government*, May, 21, 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmfaff/1488/148802.htm.

150 Ibid.

151 "Government Response to the Intelligence and Security Committee of Parliament Report "Russia"." *HM Government*, July, 2020: 17, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf.

152 Ibid.

153 Ibid.

154 Ibid.

155 Ibid.

156 Ibid.

157 Devlin, Kate. 2020. "Cross-party group of MPs to sue government over alleged failure to investigate Russian interference in UK elections." *The Independent*, October, 29, 2020, https://www.independent.co.uk/news/uk/politics/mps-lawsuit-russia-interference-uk-elections-b1403806.html.

158 "National Cyber Security Strategy 2016-2021." *HM Government*, November, 2016: 29, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

159 "Government Response to the Intelligence and Security Committee of Parliament Report "Russia"." *HM Government*, July, 2020: 7-8, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf.

160 Ibid.

161 Ibid.

162 "Disinformation and "fake news": final report." *Digital, Culture, Media and Sport Committee*, February, 18, 2019: 85, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179104.htm.

163 Ibid.

164 Ibid.

165 "Government Response to the Intelligence and Security Committee of Parliament Report "Russia"." *HM Government*, July, 2020: 14, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf.

166 Reilly, Paul. 2019. "Antidote or Placebo? Digital Literacy and the Global Fight Against "Fake News"." *Global Policy*, April, 17, 2019, https://www.globalpolicyjournal.com/blog/17/04/2019/antidote-or-placebo-digital-literacy-and-global-fight-against-fake-news.

167 Cairncross, Dame Frances. 2019. "The Cairncross Review: A sustainable future for journalism", Department for Digital, Culture, Media & Sport, UK Government, February, 12, 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf

168 "Government response to the Cairncross Review: a sustainable future for journalism." HM Government, Department for Digital, Culture, Media & Sport, January, 27, 2020, https://www.gov.uk/government/publications/the-cairncross-review-a-sustainable-future-for-journalism/government-response-to-the-cairncross-review-a-sustainable-future-for-journalism.

169 Hutchings, Stephen, Chatterje-Doody, Precious N, and Crilley, Rhys. 2018, Ibid.

170 Crilley Rhys, Gillespie, Marie, and Willis, Alistair. 2019. "Tweeting the Russian revolution: RT's #1917LIVE and social media re-enactments as public diplomacy." *European Journal of Cultural Studies*, October, 5, 2019: 23, https://journals.sagepub.com/doi/10.1177/1367549419871353 and Fisher, Aleksandr. 2020. "Demonizing the enemy: the influence of Russian state-sponsored media on American audiences." *Post-Soviet Affairs*, vol. 36, no. 4: 281-296, https://www.tandfonline.com/doi/abs/10.1080/1060586X.2020.1730121.

171 "Disinformation and "fake news": final report." *Digital, Culture, Media and Sport Committee*, February, 18, 2019: 75, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179104.htm.

172 Ibid.

173 Ibid.

174 "Online Harms White Paper: Full Government Response to the consultation." *HM Government*, December 2020, Ref: CP 354, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf.

175 "Government Response to the Intelligence and Security Committee of Parliament Report "Russia"." *HM Government*, July, 2020: 13, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902342/HMG_Russia_Response_web_accessible.pdf.

176 Ibid.

177 Kofman, Michael. 2020. "The Emperors League: Understanding Sino-Russian Defense Cooperation." *War on the Rocks*, August, 6, 2020, https://warontherocks.com/2020/08/the-emperors-league-understanding-sino-russian-defense-cooperation.

178 Foa, Roberto Stefan, and Mounk, Yascha. 2017. "The Signs of Deconsolidation." *Journal of Democracy,* January, 2017, vol. 28, no. 1: 5-16.

179 Shekhovtsov, Anton. 2017. "Foreign Politicians' Visit to Crimea Is Russia's Latest Disinformation Failure." *The Moscow Times*, March, 29, 2017, https://www.themoscowtimes.com/2017/03/29/foreign-politicians-visit-to-crimea-is-russias-latest-disinformation-failure-a57569.

180 Limnell, Jarno. 2018. "Russian Cyber Activities in the EU." In "*Hacks, leaks and disruptions: Russian cyber strategies*" *edited by Popescu, Nicu, and Secrieru, Stanislav, The European Union Institute for Security Studies*, October, 23, 2018, https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-%E2%80%93-russian-cyber-strategies.

181 "European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties." *European Parliament*, November, 23, 2016, https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html.

182 Galeotti, Mark. 2017. "Controlling Chaos: How Russia manages its political war in Europe." *European Council on Foreign Relations*, September, 1, 2017, https://www.ecfr.eu/publications/summary/controlling_chaos_how_russia_manages_its_political_war_in_europe.

183 Jonsson, Oscar, Campanella, Edoardo, and Owen, Taylor. 2020. "The New Digital Domain. How the Pandemic Reshaped Geopolitics, the Social Contract and Technological Sovereignty." *Center for the Governance of Change*, https://www.ie.edu/cgc/research/new-social-contract-digital-age/.

184 Smyth, Sara M. 2019. "The Facebook Conundrum: Is it Time to Usher in a New Era of Regulation for Big Tech?" *International Journal of Cyber Criminology*, vol. 13, no. 3: 578-595, https://www.cybercrimejournal.com/SmythVol13Issue2IJCC2019.pdf.

185 Soldatov, Andrei, and Borogan, Irina. 2015. *The Red Web: The Kremlin's War on the Internet*, 149-74. Washington, DC: PublicAffairs.

186 "Russia: Internet Legislation Merits Greater Scrutiny Before Passage." *Human rights watch*, July, 11, 2012, https://www.hrw.org/news/2012/07/11/russia-internet-legislation-merits-greater-scrutiny-passage.

187 Garmazhapova, Aleksandra. 2013. "Gde zhivyt trolli. I kto ix kormit (Where the trolls live. And who feeds them)." *Novaya Gazeta*, September, 9, 2013, http://novayagazeta.spb.ru/articles/8093/.

188 Mueller, Robert S. 2019. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election." *U.S. Department of Justice*, March, 2019, https://www.justice.gov/storage/report.pdf.

189 Francois, Camille, Nimmo, Ben, and Eib, C. Shawn. 2019. "Russian Accounts Posing as Americans on Instagram Targeted Both Sides of Polarizing Issues Ahead of the 2020 Election." *Graphika*, October, 21, 2019, https://graphika.com/reports/copypasta/.

190 Menn, Joseph. 2020. "Russian-backed organizations amplifying QAnon conspiracy theories, researchers say." *Reuters*, August, 24, 2020, https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T.

191 Galeotti, Mark. 2019. *Russian Political War: Moving Beyond the Hybrid*. Abingdon: Routledge.

192 Tomovic, Dusica, and Zivanovic, Maja. 2018. "Russia's Fancy Bear Hacks its Way into Montenegro." *Balkan Insight*, March, 5, 2018, http://www.balkaninsight.com/en/article/russia-s-fancy-bear-hacks-its-way-into-montenegro-03-01-2018.

193 Hacquebord, Feike. 2018. "Update on Pawn Storm: New Targets and Politically Motivated Campaigns." *Trend Micro*, January, 12, 2018, https://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns.

194 Garcevic, Vesko. 2017. "Congressional Testimony to Committee on Senate Select Intelligence," June, 28, 2017. https://www.intelligence.senate.gov/sites/default/files/documents/sfr-vgarcevic-062817b.pdf

195 Bechev, Dimitar. 2018. "The 2016 Coup Attempt in Montenegro: Is Russia's Balkans Footprint Expanding?" *Foreign Policy Research Institute*, April, 2018, https://www.fpri.org/article/2018/04/the-2016-coup-attempt-in-montenegro-is-russias-balkans-footprint-expanding/.

196 Jonsson, Oscar. 2018. "The next front: the Western Balkans." In "*Hacks, leaks and disruptions: Russian cyber strategies*" *edited by Popescu, Nicu, and Secrieru, Stanislav, The European Union Institute for Security Studies*, October, 23, 2018, https://www.iss.europa.eu/content/hacks-leaks-and-disruptions-%E2%80%93-russian-cyber-strategies.

197 "Moscow is regaining sway in the Balkans." *The Economist*, February, 25, 2017, https://www.economist.com/news/europe/21717390-aid-warplanes-and-propaganda-convince-serbs-russia-their-friend-moscow-regaining-sway.

198 Kragh, Martin, and Åsberg, Sebastian. 2017. Russia s Strategy for Influence through Public Diplomacy and Active Measures: The Case of Sweden." *Journal of Strategic Studies*, vol. 40, no. 6.

199 Kragh, Martin. 2020. Martin Kragh är ett demokratiskt problem (Martin Kragh is a democratic problem). *Statsvetenskaplig Tidskrift*, vol.122, no. 3: 419-447, https://journals.lub.lu.se/st/article/view/22141.

200 Wanless, Alicia, and Walters, Laura. 2020. "How Journalists Become an Unwitting Cog in the Influence Machine." *Carnegie Endowment for International Peace*, October, 23, 2020, https://carnegieendowment.org/2020/10/13/how-journalists-become-unwitting-cog-in-influence-machine-pub-82923.

201 Polyakova, Alina, and Fried, Daniel. 2019. "Europe is starting to tackle disinformation. The US is lagging." *Washington Post*, June, 17, 2019, https://www.washingtonpost.com/opinions/2019/06/17/europe-is-starting-tackle-disinformation-us-is-lagging/?utm_term=.ac9f08609112.

202 "How two information portals hide their ties to the Russian News Agency Inforos." *OSINT Investigation*, *EU DisinfoLab*, June, 2020, https://www.disinfo.eu/wp-content/uploads/2020/06/20200615_How-two-information-portals-hide-their-ties-to-the-Russian-Press-Agency-Inforos.pdf.

203 "NATO's approach to countering disinformation: a focus on COVID-19." *The North Atlantic Treaty Organization*, July, 17, 2020, https://www.nato.int/cps/en/natohq/177273.htm#case.

204 Ibid.

205 Ibid.

206 Świątkowska, Joanna. 2020. "Offensive Actions in Cyberspace – A Factor in Shaping Geopolitical Order." in Albrycht, I (ed) et al., *Geopolitics of Emerging and Disruptive Technologies*, Krakow: The Kosciuszko Institute. https://ik.org.pl/wp-content/uploads/geopolitics-of-emerging-and-disruptive-technologies-2020.pdf

207 Rid, Thomas. 2016. "How Russia Pulled Off the Biggest Election Hack in U.S. History." *Esquire*, October, 20, 2016, https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/.

208 "Assessing Russian Activities and Intentions in Recent US Elections." *Office of the Director of National Intelligence*, January, 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

209 Rid, Thomas. 2020. "Insisting that the Hunter Biden laptop is fake is a trap. So is insisting that it's real." *Washington Post*, October, 24, 2020, https://www.washingtonpost.com/outlook/2020/10/24/hunter-biden-laptop-disinformation/.

210 Ibid.

211 Howard, Philip N., Bolsover, Gillian, Kollanyi, Bence, Bradshaw, Samantha, and Neudert, Lisa-Maria. 2017. "Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?" *The Project on Computational Propaganda*, *Oxford Internet Institute*, March, 26, 2017, https://comprop.oii.ox.ac.uk/research/posts/junk-news-and-bots-during-the-u-s-election-what-were-michigan-voters-sharing-over-twitter/.

212 Spocchia, Gino. 2020. "Trump says 2020 will be 'one of greatest, most fraudulent elections ever." *The Independent*, October, 9, 2020, https://www.independent.co.uk/news/world/americas/us-election/trump-2020-election-fraud-biden-fox-hannity-mail-ballots-voter-id-b908650.html.

213 Sampathkumar, Mythili. 2018. "Trump says defending "aggressive" Montenegro as a NATO member 'will lead to World War III." *The Independent*, July, 18, 2018, https://www.independent.co.uk/news/world/americas/us-politics/donald-trump-nato-montenegro-world-war-mutual-defence-a8453446.html.

214 Nelson, Louis. 2016. "Obama says he told Putin to "cut it out" on Russia hacking." *Politico*, December, 16, 2016, https://www.politico.com/story/2016/12/obama-putin-232754.

215 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks." *US Department of Treasury*, March, 15, 2018, https://home.treasury.gov/news/press-releases/sm0312.

216 Giles, Keir. 2017. "Countering Russian Information Operations in the Age of Social Media." *Council on Foreign Relations*, November, 21, 2017, https://www.cfr.org/report/countering-russian-information-operations-age-social-media.

217 Galeotti, Mark. 2020. "The Navalny poisoning case through the hybrid warfare lens." *The European Centre of Excellence for Countering Hybrid Threats*, October, 2020, https://www.hybridcoe.fi/wp-content/uploads/2020/10/202010_Hybrid-CoE-Paper4_Navalny-case-through-a-hybrid-lens.pdf.

218 Fishman, Edward. 2020. "Make Russia Sanctions Effective Again." *War on the Rocks*, October, 23, 2020, https://warontherocks.com/2020/10/make-russia-sanctions-effective-again/.

219 Fiott, Daniel, and Parkes, Roderick. 2019. "Protecting Europe: EU's response to hybrid threats." *European Union Institute for Security Studies*, *Chaillot Paper/151*, April, 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/EUISS_CP_151.pdf.

220 "A Europe that Protects: The EU steps up action against disinformation." *European Commission*, December, 5, 2018, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6647.

221 "EU imposes the first ever sanctions against cyber-attacks." *European Council*, July, 30, 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

222 Dodd, Vikram, Morris, Steven, and Bannock, Caroline. 2018. "Novichok in Wiltshire death 'highly likely' from batch used on Skripals." *The Guardian*, July, 9, 2018, https://www.theguardian.com/uk-news/2018/jul/09/novichok-wiltshire-death-dawn-sturgess-highly-likely-same-batch-used-on-skripals.

223 Polyakova, Alina. 2020. "The Kremlin's Plot Against Democracy: How Russia Updated Its 2016 Playbook for 2020." *Foreign Affairs*, September/October, 2020, https://www.foreignaffairs.com/articles/russian-federation/2020-08-11/putin-kremlins-plot-against-democracy?utm_medium=social.

224 Paul, Kari. 2020. "Facebook and Twitter restrict controversial New York Post story on Joe Biden." *The Guardian*, October, 14, 2020, https://www.theguardian.com/technology/2020/oct/14/facebook-twitter-new-york-post-hunter-biden.

225 'Hacked, again'. 2020. *New York Times*, December 16, 2020. https://www.nytimes.com/2020/12/16/podcasts/the-daily/russian-hack-solar-winds.html.

226 U.S. Department of Defence Cyber Strategy Summary, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org