VOLUME 10, ISSUE 1, 2020

per Concordiam

Journal of European Security and Defense Issues

■ **WHAT RUSSIA LEARNED IN GEORGIA**
No two information operations are the same

■ **WINNING NONMILITARY CONFLICTS**
The need to broaden deterrence theories

■ **WHEN STATES WEAPONIZE THE LAW**
Using 'lawfare' to exploit established norms

■ **NONSTATE ACTORS JOIN THE BATTLE**
New foes pose unconventional threats

PLUS
Are some cyber attacks an act of war?
The 'gray zone' between war and peace
Bulgaria's strategy to counter Moscow

Perspectives on HYBRID WARFARE

features

departments

in every issue

BOOK REVIEW

on the cover:

Weaponizing information technology allows state and nonstate actors to shape public opinion.

PER CONCORDIAM ILLUSTRATION

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the 37th issue of *per Concordiam*. In this edition, we explore the concept of hybrid warfare and how to counter the threat across its various domains. There is no fixed definition of hybrid warfare, but it includes elements of cyber and information warfare, economic and political manipulation, and kinetic military action. Hybrid warfare often exists in a gray area between war and peace, and its practitioners shape their tactics to take advantage of this ambiguity.

In this issue's Viewpoint, the Marshall Center's James K. Wither introduces the concept of hybrid warfare, its evolution and how Russia used hybrid tactics in the 2014 invasion of Crimea. He discusses how Russia's current, ongoing actions are drawing the attention of Western policymakers and military strategists. He also looks at the use of hybrid tactics by other actors and notes that while asymmetric in nature, hybrid warfare has the same objective as traditional warfare — gaining advantage over an adversary.

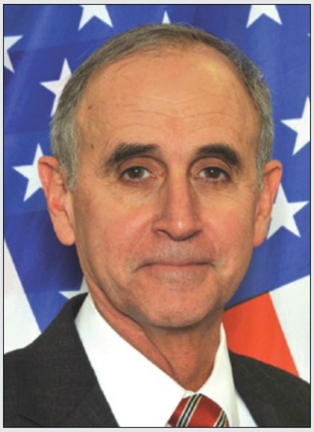
Other contributing authors include U.S. Army Col. John J. Neal, who examines deterrence theories and how to use them in a changing strategic environment where state and nonstate actors pose threats. He makes the point that agile and innovative countermeasures are required. U.S. Army Col. Ryan L. Worthan focuses on deterring Russia and its attendant nonstate actors. Cmdr. Roslaw Jezewski, a Polish naval officer, contributes a study on how Russia uses information and cyber warfare measures against the Baltic states with the aim of weakening NATO's eastern flank by targeting ethnic Russian minorities.

This issue also considers Bulgaria's new strategy for countering hybrid threats, and Russia's weaponization of international and domestic law, among other topics.

As always, we at the Marshall Center welcome comments and perspective on these topics. Please feel free to contact us at editor@perconcordiam.org

Sincerely,

Keith W. Dayton
Director



Keith W. Dayton

Director, George C. Marshall European Center for Security Studies

Keith W. Dayton retired as a Lieutenant General from the U.S. Army in late 2010 after more than 40 years of service. His last assignment on active duty was as U.S. Security Coordinator to Israel and the Palestinian Authority in Jerusalem. An artillery officer by training, he also has served as politico-military staff officer for the Army in Washington, D.C., and U.S. defense attaché in Russia. He worked as director of the Iraqi Survey Group for Operation Iraqi Freedom in Iraq. He earned a Senior Service College Fellowship to Harvard University and served as the Senior Army Fellow on the Council on Foreign Relations in New York. Gen. Dayton has a bachelor's degree in history from the College of William and Mary, a master's degree in history from Cambridge University and another in international relations from the University of Southern California.

CONTRIBUTORS

Lt. Douglas Cantwell is an officer and attorney in the Judge Advocate General's Corps, United States Navy. He received his Juris Doctor degree from Columbia Law School, master's degree from the Graduate Institute of International and Development Studies, and bachelor's degree from Stanford University. He is a former international law fellow at the American Society of International Law.

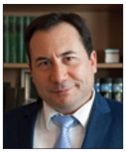
Emilio J. Iasiello is a cyber security expert with more than 15 years' experience in cyber threat intelligence, leading teams in the public and private sectors. He has delivered cyber threat presentations and has published extensively in peer-reviewed journals and cyber security blogs. He has a bachelor's degree from the College of Holy Cross, a master's degree from George Mason University, and a master's degree from the online American Military University.

Cmdr. Roslaw Jezewski serves in the Polish National Military Representative Office for NATO's Supreme Headquarters Allied Powers Europe in Belgium. He has a background in the Polish Navy and the Polish Operational Command in the Current Operations and Planning branches. He has been deployed to Ethiopia as a United Nations military observer and to Afghanistan as an advisor to the Afghan Army.

Mihail Naydenov has served as a civilian expert at the Defense Policy and Planning Directorate of the Ministry of Defense of Bulgaria since 2001. He has a master's degree in international relations from Sofia University and has studied at the NATO School in Oberammergau, Germany, the European Security and Defense College, the Swedish National Defense College, and the Ecole nationale d'administration in France. He is a member of the Atlantic Council of Bulgaria.

Col. John J. Neal is a U.S. Army War College fellow at the Marshall Center. He attended the Command and General Staff College and has a master's degree in international relations from Webster University. He earned a master's in military arts and science from the School of Advanced Military Studies before being deployed to the International Security Assistance Force headquarters in Afghanistan.

Piret Pernik is a researcher at the Estonian Academy of Security Sciences who has written extensively on national, NATO and European Union cyber security policies and strategies. She also has worked on defense policy planning at the Estonian Ministry of Defence and served as an advisor to the National Defence Committee of the Estonian Parliament on national defense matters.



Mark Voyger is the cultural advisor and senior Russia expert at NATO's Allied Land Command. Between 2009 and 2013 he worked for the U.S. Army in Iraq and Afghanistan and has worked for nongovernmental organizations and think tanks in the U.S. and Eastern Europe. He has a master's degree in law and diplomacy from the Fletcher School of Law and Diplomacy at Tufts University, and a master's degree in public administration from Harvard's Kennedy School of Government.

James K. Wither is a professor of national security studies and director of senior fellowship programs at the Marshall Center. He also is a faculty member for the center's Program on Terrorism and Security Studies. He holds a master's in strategic studies from the University of Wales; a master's in business administration from the Open University in the United Kingdom; a bachelor's in history from Kings College, University of London; and a postgraduate diploma in further and higher education from Garnett College, the University of London.

Col. Ryan L. Worthan is a U.S. Army infantry officer serving as the commander of Area Support Group-Kuwait. He holds a master's degree in national security studies from the Naval War College and a master's of engineering management from Duke University. His areas of expertise are international and national security, and systems engineering, with a special focus on NATO, Central Europe and the Baltic states. He has been a professor of international security studies, an Army War College fellow at the Marshall Center, and has served in the Office of the Army Chief of Staff.

per Concordiam

Journal of European Security and Defense Issues

Hybrid Warfare

Volume 10, Issue 1, 2020

George C. Marshall European Center for Security Studies

Leadership

Keith W. Dayton
Director

Dieter E. Bareihs
U.S. Deputy Director

Helmut Dotzler
German Deputy Director

Marshall Center

The George C. Marshall European Center for Security Studies is a German-American partnership founded in 1993. The center promotes dialogue and understanding between European, Eurasian, North American and other nations. The theme of its resident courses and outreach events: Most 21st century security challenges require international, interagency and interdisciplinary response and cooperation.

Contact Us

per Concordiam editors
Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
editor@perconcordiam.org

per Concordiam is a professional journal published quarterly by the U.S. European Command and the George C. Marshall European Center for Security Studies that addresses defense and security issues in Europe and Eurasia for military and security practitioners and experts. Opinions expressed in this journal do not necessarily represent the policies or points of view of these institutions or of any other agency of the German or United States governments. Opinions expressed in articles written by contributors represent those of the author only. The secretary of defense determined that publication of this journal is necessary for conducting public business as required of the U.S. Department of Defense by law.

ISSN 2166-322X (print)
ISSN 2166-3238 (online)

A DOUBLE DOSE ONLINE

Read current and past issues of *per Concordiam*

http://perconcordiam.com

Submit articles, feedback and subscription requests to the Marshall Center at: editor@perconcordiam.org

per Concordiam
GEORGE C. MARSHALL
European Center for Security Studies
home / features / departments / archives / letters to the editor / about per concordiam / contributors
ENGLISH (ENGLISH)
РУССКИЙ (RUSSIAN)
SOCIAL MEDIA INTELLIGENCE
Menu

per Concordiam is a professional journal published quarterly by the George C. Marshall European Center for Security Studies that addresses defense and

Get the freshest *global security news* updated weekly:

transnational weekly

http://www.marshallcenter.org

GEORGE C. MARSHALL EUROPEAN CENTER FOR SECURITY STUDIES
DEMOCRATIA PER FIDEM ET CONCORDIAM

Defining HYBRID WARFARE

By **JAMES K. WITHER**

Following the Russian Federation's invasion of Crimea in March 2014, hybrid warfare ceased to be a subject studied only by military strategists and entered the wider policy domain as a significant security challenge for the West. The term hybrid warfare attempts to capture the complexity of 21st-century warfare, which involves a multiplicity of actors, blurs the traditional distinctions between types of armed conflict, and even between war and peace. Although hybrid warfare is a Western term, not Russian, all sorts of hostile Russian activities — from the covert use of special forces to election manipulation and economic coercion — have been labeled hybrid and caused growing alarm in Western security establishments. There are many definitions of hybrid warfare and these definitions continue to evolve. Defining hybrid warfare is not just an academic exercise because these definitions may determine how states perceive and respond to hybrid threats and which government agencies are involved in countering them.

Historians have used the term hybrid warfare simply to describe the concurrent use of conventional and irregular forces in the same military campaign. Peter R. Mansoor, for example, defined hybrid warfare as "conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents and terrorists), which could include both state and nonstate actors, aimed at achieving a common political purpose." These characteristics have been typical of wars since ancient times. From a historical perspective, hybrid warfare is certainly not a new phenomenon. In the 2000s, the use of the term hybrid became a common way to describe the changing character of contemporary warfare, not least because of the increasing sophistication and lethality of violent nonstate actors and the growing potential of cyber warfare. Definitions of hybrid warfare emphasized the blending of conventional and irregular approaches across the full spectrum of conflict. Writing in 2007, Frank Hoffman defined hybrid warfare as "different modes of warfare

Russian President Vladimir Putin speaks at a concert in Crimea's regional capital of Simferopol in March 2019. Putin has used a full arsenal of hybrid warfare tools to advance Russia's interests in the region. GETTY IMAGES including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both sides and a variety of nonstate actors." The integration of conventional and irregular methods of warfare arguably distinguished such hybrid wars from their historical forms. Traditionally, conventional and irregular operations tended to take place concurrently, but separately, and operations by irregular fighters were normally secondary to campaigns by conventional military forces. Before 2014, military analysts considered the brief war between Israel and Hezbollah in 2006 as the conflict that most fitted contemporary definitions of hybrid war. Hezbollah surprised the Israel Defense Forces with its sophisticated combination of guerrilla and conventional military tactics and weaponry as well as its effective strategic communication campaign.

Police in Ukraine stand guard near a "green men" symbol drawn by anti-Russia activists on the wall of a bank in Kyiv in 2014. Prosecutors suspect the bank was used to fund pro-Moscow activities. Green men refers to the camouflaged gunmen sent to Crimea as part of Russia's hybrid assault. AFP/GETTY IMAGES

Hybrid warfare is by its very nature asymmetrical. U.S. military analysts use the term asymmetrical warfare to describe the strategies and tactics of state and nonstate opponents of the United States seeking to advance their strategic objectives despite its superior conventional military power. Asymmetrical methods of warfare, essentially pitting one's strengths against another's weaknesses, have always been a feature of successful strategy. Asymmetry naturally includes nonkinetic approaches that exploit the gray area between war and peace. However, the impact of emerging information technology allows state and nonstate actors to target decision-makers and the public through the globalized, networked media and the internet. This potentially widens the concept of war to include cultural, social, legal, psychological and moral dimensions where military power is less relevant.

Russia's actions in Ukraine in 2014 created the current preoccupation with hybrid warfare. Western commentators used hybrid as the most appropriate term to describe the variety of methods employed by Russia during its annexation of Crimea and support to rebel militant groups in eastern Ukraine. Russian techniques included the traditional combination of conventional and irregular combat operations, but also the sponsorship of political protests, economic coercion, cyber operations and, in particular, an intense disinformation campaign. The 2015 edition of *The Military Balance* provided arguably the most comprehensive definition of the latest manifestation of hybrid warfare: "the use of military and nonmilitary tools in an integrated campaign, designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure." This definition of hybrid warfare differs from those discussed earlier because it emphasizes nonmilitary methods of conflict and, in particular, information warfare that targets public perception, a key center of gravity in contemporary conflict.

Use of weaponized information is the most distinguishing feature of Russia's campaign in 2014 and its more recent efforts to divide and destabilize Western states. The Russian approach to information warfare combines psychological and cyber operations, which are critical components of what Russian analysts, most notably Chief of the General Staff Gen. Valery Gerasimov, have called new generation or nonlinear warfare. Russian information warfare seeks to blur the lines between truth and falsehood and create an alternative reality. It exploits existing societal vulnerabilities in target states, attempts to weaken state institutions and undermine the perceived legitimacy of governments. New generation warfare emphasizes the use of nonkinetic techniques that promote social upheaval and create a climate of collapse, so that little or no military force is necessary. The armed forces have a supplementary role in this strategy. Special forces may conduct reconnaissance, subversion and espionage while, if necessary, large-scale conventional military exercises close to a target state's borders seek to coerce and intimidate. Ideally, the use of armed force remains below the threshold that might trigger a conventional military response. Latvian analyst Jānis Bērziņš summarizes the Russian approach to modern warfare: "The main battlespace is in the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare. ... The main objective is to reduce the necessity for deploying hard military power to the minimum necessary."

In many respects, Russian methods date back to the Soviet era and the application of *maskirovka* — military deception. Advances in information technology and processing have greatly increased the scope of maskirovka, allowing the Russian government to employ multimedia propaganda and misinformation on a massive scale. The concept of "reflexive control" (perception management) is a key element of maskirovka. This concept, which originated with the work of Soviet psychologist Vladimir Lefebvre, employs specially prepared information that inclines an opponent to make decisions that have been predetermined as desirable by the initiator of the information. Reflexive control methods include blackmail, camouflage, deception and disinformation, all intended to interfere with an opponent's decision-making cycle in a way favorable to Russian policy.

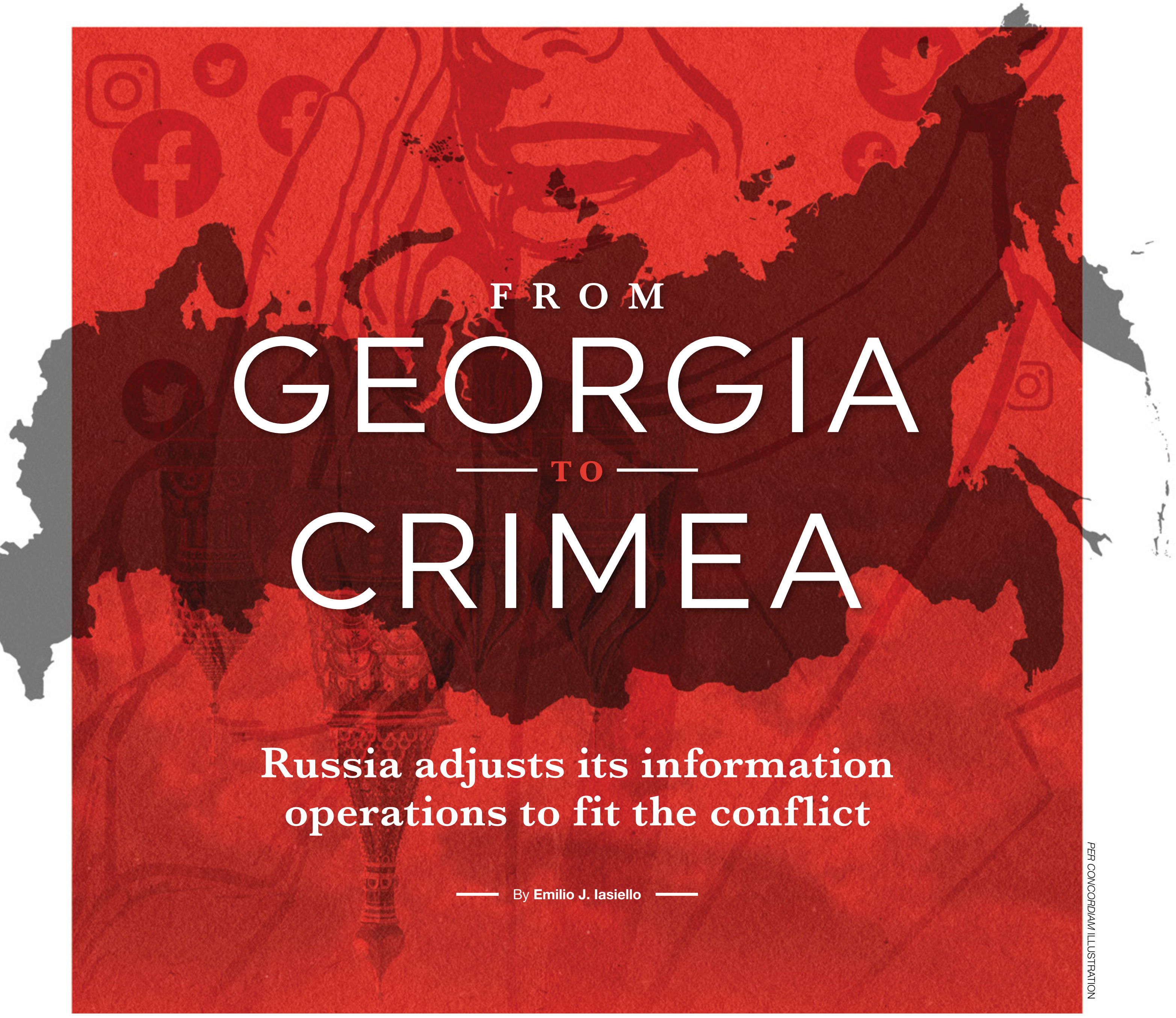
Russia is not the only state to exploit hybrid forms of warfare. China has studied so-called unrestricted warfare methods since the late 1990s. Unrestricted warfare techniques include computer hacking and viruses, subversion of the banking system, market and currency manipulation, urban terrorism and media disinformation. The extent to which unrestricted warfare has become official Chinese doctrine is not clear, although elements of the concept are evident in China's "Three Warfares" policy regarding its territorial claims in the East and South China seas. China has avoided the overt use of military force, but has exploited psychological operations, media manipulation and legal claims (lawfare) to advance its objectives.

Like the planners of unrestricted warfare, Russian analysts make no secret that their objective is to counter perceived overweening U.S. power. Russian commentators and analysts claim that Russia has remained under sustained and effective information attack by the U.S. since the end of the Cold War. From a Russian perspective, events such as perestroika and the "color revolutions," as well as multilateral organizations such as the International Monetary Fund and World Bank, are instruments of hybrid warfare intended to destabilize Russia. Russian President Vladimir Putin has even accused the U.S. of seeking to undermine the Russian state's core identity and values. Certainly, the U.S. and its close allies engaged in political warfare against the Soviet Union in the Cold War, using propaganda and psychological operations akin to those of contemporary hybrid warfare, but these operations were discontinued after the Soviet Union collapsed.

It has been long-standing Russian policy to seek ways to weaken, divide and ultimately neutralize NATO. The security of the Baltic states, with their significant Russian-speaking minorities, is of particular concern because the countries border Russia, and these minorities potentially provide Putin with leverage to create problems for the Alliance. Other countries on NATO's periphery are also vulnerable to Russian influence. There are fears that Bulgaria, for example, may be susceptible to state capture by criminal organizations linked to Russian intelligence agencies. NATO has recognized its vulnerability to Russian hybrid warfare techniques and has stationed forces in the most vulnerable countries to reassure member governments and bolster military deterrence. Alliancewide efforts have been made to identify and counter Russian cyber and information operations through new initiatives such as the Counter Hybrid Support Teams, established in 2018. Nordic states have embraced or revived whole-of-society or total-defense concepts. For example, Estonia's National Defence Concept of 2017 addresses psychological, civil and economic defensive measures as well as military preparedness. Since its Warsaw summit in 2016, NATO has put renewed emphasis on civil preparedness to boost member-state population and institutional resilience through collaboration between government ministries, civic organizations, the private sector and the public. Awareness of Russian information warfare has made governments, publics and, critically, social media companies less susceptible to disinformation and deception. This mindfulness should prevent Russian intelligence services from effective influence operations, such as their interference in the U.S. election in 2016.

Gen. Valery Gerasimov, Russia's first deputy defense minister and chief of the general staff of the Russian Armed Forces, arrives for a Victory Day parade in Moscow in May 2019. REUTERS

Hybrid warfare does not change the nature of war. Coercion remains at the core of hybrid warfare as it does any form of war. The aim remains the same, namely to gain physical or psychological advantage over an opponent. It is undoubtedly a challenge for national security establishments to address the wide range of threats that can be labeled hybrid warfare. Cast the definitional net too wide and hybrid warfare becomes too broad a term to be of any practical use to policymakers. Define warfare too narrowly and officials may fail to appreciate the significance of nontraditional techniques of warfare employed by an adversary as a prelude to the use of direct military force. □



PER CONCORDIAM ILLUSTRATION

FROM GEORGIA TO CRIMEA

Russia adjusts its information operations to fit the conflict

By **Emilio J. Iasiello**

Russia has a long history of propaganda and disinformation operations — techniques it now adapts to the online environment. As the information space expands beyond the technologies facilitating its use, Russia uses broad information-based efforts classified by their effects: information-technical and information-psychological. A major milestone for these efforts surfaced in 2008 when pro-Russian cyber attacks occurred concurrently with Russian military operations in Georgia. During that brief conflict, a resilient Georgia overtook Russia in the larger information war, forcing Russia to rethink how it conducted information-based operations. Six years later, Russia adjusted its information confrontation strategy against Ukraine to quickly and bloodlessly reclaim Crimea and keep potentially intervening countries at bay. Clearly, Russia finds value in manipulating the information space, particularly in an age when news can be easily accessed through official and nonofficial outlets. Building on its success in Crimea, Russia is outpacing its adversaries by leveraging the information space to bolster its propaganda, messaging and disinformation capabilities in support of geopolitical objectives.

INFORMATION CONFRONTATION

Russia views offensive information campaigns more as influencing agents than as destructive actions, though the two are not mutually exclusive. Simply put, the information space allows information resources, including "weapons" or other informational means, to affect internal and external

Russian troops atop an armored vehicle pass by a poster of then-Russian Prime Minister Vladimir Putin as they leave Tskhinvali, the capital of Georgia's separatist-controlled territory of South Ossetia, in August 2008. THE ASSOCIATED PRESS

audiences through tailored messaging, disinformation and propaganda campaigns. Igor Panarin, an influential scholar and well-regarded Russian information warfare expert, outlined the basic instruments involved in the larger information struggle: propaganda (black, gray and white); intelligence (specifically, information collection); analysis (media monitoring and situation analysis); and organization (shaping the opinion of politicians and mass media). In terms of influence operations, Panarin identified information warfare vehicles such as social control, social maneuvering, information manipulation, disinformation, purposeful fabrication of information, lobbying, blackmail and extortion.

Therefore, the essence of information confrontation focuses on this constant information struggle between adversaries. Reviewing the application of these principles in Georgia and Crimea, two well-known instances of Russian geopolitical involvement, help illustrate how Russia's understanding of information confrontation has evolved. It also provides insight into the outcomes of such practices in the context of on-demand media coverage.

GEORGIA, 2008

Russia and Georgia competed to control the flow of information to the global community during their brief conflict in 2008. Both sides employed kinetic (conventional military strikes and troop movements) and nonkinetic (cyber attacks, propaganda, and denial and deception) offensives. Russia's analysis and criticism of its efforts in the conflict led to some serious military reforms in its larger defense apparatus, wrote Athena Bryce-Rogers in an article in *Demokratizatsiya: The Journal of Post-Soviet Democratization*. Although experts observed alternating mission successes, the general consensus is that the Georgian government used the information and media space to its advantage to influence public opinion more successfully than Russia did.

Information-technical warfare

Russia's perception of technical and psychological information confrontation, working in concert with military attacks, became evident during the conflict in Georgia. Despite the lack of a substantive connection between the orchestrators of the cyber attacks and the Russian government, policy analyst David Hollis in a Small Wars Journal article, claimed that this nonattributable action was the first time cyber attacks and conventional military operations had been used together. Such attacks included webpage defacements, denial-of-service and distributed-denial-of-service attacks against Georgian government, media, and financial institutions, as well as other public and private targets. The attacks successfully denied citizen access to websites related to communications, finance and government, leaving some to speculate about Russian complicity, though no hard connection was made.

Information-psychological warfare

Russia also engaged in concurrent information-psychological operations, including propaganda, information control and disinformation campaigns, with varying results, especially in contrast to Georgia's efforts in the same areas. According to Ariel Cohen and Robert E. Hamilton in their 2011 book, *The Russian Military and the Georgia War: Lessons and Implications*, Russia focused on delivering key themes to the international community: Georgia and Mikheil Saakashvili, its president, were the aggressors; Russia was compelled to defend its citizens; neither the United States nor its Western allies had any basis for criticizing Russia because of similar actions these nations had taken in other areas of the world. By using television footage and daily interviews with a military spokesman, Russia attempted to control the flow of international information and sought to influence local populations by dictating news, sharing the progress of Russian troops protecting Russian citizens, and propagandizing Georgian "atrocities." A review of Georgian, Russian and Western media coverage during this period revealed then-Russian President Dmitry Medvedev was perceived as less aggressive than his Georgian counterpart. Indeed, a CNN poll conducted at the time found 92% of respondents believed Russia's intervention was justified.

Georgia wins the information war

But instead of acquiescing to Russia's information confrontation over the course of the crisis, Georgia launched an aggressive counterinformation campaign by employing its own disinformation and media manipulation. Georgia requested assistance from professional public relations firms and private consultancies to help promote its message, limited the availability of Russian news coverage, and reported Russian air raids on civilian targets, thereby becoming the victim of a Russian military invasion. Ultimately, Georgia gained the upper hand in the information conflict, a fact corroborated by Russia's review of its military's performance, which noted deficiencies in both the information-technical and information-psychological domains. Georgia won the hearts and minds of the global community even though Russia won the physical battlespace.

A Ukrainian soldier guards a road not far from the Russian border in April 2014 as a reported 40,000 Russian troops gathered along the border just weeks after annexing Crimea. AFP/GETTY IMAGES

UKRAINE, 2014

Six years after the Georgian conflict, Russia applied the lessons learned from its information activities in Georgia to its efforts in Ukraine. It learned to employ dedicated "information troops" and to strategically time cyber attacks, long considered a first-strike option for maximum effectiveness, particularly against important targets such as critical infrastructures. Unlike the concurrent digital attacks and military invasion in Georgia, cyber attacks against Crimea shut down the telecommunications infrastructure, disabled major Ukrainian websites and jammed the mobile phones of key Ukrainian officials before Russian forces entered the peninsula on March 2, 2014. Cyber espionage before, during and after Crimea's annexation also leveraged information that could support short-term and long-term objectives.

Information-technical means

Cyber espionage operations employed simultaneously with other methods of information collection appeared to accelerate battlefield tactics. Unlike in Georgia, cyber espionage targeted the computers and networks of journalists in Ukraine in addition to Ukrainian officials and those with NATO and the European Union. Exploiting such targets can provide insight into opposing journalistic narratives as well as advanced knowledge of important diplomatic initiatives. Operation Armageddon, for example, began targeting Ukrainian government, law enforcement and military officials in mid-2013 — just as active negotiations began for an EU-Ukraine Association Agreement, which Russia publicly deemed a national security threat.

As in Georgia, nationalistic hackers, such as the Ukraine-based CyberBerkut, also engaged in a variety of cyber attacks against Ukraine. This group executed distributed denial-of-service attacks and defacements against Ukrainian and NATO webpages, intercepted U.S.-Ukrainian military cooperation documents, and attempted to influence the Ukrainian parliamentary elections by disrupting Ukraine's Central Election Commission network. There was no evidence of collusion or direction by the Russian government, but the attacks did lend to the overall confusion during the crisis, particularly for Ukraine. Such attacks indicated that the Russian military had embraced Russian Gen. Valery Gerasimov's strategy on future warfare, that conflicts will retain an information aspect that is part of larger "asymmetrical possibilities for reducing the fighting potential of the enemy."

Information-psychological means

Unlike Russia's forceful invasion of Georgia, the contest over Crimean territory was more of an infiltration. In the absence of a direct threat, Russia relied on nonkinetic options such as propaganda, disinformation, and denial and deception to influence internal, regional and global audiences. This reflexive control strategy — implementing initiatives to convey specially prepared information to an ally or an opponent to persuade them to make a voluntary decision predetermined by the initiator of the initiative — explains Russia's reliance on the approach as an extension of information-psychological activities in Ukraine during and after the Crimean crisis, as well as the method's prominence in Russia's information confrontation philosophy. According to British academic Keir Giles, in an article for NATO's Strategic Communications Centre of Excellence, the Russian approach to information confrontation was evolving, developing, adapting and, just like other Russian operational approaches, identifying and reinforcing success while abandoning failed attempts and moving on.

In a noticeable improvement from its efforts in Georgia, Russia used television broadcasts to generate support for actions in Crimea and to bolster Moscow's claim that its intervention was necessary to protect native Russian speakers. Additionally, pro-Russian online media mimicked anti-Russian news sources to influence opinion. For example, the website Ukrayinska Pravda was a pro-Russian version of the popular and generally pro-Ukrainian news site Ukrains'ka Pravda. The pro-Russian sources communicated false narratives about actual events, such as denying the Russian military's presence in Ukraine or blaming the West for conducting extensive informational warfare against Russia.

One significant lesson Russia learned from the Georgian conflict was how pervasively the internet could disseminate news from legitimate and semi-official organizations as well as personal blogs. Russian President Vladimir Putin acknowledged the role the internet played in influencing the outcome of regional conflicts and recognized Russia was behind other governments in this space, saying, "We surrendered this terrain some time ago, but now we are entering the game again." Russia began to support journalists, bloggers and individuals within social media networks who broadcast pro-Russian narratives. In one case, Russia paid a single person to hold different web identities, another person to pose as three different bloggers with 10 blogs, and a third to continually comment on news and social media. Such Russian trolls may be crass and unconvincing, but they do gain visibility by occupying a lot of space on the web. Arguably, "Russia's new propaganda is not … about selling a particular worldview, it is about trying to distort information flows and fueling nervousness among European audiences," wrote Alexey Levinson on the fact-checking website Stopfake.org. By adapting denial-and-deception strategies applied during the Georgian conflict, outside interlopers remained confused during the Crimean crisis. By denying involvement in the attacks until the later stages of the conflict, Russia could continue messaging its desire to de-escalate the crisis while increasing chaos. Since the U.S., NATO and the EU could not predict Russia's objectives, Russia could leverage reflexive control to operate within Western decision-making loops, reducing the costs of its actions against Ukraine and keeping the U.S. and its allies out of the conflict. Once Putin admitted the presence of Russian troops in Ukraine, he had already annexed Crimea. Ultimately, the U.S. conceded Russian control of Crimea and sent then-Secretary of State John Kerry to mitigate the threat of further expansion into Ukraine.

Russia's victory

Noticeably improved, Russia's strategic communications proactively targeted pro-Russian rebels, the domestic population and the international community to alienate Ukraine from its allies and sympathizers. Two key themes promoted the Ukrainian government as being anti-Russian and fascist and declared that the Russian administration would improve the population's quality of life. Messages directed at the pro-Russian rebels kept them engaged in the fight whereas messages to the domestic population in Russia created moral justification for supporting the rebels in eastern Ukraine and conveyed the extant intermittent prospect of widespread combat operations there. Six years after the U.S., NATO and several European governments sided with Georgia, Moscow sought to mitigate Crimea's external support via information activities aimed at influencing foreign government actions.

Moscow used pro-Russian media sources to spread photos of Ukrainian tanks, flags and soldiers altered to bear Nazi symbols in an effort to associate the Ukrainian government with resurgent Nazism, and thereby influence some European countries, such as Germany, to distance themselves from Kyiv. Another example involved disseminating images depicting columns of "refugees" fleeing Ukraine to Russia, when in reality these were people who commuted between Ukraine and Poland daily.

While the larger struggle with Ukraine continues, Russia's successful and bloodless usurpation of Crimea testifies to the lessons learned in Georgia's South Ossetia region. Russia's information confrontation strategy was more centralized and controlled in Crimea. Perhaps the most telling aspect of its success is that Russia kept its biggest adversaries, the U.S. and NATO, from intervening, thereby enabling a referendum in which the Crimean Parliament voted to join Russia. While the West refuses to acknowledge Crimea's secession, Russia claims full compliance with democratic procedures, a fact difficult to argue against on the international stage.

UKRAINE NOW

While some believe Ukraine is winning the information war because of the EU sanctions against Russia, discontent with the sanctions is growing among the EU citizenry, particularly in Greece, Hungary, Italy and, perhaps most importantly, in Germany. Furthermore, the sanctions are not the result of Ukrainian information warfare efforts as much as the international perception of Russia as the aggressor state, a view influenced by Russia's annexation of the region and suspected involvement in the downing of a Malaysia Airlines flight in 2014.

What's more, the longer Russia engages in eastern Ukraine, the more its objectives evolve. Russia is no longer entirely focused on inspiring pro-Russia militants in the region to rejoin Russia. It also seems to be combating U.S. influence while trying to keep Ukraine out of NATO. According to a 2015 report by the Institute for the Study of War, Russia has demonstrated that obfuscating its true intent preserves its options while confusing its adversaries. Hypothesizing by adversaries over Russia's true intent gives it the advantage, where it can leverage its flexibility to reach resolutions that benefit its interests. For example, while the U.S. and Russia were at odds over how to handle Syria, Russia's aid to embattled Syrian President Bashar al-Assad's forces successfully stopped U.S.-backed oppositionists to the extent that it compelled the U.S. into a quid-pro-quo relationship in which U.S. operational coordination against terrorist groups was given in exchange for Russia's commitment to stop Assad from attacking civilians and the U.S.-backed moderate opposition.

THE COLOR REVOLUTIONS, WHICH RESULTED IN SUCCESSFUL REGIME CHANGES, REINFORCED THE BELIEF THAT CONSTRUCTING, CONTROLLING AND DISSEMINATING INFORMATION EFFECTIVELY AND SUBSTANTIALLY INFLUENCES THE OUTCOME OF GEOPOLITICAL EVENTS.

This involvement made Russia an equal partner in the region, regardless of al-Assad's return to power. Similarly, Russia may surrender its short-term goals for eastern Ukraine to have autonomous rights in favor of the strategic gain of Ukraine not joining NATO. Some believe the economic burdens of eastern Ukraine may be too much for Russia to take on. If true, using the region as a bargaining chip for the greater prize serves Russia's long-term objectives.

EVOLUTIONARY THINKING

Information warfare has been referred to as an asymmetric weapon, and the incidents with Georgia and Crimea certainly support this categorization. The color revolutions, which resulted in successful regime changes, reinforced the belief that constructing, controlling and disseminating information effectively and substantially influences the outcome of geopolitical events. Russia, generally perceived as one of the leading powers in information warfare, lost its information struggle against Georgia in the early stages of the conflict. Conversely, by applying an adaptive approach, Russia adjusted its information confrontation strategy, successfully facilitating its appropriation of Crimea from Ukraine. Simply put, Russia learned from its mistakes in Georgia and thereby influenced the outcome in Crimea. As one Russia expert remarked during a Radio Free Europe/Radio Liberty report, "When you look at how Russia is attempting to copy Western style press briefings by the military ... it speaks volumes to their understanding of how better to structure public opinion around a military operation."

After its distributed denial-of-service attacks in Estonia in 2007, Russia's information-confrontation activities evolved from a tool used primarily for disruption to a tool of influence. The managing director for the Center for Security and Strategic Research at the National Defense Academy of Latvia echoes this sentiment by asserting influence operations are "at the very center of Russia's operational planning." Indeed, the more nonmilitary means are employed in areas of geopolitical tension, the more essential the leveraging of information confrontation becomes. As information is generally regarded as soft power, it may be most effectively implemented when there is no force-on-force military conflict, when information can be used to inform, persuade, threaten or confuse audiences, such as Russia's efforts to influence the 2016 elections in the U.S.

Unsurprisingly, Russian writing on information confrontation continues to evolve, a testament to the strategy being dynamic, much like the domain in which it is applied. While Gerasimov may have helped redirect Russian military thinking about the role of nonmilitary methods in the resolution of conflicts, other military experts built on that foundation. In 2013, retired Russian Col. S.G. Chekinov and retired Russian Lt. Gen. S.A. Bogdanov wrote that "a new-generation war will be dominated by information and psychological warfare that will seek to achieve superior control of troops and weapons and to depress opponents' armed forces personnel and population morally and psychologically. In the ongoing revolution in information technologies, information and psychological warfare will largely lay the groundwork for victory."

The use of the term "new-generation war" is a nod to the criticality of information dominance at a time when both the content of information and the technologies it traverses are heavily relied upon for civilian and military matters. Though new-generation war does not appear to have been used in military writings since 2013, a lack of official refutation by military officers suggests it may still be a relevant professional approach toward warfare.

Many Western scholars have categorized Russian tactics in Ukraine as hybrid warfare, the use of hard and soft tactics that rely on proxies and surrogates to prevent attribution, to conceal intent, and to maximize confusion and uncertainty. A 2015 article in *Military Thought* suggests this interpretation of the events in Ukraine may be incorrect and more accurately describes Western actions. In fact, by the end of 2015, Russian officers altogether refuted the use of "hybrid" to describe their activities. Nevertheless, the complementary and supportive role of information confrontation in Ukraine suggests it is best implemented in concert with other conventional and unconventional activities to achieve maximum effectiveness in larger campaigns and not as a stand-alone tactic.

In 2015, the director of the Russian General Staff's Main Operational Directorate explained a "new-type warfare," similar yet distinct from hybrid and new-generation warfare, that associates indirect actions with hybrid ones. Other authors of new-generation warfare accepted the new terminology, particularly for activities focused on military, nonmilitary and special nonviolent measures to achieve information dominance, which logically includes actions in Ukraine. According to analyst Timothy L. Thomas, one author stressed that "information warfare in the new conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, the global computer networks (blogs, various social networks, and other resources)."

Unsuccessful attempts to place information confrontation under the rubric of any specific modern warfare strategy, such as new-generation war, hybrid warfare, or new-type warfare, may further testify to the reciprocally dynamic and malleable nature of the strategy and conflict activities. The one aspect consistently carried through official Russian documents concerning information security doctrine and military strategy, and carried out in these regional conflicts, is the belief that information superiority is instrumental to future victories.

As the world moves toward conflicts in which, as Gerasimov describes, "Wars are not declared but have already begun," it is evident that — whether referred to as information warfare, information confrontation, information operations or information struggle — no state is guaranteed victory based solely on an abundance of resources or capabilities. The art of information confrontation must be practiced continuously, refined over time and tailored to specific audiences.

Russia actively refines its methods in real-time conflicts as it leverages and incorporates its information struggle into nonmilitary means to achieve political objectives. In this way, Russia is not learning from others as much as it is learning from itself. And therein may lie information confrontation's greatest strength: There is no cookie-cutter playbook from which it originates or to which it applies. Information campaigns can be tailored to suit each unique environment. The information campaign that worked in Crimea may produce different outcomes elsewhere, which reinforces Russia's lessons-learned approach — do not fight the next battle in the same way as the last one. The greatest asset of this capability is its flexibility to assume greater or lesser responsibilities dependent on requirements. This is paramount as the role of nonmilitary means to achieve political and strategic goals in conflicts has significantly increased.

CONCLUSION

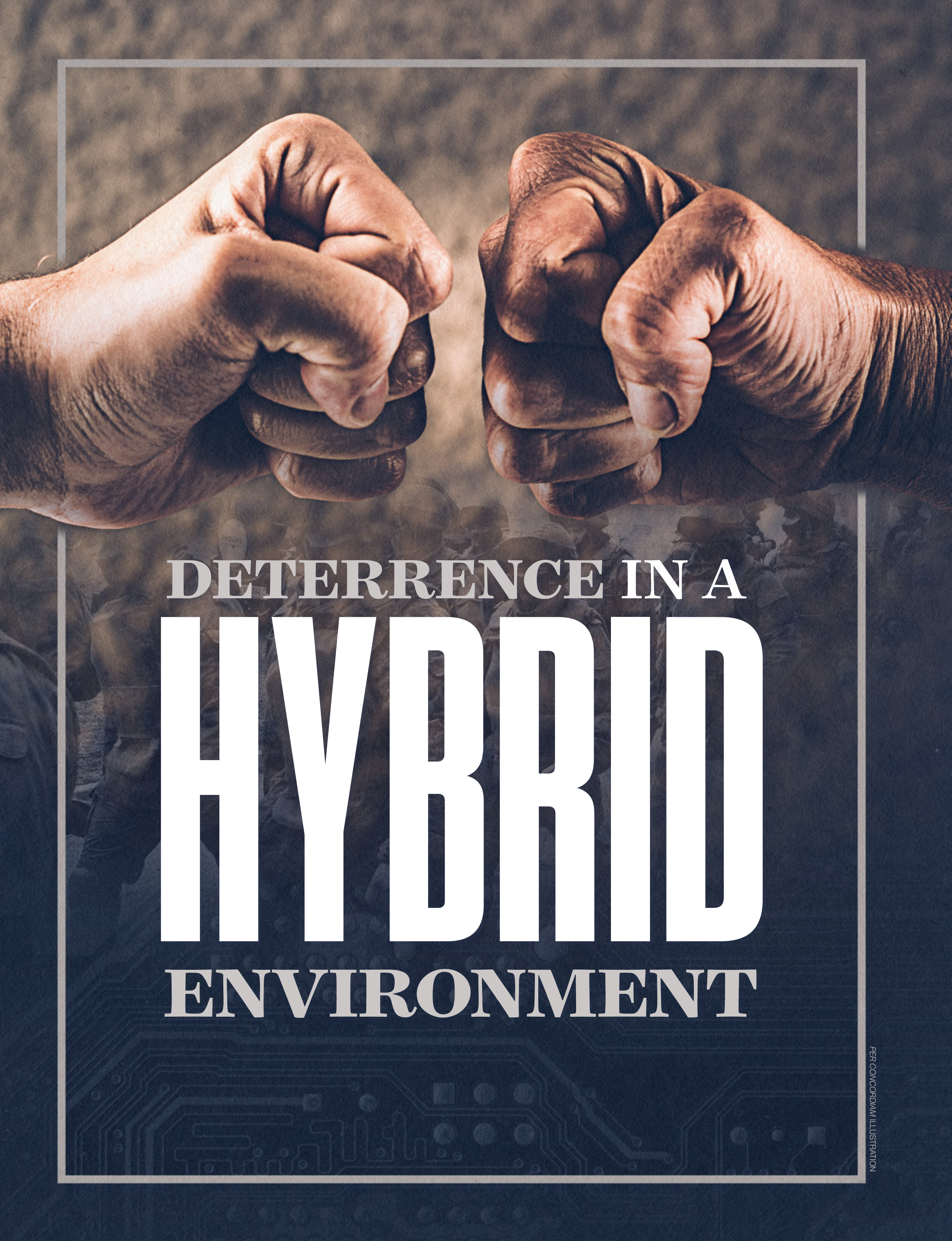
Applying information warfare theories in today's geopolitical climate remains a work in progress. An around-the-clock news cycle and the various ways of disseminating and consuming information worldwide make it challenging to compete in information-based operations. But as observed in Georgia, smaller nations can competitively control information and influence target audiences to at least mitigate the efforts of, if not defeat, larger nations. Even after learning from its missteps in Georgia, Russia did not gain many Ukrainian regions. It lost opportunities in Luhansk and Donetsk when Russian troops were unable to penetrate the regions promptly. Russia, however, appears to be guided by Gerasimov's principle of refining information confrontation strategies by continuing to engage in various forms of official and unofficial messaging, as well as perfecting the art.

Ukrainian border guards patrol the Ukrainian side of the Ukraine-Russia border in Milove in eastern Ukraine in 2018. THE ASSOCIATED PRESS

One scholar of Russian propaganda refers to it as a war on information rather than an information war. Given the value Russia places on manipulating information, perceptions of the information space as potentially dangerous, and a successful agent for ousting governments and influencing public opinion and behavior, are understandable. A former KGB general stated the overall goal of Soviet propaganda was not far from the "subversion" pursued by Russia's modern internet disinformation campaign: "active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs."

While the media has focused on offensive cyber attacks and disruptive efforts to cripple critical infrastructures and to impede public access to financial institutions and emergency services, Russia understands the potential power associated with influencing via cyberspace. As such, Russia continues to refine its online information operations against regional and international targets, outpacing opponents in its nonoffensive cyber capabilities and demonstrating that not all threats in cyberspace are written in binary. □

This article first appeared in the journal *Parameters*.



PER CONCORDIAM ILLUSTRATION

DETERRENCE IN A HYBRID ENVIRONMENT

Defending against nonlinear threats

By **Col. John J. Neal**, U.S. Army

Cold War deterrence theories are no longer sufficient to guide states in the current era of great power competition. The linear concept of military escalation is not valid in an environment where nonmilitary means are the tools of choice for aggressors to advance their strategic goals. Activities categorized as below the level of armed conflict now pose a significant threat to national security, potentially on par with military threats. States are also more willing to use nonmilitary means because of the inherent ambiguity and lack of behavioral norms associated with the use of these tools. Therefore, governments must revise the way they think about deterrence to take these changes into account and develop effective strategies that can better address national security concerns.

The inherent ambiguity in the current security environment is reflected in the lack of distinction between military and nonmilitary means. The military tools available to the state have been greatly expanded. These have traditionally included land, air and maritime formations and the capabilities designed to inflict lethal harm on an adversary, which is how they are defined for the purposes of this article. However, state armed forces now often control some means not usually associated with the military, such as cyber, information and economic tools. This lack of distinction between military and nonmilitary means further complicates deterrence in the current environment.

Deterrence concepts developed during the Cold War focused primarily on the use of military means based on a clear correlation of forces that indicated the probability of success. Escalation along a commonly understood scale played a key role. These ideas were applied to deterrence by denial and by punishment strategies to protect national interests. In addition, deterrence thinking yielded key framing questions, identified basic requirements and recognized that adversaries would take an incremental approach to undermine deterrence efforts. These ideas were valid in a world where military tools were the primary means of aggression.

Policymakers have turned to a combination of Cold War and emerging deterrence theories to address the confrontational behavior of Russia and China over the past two decades. In doing so, they have not sufficiently accounted for the differences between the Cold War and the current environment. There are still significant shortfalls in deterrence thinking that need to be addressed. First, the central role of military force and the linear nature of conflict are no longer applicable. These ideas should be replaced by an understanding of the parity of military and nonmilitary means to threaten national interests. In addition, the Cold War concepts of basic deterrence requirements, key framing questions, and the adversaries' incremental approach are still valid, but these ideas have new meaning in the context of nonmilitary means.

Changes in the environment

There are three nonmilitary areas in particular that are greater threats than they were several decades ago: cyber, information warfare and economic. These tools also have different employment-time considerations than military means. Each poses similar challenges of response and scale that complicate the formulation of deterrence strategies.

Blasts from NATO's Exercise Trident Juncture 18, off the coast of Trondheim, Norway, send up water geysers. Such exercises deter aggression by demonstrating NATO's capability and resolve. REUTERS

The cyber threat is of particular concern. Cyber tools can be used to support military, economic and information warfare operations, or they can be used to surveil, damage or destroy systems in the cyber domain. There are numerous examples of these actions committed by state actors. Andy Greenberg noted in a *Wired* magazine article that the Russian "NotPetya" cyber attack against Ukraine in 2017 caused more than $10 billion of damage worldwide. In 2011, a group of hackers based in North Korea — presumably affiliated with that government — attacked Sony Pictures' networks for producing a movie satirizing North Korean leader Kim Jong Un. According to a study by the Foundation for Defense of Democracies, Chinese cyber incursions and network exploitations have caused significant damage to foreign companies. Despite numerous confirmed attacks by state actors, there is still no consensus on where these actions fit in the spectrum of conflict.

While the use of information against adversaries is millennia old, it became much more prevalent with the advent of digital mass media and the internet. Some states take a broad and less constrained approach to information warfare. In a 2011 conceptual document on activities in the information space, the Russian Defense Ministry described information warfare as carrying out psychological campaigns against a state's population to destabilize both the society and the government. Russian information warfare has increased capacity and access over the past two decades through wider media presence, social networks and cyber tools. These changes have significantly increased information warfare's potential to threaten national security.

As with information warfare, economic tools have been used for centuries to influence other states, but the increased interconnectedness of globalization, coupled with economic digital vulnerabilities, means that it poses a greater threat than in the past. There is strong evidence to suggest that Russia uses economic tools to manipulate other states and advance its national interests. A 2016 Center for Strategic and International Studies report finds a correlation between the level of Russia's economic presence in a country and the deterioration of democratic values and standards. Similarly, Chinese theft of business intelligence and intellectual property is used to increase the competitiveness of Chinese businesses while negatively affecting companies outside China, as highlighted in a MindPoint Group white paper from 2014. Economic means are also ambiguous in terms of how they fit in the spectrum of conflict because while some economic behaviors such as tariffs are well understood in escalation, others such as economic influence are not.

An overarching issue is how nonmilitary means change the nature of time and tempo in conflict. In military conflict, there is typically a distinct initiation of hostilities, usually through the overt use of lethal force, preceded by a buildup, which may offer a warning of impending aggression. Nonmilitary means have very different timelines for execution and effect. Information operations take months or even years to produce effects. Conversely, cyber tools can cause catastrophic effects in a matter of minutes, potentially with no warning. These widely varying chronological factors must be accounted for in developing future approaches to deterrence.

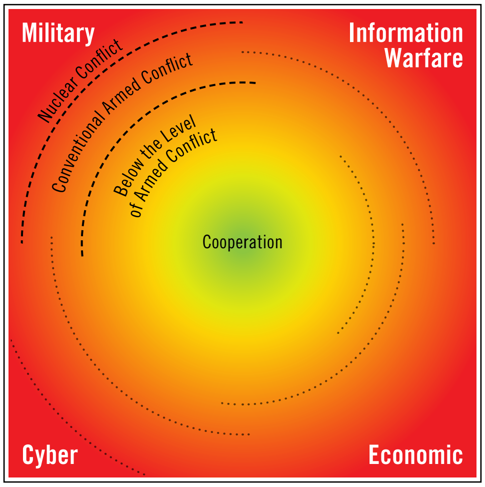
U.S. Marines with the 24th Marine Expeditionary Unit hike to a cold-weather training site in Iceland during NATO's Exercise Trident Juncture 18. REUTERS

Table 1. **Nonlinear Deterrence**

Understand the Environment

1. Know the adversary.
2. Recognize the increased threat nonmilitary means pose to national security.
3. Lower the threshold for the use of nonmilitary means.
4. Know the adversary's incremental approach.
5. Recognize the indistinctness of peace and war.

Visualize the Environment



Deterrent Approaches

1. Reduce ambiguity.
2. Go beyond domain-limited actions.
3. Apply key aspects of deterrence theory:

- Decide who, what and when to deter, and what is worth deterring.
- Identify the aggressor; clearly signal the aggressor; possess the capability to respond.
- Deter by punishment.

Source: Col. John J. Neal, U.S. Army

Deterrence theory

There are several aspects of military deterrence that must be reassessed to create future deterrence policy. First, in military deterrence the spectrum of conflict is viewed as linear, where the use of force occurs along a known scale. Secondly, this scale infers that the use and effects of specific military tools are widely understood. This understanding is reinforced by a competitor's assessment of the correlation of forces, which typically focuses on military capabilities. Finally, military deterrence theory does not account for the effects of nonmilitary tools in waging war.

The linear spectrum of conflict is one of the best-known legacies of the Cold War. In 1965, theorist Herman Kahn used a ladder metaphor to frame escalation. This consists of a linear arrangement of crisis levels, with associated levels of risk. Actors ascend or descend the ladder by conducting actions that correspondingly increase or decrease the opponent's threat level. The concept had applications for Cold War scenarios and, in particular, conflict between the U.S. and the Soviet Union.

The correlation-of-forces method used to determine the costs of a given action is greatly facilitated by the relative ease with which each state can quantitatively measure their respective strengths and weaknesses. However, nonmilitary tools do not lend themselves to this kind of quantitative examination, so the potential impact of the use of these tools is much more abstract. There is also a commonly accepted framework of the potential costs and reactions to military escalation. The same cannot be said of the nonmilitary means. All of this complicates the calculation of the deterrent effect of nonmilitary tools.

Though there are bodies of literature on the use of military, cyber, information and economic tools, each area is often treated in isolation when addressing deterrence. Deterrence thinking tends to focus on symmetrical domain or area responses, such as a military reaction to a military provocation, without viewing these activities in the larger context of the competitor's behavior and intent. A fully integrated, multidomain approach to deterrence that recognizes the changing nature of conflict is required to shape effective deterrence policy.

State-versus-state deterrence

For a theory to be useful to practitioners, it must provide a consistent way of approaching a complex problem with multiple factors and variables. Changes in the security environment, including the interdependent use of military and nonmilitary means along widely varying timelines where competitors seek to exploit ambiguity and nonattribution, have made deterrence inherently more complex. Existing deterrence theory and associated scholarship do not adequately address these changes. I propose the idea of "nonlinear deterrence" to describe an updated concept that accounts for these changing conditions. Nonlinear deterrence is composed of three elements. The first, understanding the environment, is composed of five principles that account for adversary behavior, emerging tools, and the effect both have on the concepts of peace and war. The second part is visualizing the environment. Table 1 (above) depicts the interaction of military and nonmilitary means with relative risks to national security. The third part of the concept is deterrent approaches; practical applications to drive deterrence policy development in the future.

Understand the environment

The first component of nonlinear deterrence is understanding the environment. It consists of five principles, which are an amalgamation of emerging scholarship that includes Michael Mazarr's seven hypotheses of the gray zone (aggression that is coercive but below the threshold of conventional military conflict); traditional thinking on deterrence from theorists like Lawrence Freedman, John Mearsheimer, Alexander George and Richard Smoke; and ideas gleaned from trends in the environment. The first principle is understanding the aggressor. Theorist André Beaufre put it succinctly when he wrote that "deterrence must therefore be played with the enemy's doctrines as a yardstick." Both Russia and China have published concepts of modern warfare that embrace the use of nonmilitary means. Russian military theorists first put forth their idea of "new generation" warfare in 2013 in the journal *Military Thought*. The authors, S.G. Chekinov and S.A. Bogdanov, described a concept that involves the combined use of nonmilitary and military tools to target the adversary's armed forces and its population. In fact, Russian theorists have advanced the idea that nonmilitary means could be the predominate factor in determining the outcome of hostilities.

The Cold War-era U.S. listening station Field Station Berlin is no longer used. Technology has advanced, but the need to monitor Russian activity remains.

AFP/GETTY IMAGES

The second principle in understanding the environment is recognizing the increased threat nonmilitary means pose to national security. As with the first principle, this is clearly a concept that some states embrace. There are numerous examples of how cyber, information warfare and economic means have been used to cripple other states. These tools currently pose a threat to national security on par with military means. In addition, they do not have the geographic limitations or timelines associated with military tools, requiring a different understanding of their applications.

The third principle is the greater willingness to use nonmilitary rather than military means. This is in part why some countries apply these tools to support the methods described in the first principle. Nonmilitary actions, particularly in cyber and information warfare, are difficult to attribute, freeing states to use them with less risk of punishment. There are far fewer treaties, agreements and laws, if any, that govern the use of nonmilitary tools, so there is less of a codified basis for retaliation. Furthermore, there are no established scales of behavior that define the severity of specific nonmilitary actions. All of these assist countries in advancing their goals.

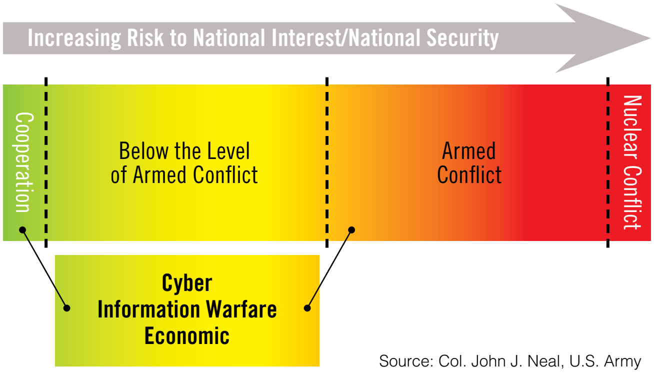
The fourth principle is recognizing that some states take an incremental approach, using a series of small actions to achieve long-term ends and avoid overt conflict. Thomas Schelling termed this concept "salami-slicing" during the Cold War and it has been further described as "gradualism" by Mazarr. In this process, a state conducts a series of activities that in and of themselves do not escalate the level of tension between states. However, collectively these actions create a new status quo advantageous to the aggressor. This approach necessitates an interconnected view of military and nonmilitary actions over time to understand the broader context and intent.

The fifth principle is to stop thinking strictly in terms of peace and war. Instead, it should be recognized that the line between the two has been blurred to the point that they are no longer distinct. This state of affairs puts governments at a disadvantage since they traditionally think in binary terms and compartmentalize their tools. Conversely, this condition, described by Lucas Kello as "unpeace" in his book *The Virtual Weapon*, favors the aggressor, allowing them to maximize the use of nonmilitary means and exploit the incremental approach.

Visualize the environment

The second part of nonlinear deterrence is visualizing the environment. The ability to see and understand the connections between the use of military and nonmilitary tools over time is crucial to recognizing how adversary activities threaten national interests. It facilitates the development of coherent policies and actions to deter further aggression and to anticipate possible areas of concern. To present the nonlinear visual model, it is necessary to review past, current and evolving graphic depictions of the spectrum of conflict and where the various means fit into them.

Figure 1. **Linear Spectrum of Conflict Focused on Military Means**



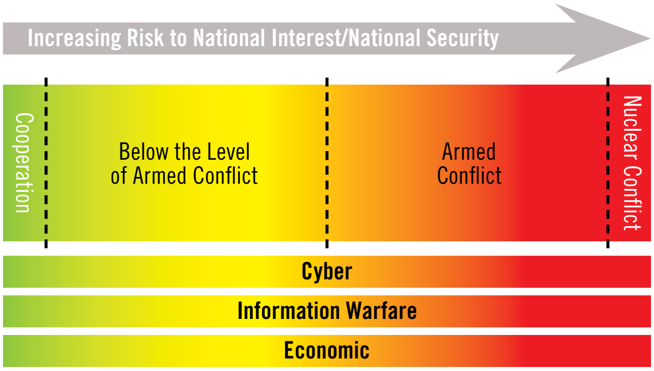
Increasing Risk to National Interest/National Security
Cooperation
Below the Level of Armed Conflict
Armed Conflict
Nuclear Conflict
Cyber
Information Warfare
Economic

Source: Col. John J. Neal, U.S. Army

Past concepts have taken the form of a sliding scale, which focused on the use of military force with nonmilitary means being a complementary aspect of military tools (see Figure 1, above). This reflected the idea that military actions have a well-defined escalatory hierarchy with clear distinctions and that nonmilitary means have an ill-defined supporting role and only pose a marginal threat.

We now recognize that nonmilitary means pose greater levels of threat to national security, potentially on par with military means. However, these areas are often viewed in isolation, with a potential theoretical scale of escalation applied (see Figure 2, below). This reflects the current focus on domain-specific deterrence without accounting for how actions in each of these areas contribute to a deteriorating security environment.

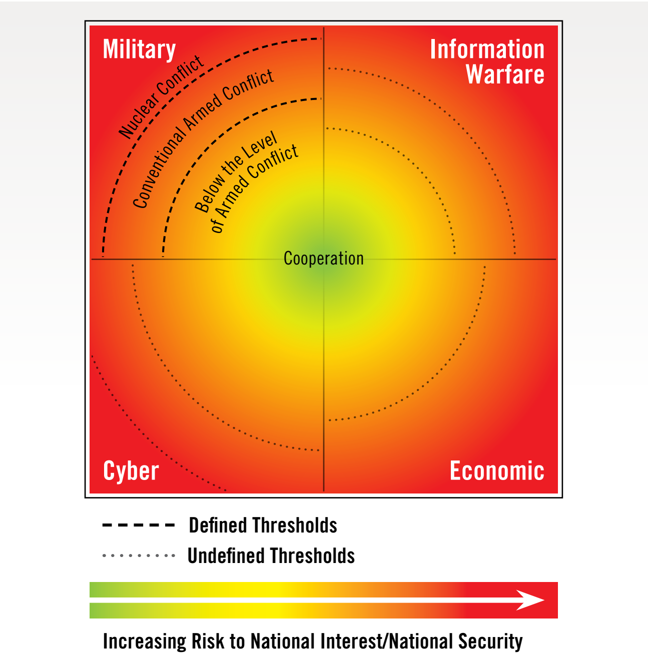
Figure 2. **Spectrum with Parity of Military and Nonmilitary**


Increasing Risk to National Interest/National Security
Cooperation
Below the Level of Armed Conflict
Armed Conflict
Nuclear Conflict
Cyber
Information Warfare
Economic

Source: Col. John J. Neal, U.S. Army

The evolving concept model moves away from the escalation ladder, since it is less relevant as competitors seek ways to circumvent established norms. In this model, military and nonmilitary means are represented as having equality in their threat to national interests and national security. The thresholds for the use of military force are demarcated, and the potential for thresholds in the nonmilitary means are also accounted for, should they be defined (see Figure 3, below).

Figure 3. **Multivector Spectrum of Conflict**


Military
Information Warfare
Nuclear Conflict
Conventional Armed Conflict
Below the Level of Armed Conflict
Cooperation
Cyber
Economic
- - - - Defined Thresholds
········ Undefined Thresholds
Increasing Risk to National Interest/National Security

Source: Col. John J. Neal, U.S. Army

However, the military and nonmilitary categories cannot be viewed in isolation. The quadrant lines in this model reflect the idea that each area is distinct and separate, which is the same concept portrayed in Figure 2 using parallel lines.

The nonlinear deterrence visualization of the environment combines the idea of threat parity among military and nonmilitary means, the interdependence of these means, and the aggregate increased risk to national interests and national security. This model is designed to highlight how actions in one area are connected to activities in another, such as the use of military force to create an economic effect. This model also shows how potential thresholds may be applicable in more than one area. To illustrate these concepts, actions in and around Ukraine from April to November 2018 are displayed. It shows how activities in multiple areas are connected and how they push the limits of acceptable behavior (see Figure 4, following page). This example depicts a state operating in a specific geographic area acting against another state. The model can be expanded to a state acting across the globe over a longer period of time or contracted to a smaller area and a shorter period in order to draw out connections and risks.

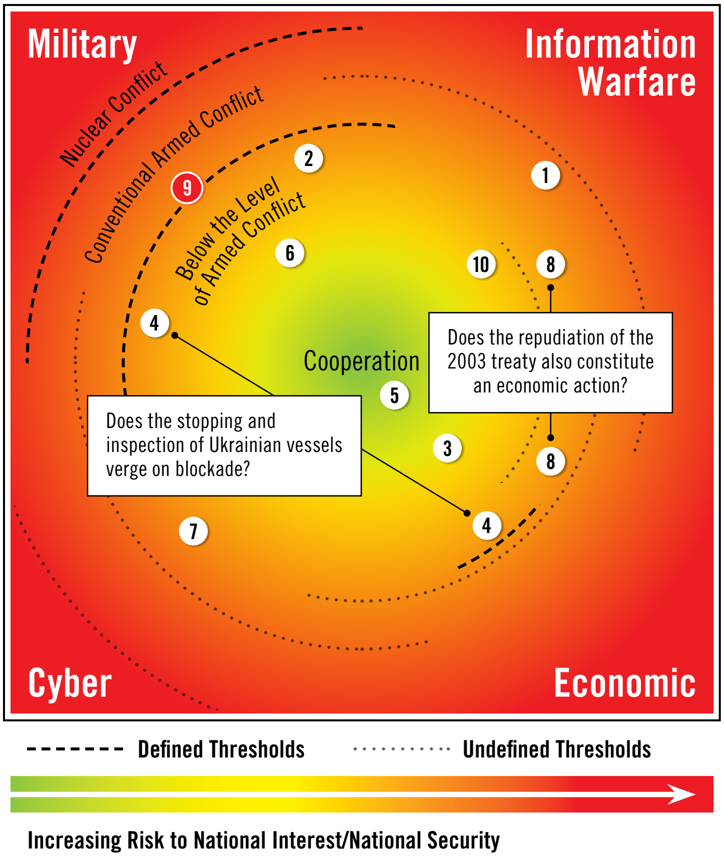
Visualization of the environment is a key element of the nonlinear deterrence concept. It incorporates and characterizes the principles of "understanding the environment" in a graphic display that sets the conditions for the application of the "deterrent approaches" principles. The model is also adaptive. It is designed so that it can incorporate emerging deterrence concepts and terminology to account for the changing nature of conflict and the role that various tools play in the environment.

Deterrent approaches

The first principle of deterrent approaches is reducing ambiguity. Ambiguity is a critical enabler of competitor strategies. Decreasing it will significantly degrade an aggressor's ability to achieve its goals. Doing so involves establishing defined parameters and norms of behavior and challenging adversaries when they violate them. As described by Thomas Schelling in *The Strategy of Conflict*, when disrupting an incremental threat, disrupting individual acts is more effective than countering the overall objective. Using this method, states can incrementally hinder adversaries before conditions irrevocably change in the adversary's favor.

One way to define parameters is to establish clear red lines for actions that threaten national interests. In doing so, states can definitively challenge adversary behavior. Red lines are defined as the stated position of an entity that it will act if another violates that position. One example is Article 5 of the North Atlantic Treaty, which states that an armed attack against one member of the Alliance will be answered by all. However, there are inherent vulnerabilities in red lines. David Altman noted in "Red Lines and Faits Accomplis in Interstate Coercion and Crisis" that red lines are arbitrary and can be imprecise, incomplete and unverifiable. NATO's Article 5 illustrates some of these vulnerabilities. In 2014, NATO members agreed that a cyber attack met the criteria for an Article 5 violation. This step made sense, given the

Figure 4. Nonlinear Visualization of the Environment


Military
Information Warfare
Nuclear Conflict
Conventional Armed Conflict
Below the Level of Armed Conflict
Cooperation
1
2
9
6
10
8
4
5
3
8
7
4
Does the repudiation of the 2003 treaty also constitute an economic action?
Does the stopping and inspection of Ukrainian vessels verge on blockade?
Cyber
Economic
Defined Thresholds
Undefined Thresholds
Increasing Risk to National Interest/National Security

Actions in and around Ukraine

(April-November 2018)

1. **2018:** Russian disinformation campaign claims: Ukraine infected sea with cholera, Ukraine attempted to smuggle a nuclear bomb into Crimea, Ukraine naval base is for NATO.
2. **April-November:** Russian buildup of land and maritime units in Crimea/Sea of Azov.
3. **May:** Russia opens Kerch Bridge leading to a loss of Ukraine freight traffic.
4. **May-October:** Russia stops and inspects merchant ships bound for Ukraine ports in Sea of Azov.
5. **September:** Russia states it complies with 2003 treaty that Kerch Strait is both Ukraine and Russia.
6. **October:** Russian joint maritime/land exercises in Crimea, Black Sea.
7. **October-November:** Russian cyber data collection and attacks on Ukraine government in conjunction with Russian Kerch Strait operations.
8. **November 15-21:** Russia declares it has complete sovereignty over Kerch Strait; United Nations Convention on the Law of the Sea not applicable.
9. **November 23-26:** Russia attacks three Ukrainian ships and captures Ukrainian sailors while transiting the Kerch Strait.
10. **November 26:** TASS reports Ukrainian ships violated Russian border.

Source: Col. John J. Neal, U.S. Army

increased cyber threat, but it highlights some of the red line vulnerabilities. However, this position is both imprecise and incomplete, since the Alliance has not clearly defined what constitutes a cyber attack. It is also difficult to verify, since one of the advantages to cyber is its inherent deniability. Finally, in the years since NATO took this position there have been multiple cyber attacks on its members with no clear retaliation and no declaration of Article 5. To be effective, red lines must be clearly defined, backed by a credible threat and, most importantly, they must be enforced.

Another method is establishing the legal framework for accepted behavior through treaties, international agreements and national policy. One of the fundamental issues with nonmilitary means is the lack of such a framework, enabling adversaries to exploit these means to great effect. The idea of a treaty that governs cyber activity is not new. National governments, international organizations and private corporations have all called for a digital Geneva Convention that would govern the use of cyber tools. This raises several issues. One is the difficulty in getting powerful competitors to agree on meaningful standards, particularly since it is in the interest of many of them not to do so. Another is that some states will not adhere to the treaty to which they agreed. Finally, since one of the major issues with nonmilitary means is attribution, verifying treaty violations will be difficult. Even with these drawbacks, it is still advantageous to work to establish these agreements. In addition, states can create their own standards of behavior and thresholds for retaliation in order to reduce ambiguity. This may be an effort to define an escalation hierarchy similar to the escalation ladder of military actions.

The second principle of deterrent approaches is going beyond domain-limited actions. In many cases, states respond or posture in the same domain where the aggressor is operating. For example, the U.S. is taking a stronger position in opposing cyber threats by expanding operations in cyberspace. NATO has enlarged its military force posture and activities in response to increased military aggression by Russia. To be more effective, states need to develop a codified strategy that integrates the use of tools across multiple domains to precisely target aggressor actions.

The third principle of deterrent approaches is accounting for key aspects of deterrence theory. The foremost of these aspects is deciding who, what and when to deter, and, fundamentally, what is worth deterring. These requirements establish the foundation for a deterrence strategy and allow policymakers to examine threats in the context of national interests in order to prioritize efforts and resources in a coherent manner.

The three requirements for deterrence, described by Schelling in *Arms and Influence*, are also applicable in the current environment. The first is attribution; the state can unmistakably identify the aggressor. The second is signaling;

A member of the Swedish Army's Gotland regiment positions a machine gun as part of a live-fire exercise on the island of Gotland in February 2019. After the annexation of Crimea, the conflict in Ukraine, incidents of Russian military jets approaching Swedish aircraft, and the 2014 sighting near Stockholm of a mystery submarine suspected to be Russian, Sweden has scrambled to beef up a military that was cut back after the end of the Cold War. AFP/GETTY IMAGES

the state clearly conveys its messages to the aggressor. The third is credibility; the state possesses a viable capability that it will actually use. Each of these requirements are challenging in the context of nonmilitary means. Cyber and information warfare work optimally when they are unattributable. Even economic means, which are usually overt, may be ambiguous as to their true intent. Furthermore, revealing capabilities in nonmilitary areas to convey credibility will often result in the reduction of those capabilities since countermeasures can be rapidly developed.

The next aspect is the balance between deterrence by denial and deterrence by punishment. Both are valid methods, but deterrence by punishment is often a more viable way of deterring the use of nonmilitary means. There are several reasons for this. First, it is very difficult to deny competitors the conditions that enable attacks. Many countries are premised on free and open societies, with their inherent unrestricted access to cyberspace and media. To limit these freedoms would go against these principles. Second, the defenses against nonmilitary aggression are not effective to the point that they can deny an attacker the ability to attain its goals. Third, it is difficult to deny aggressors access to nonmilitary means since these tools are often cheap, prolific and dual-use. As conditions change and technologies advance, there may be a shift back to deterrence by denial, but for the time being punishment offers more deterrence potential.

The concepts of counterforce and countervalue targeting have applications in deterrence by punishment. These methods allow for the nuanced use of nonmilitary tools to impose costs on adversaries. Max Smeets recently described this concept for the use of cyber tools in his paper, "The Strategic Promise of Offensive Cyber Operations." He points out that this approach has already been used in multiple instances, even if the applications have not been labeled as such. This same approach can be applied to economic tools, where some actions may target a specific capability while others are focused on broader areas.

Conclusion

The nature of conflict is changing. States are increasingly turning to nonmilitary means to advance their goals, altering the concept of escalation in the process. The interdependent use of military and nonmilitary means has blurred the lines between peace and war. These factors have created conditions in which competitors exploit the ambiguity of their actions and the lack of international norms of behavior to threaten other states in ways not previously anticipated. To secure their interests in the future, states must adapt their understanding of deterrence.

Nonlinear deterrence offers a way of thinking about deterrence that can assist in addressing the current security environment. It is an amalgamation of past and current thinking and of ideas drawn from recent competitor doctrine and behavior. It is also a departure point for further discussion and additional work in the development of state-versus-state deterrence that can be applied to national policy formulation. □

Putin's Russia

PER CONCORDIAM ILLUSTRATION

A Hybrid State Unbounded by Limitations

By **Col. Ryan L. Worthan,** U.S. Army

NATO's final communique from the 2016 Warsaw summit recognized the changed security environment in which Russia's malign "activities and policies have reduced stability and security" and "increased unpredictability," requiring enhancement of its "deterrence and defence posture." Collectively, NATO has broadened its deterrent approach, encompassing a whole-of-government strategy and providing measures of reassurance and deterrence by bolstering military presence, partner capacity, interoperability and alliance resilience. The ongoing sanctions regime complements NATO's efforts by constraining the resources and mobility of select Russian individuals and businesses. This complementary approach seeks to influence Russia as a unitary state without substantively dissuading the nonstate actors (NSA) Moscow uses to shape the environment and undercut regional stability.

NATO's deterrent concept is premised on the assumption that Russia operates as a unitary state and is therefore capable of being deterred according to the tried and tested principles and assumptions embedded in rational deterrence theory. Likewise, the preponderance of contemporary Russian deterrence literature focuses on the threats and potential responses to hybrid aggression conducted by a unitary state in the nebulous space between peace and war. Russia is undoubtedly a unitary state under President Vladimir Putin, but the duality of traditional state organs and a networked patronal power structure unbounded by unitary state limitations provides Putin a broad menu of means and methods to attain strategic objectives. Bureaucratic pluralism and hybridity of associations challenge conventional deterrence thinking and call into question Moscow's evolving decision-making apparatus and risk calculus. As the Marshall Center's Graeme Herd puts it, Russia's ongoing trend of "de-globalization, de-institutionalization, and de-modernization" make it dependent upon the tools and methods employed by NSAs to exert influence abroad. Russia's weak formal institutions are increasingly influenced and often controlled by an underlying network of patronal power centers shaping Russia's strategic agenda. These trends suggest a more basic set of questions be answered regarding Russia: Is Russia a unitary state actor, or has it morphed into a hybrid state? And what does that mean with respect to deterrence?

To deter a nuclear armed, conventionally capable hybrid state actor (HSA), NATO must develop a strategy to concurrently deter the state while compelling its attendant NSAs. NATO must maintain the nuclear deterrent, continue its support of forward resilience measures and reinforce conventional defensive arrangements to deny Russian objectives, while enabling individual nations with the requisite knowledge, capabilities and capacity to deny and, if necessary, locally punish Russian malign actors.

Unitary State vs. NSA Deterrence

Rational deterrence theory argues the "balance of deterrence" leads to stability and status quo maintenance. It assumes unitary state actors approach strategic decision-making in a logical manner, pursuing outcomes through rational cost-benefit analysis. At its core, the purpose of deterrence is to dissuade a potential aggressor from taking unwanted actions by shaping the aggressor's perception of the defender's political commitment to respond, the aggressor's decision-making processes, and the aggressor's ability to accurately calculate and control risk. As Daniel Sobelman noted in his study, "Learning to Deter," "deterrence is achieved through the communication of calculated credible threats designed to shape or reshape the perception and manipulate the behavior of another actor." "Deterrence by punishment" and "deterrence by denial" are the most often applied methods. In the nuclear realm, the costs of a challenge to the status quo are both clear and high. But as Alexander L. George and Richard Smoke note in *Deterrence in American Foreign Policy: Theory and Practice*, in the conventional military realm, deterrence by denial attempts to shape an aggressor's perception that the costs and risks of an aggressive act outweigh the expected benefits. Successful deterrence maintains the status quo by removing aggressor options through denial or threat of punishment, but the initiator's possession of an increasing variety of options requires that deterrence thinking evolve or risk failure.

Deterring unitary states employing all elements of national power is challenging but widely researched and well-documented. Deterrence of NSAs is less studied and complicated by asymmetries of political will, strategic objectives, centers of gravity, operational approaches, organizational structures and political resolve, making deterrence difficult, if not impossible, to achieve.

The most studied NSAs accomplish their objectives through violence. But NSAs span licit and illicit organizations, mobilizing populations, resources and ideologies regionally and transnationally. The confluence of ideological movements, proliferation of technology, and increased access to finance and information make NSAs increasingly influential and "drivers of state action," as recognized by Anne-Marie Slaughter in *The Chessboard and the Web: Strategies of Connection in a Networked World*. While NSAs lack traditional state power, they nonetheless achieve influence by leveraging relative strength disparities, which are often intensified by patron-proxy relationships. Furthermore, the NSA's ability to exploit differing rules provides opportunities that enable relatively weak NSAs to compete, coerce, deter and often prevail against stronger state adversaries. Sobelman's study of the Israel-Hezbollah conflict highlights how a state and an NSA achieved deterrence by fulfilling the core requirements of communication, capabilities, credibility and resolve. While Hezbollah exploited asymmetry to compete with the Israeli state, Israel adapted its deterrent construct to blend the negative, defensive and static characteristics of deterrence with the positive, offensive, overt and dynamic characteristics of compellence. Ultimately, an NSA exploited asymmetry to deter a state, and the state's adapted strategic approach reverted the conflict to a symmetric framework.

A flag made of the flags of Iran, Palestine, Syria and Hezbollah is displayed in Tehran on the anniversary of Iran's Islamic revolution. Hezbollah and Palestinian Hamas are examples of nonstate actors supported by Iran. REUTERS

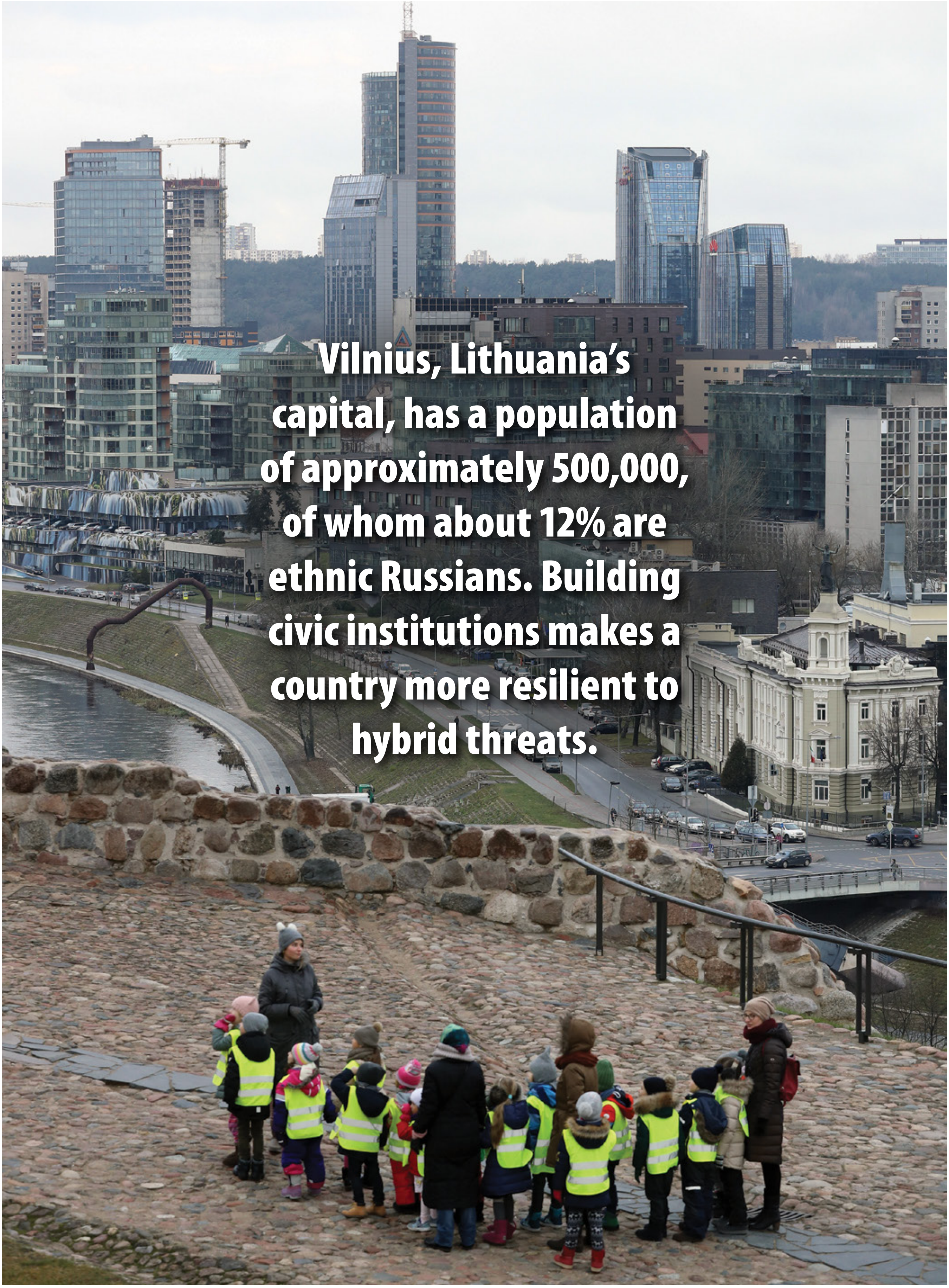
While NSAs lack unitary state power, their very asymmetry makes them inherently resilient, and those possessing patron support are significantly more challenging because they are unhindered by the patron's need for populace support, are often unencumbered by the restraints of international law and unconcerned with the legitimacy of their actions. The ideological sources of NSA resolve, decentralized operational approach and networked structures pose stark challenges to conventional deterrence due to the challenges of holding NSA interests at risk, often requiring coercion or compellence by force. Short of military action, states must compel NSA behavior change by imposing unsustainable costs to NSA interests. Successful compellence offers the NSA no choice but to change behavior, making them strategically irrelevant.

The Hybrid State: Reframing Russia

While unitary state deterrence is well documented, and the Israel-Hezbollah conflict provides insights into NSA deterrence, the concept of a hybrid state is largely unconceptualized and, therefore, deterring one is generally unconsidered. However, the emergence of the hybrid state is already changing the character of conflict.

States adapt and evolve through experiential learning and structural change. Learning facilitates improved capacity and effectiveness, while structural change broadens capabilities and resilience. Relatively weak patron-supported NSAs may attain regional effects, but external dependency exposes exploitable vulnerabilities, making compellence and coercion possible. Regional powers deliberately harnessing state resources to support or create NSAs gain a unique ability to broaden capabilities, bolster resilience and maintain deniability. The concept of state-created NSAs is not historically unique, as evidenced by a letter from 1921 between the British foreign secretary and the Soviet commissar for foreign affairs: "When the Russian government desire[s] to take some action more than usually repugnant to [the] normal international law of comity, they ordinarily erect some ostensibly independent authority to take action on their behalf. … The process is familiar and has ceased to beguile." Deliberate proxy creation allows for actor and intent ambiguity, requiring that the state and its NSA-like subsidiaries be addressed simultaneously to achieve deterrent effects.

Putin's centralization of power reinforces a patronal power structure reminiscent of the Soviet era, but devoid of Soviet ideology or its associated institutions. Richard Sakwa's dual-state model advanced the concept of a constitutional state functioning separately from the dominant power system. The Russian regime exists at the center of a shifting constellation of patronal power centers, operating outside the legal framework of the normative state. Though writing about Ukraine, Andreas Umland posited that power within a patronal system is accumulated and exercised through distinctly informal relationships between elites occupying positions of power in economic conglomerates, regional political machines and official government posts. The most powerful patronal networks penetrate every aspect of Russian society,



Vilnius, Lithuania’s capital, has a population of approximately 500,000, of whom about 12% are ethnic Russians. Building civic institutions makes a country more resilient to hybrid threats.

Kindergarten children view the Vilnius business district from the hill of Gediminas Castle. AFP/GETTY IMAGES ranging from ministries and political parties to economic conglomerates, media outlets and nongovernmental organizations. Herd describes a "Collective Putin" concept in which Putin balances the power and influence of three distinct pillars: the normative state; parastatal economic, political and social entities; and nonstate oligarchic actors. In an article for the website Open Democracy, Umland describes the glue holding these networks together as an assortment of "familial ties, personal relationships, long-term acquaintances, informal transactions, mafia-like behavior codes, accumulated obligations, and withheld compromising materials, or *kompromat*." Putin exercises power through a network of functional, regional and local *kurators* who facilitate the "exchange of posts, money, real estate, goods, services, licenses, grants and favors." These unofficial networks influence, if not covertly direct, Russian policy and decision-making. The "collective Putin" reaps the benefits of power while remaining immune to the constraints, obligations and responsibilities inherent to traditional governance postings.

Through this dichotomy of national character and power, Russia embodies the hybrid state paradigm. The HSA actively combines the benefits of unitary state legitimacy with NSA freedom of action, internally reinforcing and benefiting the elite, while affording supplementary capabilities with which to shape the strategic environment. The very nature of a patrimonial power network encourages elite participation in enterprises and activities that blur the lines between licit and illicit, formal and informal, public and private, foreign and domestic. Active and direct oligarch and *siloviki* (those associated with the security services) participation in Russia's shaping operations create a challenge, which Mark Galeotti characterizes in "Russia's Hybrid War as a Byproduct of a Hybrid State," as "complex, multi faceted, and inevitably difficult for Western agencies to comprehend, let alone counter." It is this combination of decision-making ambiguity and deniable action upon which *maskirovka*, or strategic deception, is built.

Business leaders attend a session during the Week of Russian Business, organized by the Russian Union of Industrialists and Entrepreneurs, in Moscow. The system in Russia internally employs the hard power of coercion and the soft power of attraction to maintain cooperation among oligarchs, government institutions and nongovernmental institutions. REUTERS

Maskirovka underpins Moscow's pursuit of strategic advantage and its ability to successfully operationalize deterrence-challenging typologies: controlled pressure, limited probes or faits accomplis. Nuanced application of subconventional methods executed by intermediaries affords the Kremlin deniability while obscuring operational intent. While the West traditionally views economic sanctions and diplomatic pressure as levers to prevent conflict, Russia views them as measures of war itself. Beyond Russia's view of traditional great power interactions, Galeotti highlights Putin's "'total war' approach to governance: the absence of legal, ethical and practical limitations on the state's capacity openly or covertly to co-opt other institutions to its own ends." Putin leverages the hybridity of the Russian state to weaponize every asset to play great power games without great power resources, effectively waging a political struggle with the West through political subversion, economic penetration and disinformation.

Moscow's strategic objectives are widely accepted to be: regime protection, expansion of its near-abroad influence, weakening of Western states and alliances, and reinstatement of a multipolar world. However, understanding its priorities requires a functional understanding of patronal power networks. Putin's crucial prerequisite for preserving power rests on his ability to maintain broad public support and apparent electoral success, but he is beholden to a network of actors who facilitate the criminal corruption schemes constituting the core and purpose of much of post-Soviet patronal politics. While Russia's strategic objectives are clear, regime protection is paramount, with all other objectives feeding that singular end.

Understanding the Hybrid State

To better understand the uniqueness of the hybrid state as an entity, it is helpful to explore the differences between centralized, decentralized, and hybrid organizations, which is described by Ori Brafman and Rod A. Beckstrom in their book, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. Centralized organizations have clear leadership and formal hierarchy, using command and control to keep order, maintain efficiency and conduct routine business, making them effective at management and task accomplishment, but inelastic and susceptible to system shocks. By comparison, decentralized organizations lack a clear leader and distribute power across the system, making them resilient and resistant to system shock, but often inefficient at task accomplishment. The hybrid state incorporates the hierarchical leadership necessary for system control and task accomplishment while harnessing the initiative, intellect and resources of the collective to innovate and create opportunities. Brafman and Beckstrom's analysis of hybridized business structures provides insight to Putin's organizational preferences and the techniques he employs to attain strategic options and advantages. Putin's patronal network is effectively a decentralized system composed of autonomous business units, adhering to a set of rules and norms, accountable for producing results in the form of profit, effects, or both. This approach maximizes strategic opportunities while maintaining strong directive ties to preserve veto authority.

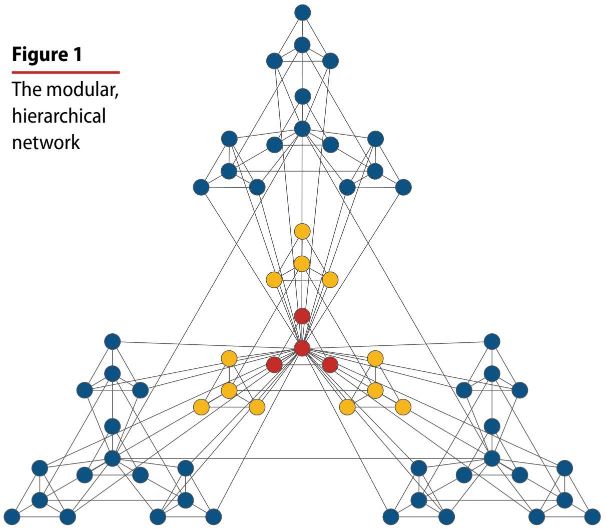
Putin maintains considerable, but not absolute, veto authority over the activities of a loose network of actors holding formal government posts and guiding informal factions conventionally labeled by Richard Sakwa in "The Dual State in Russia," as the siloviki, the "democratic-statists" and the "liberal-technocrats." The U.S. Treasury Department's January 29, 2018, "Kremlin Report" identifies a similar set of influence groups: senior political figures holding official government postings, heads of large state-owned parastatal enterprises and oligarchs. Those listed in the "Kremlin Report" are not uniformly subject to the legal rules of the normative state, allowing some the latitude to rapidly adapt to circumvent constraints and maximize opportunities. Recognizing this challenge, the Treasury Department's sanctions of April 6, 2018, sought to deter Russia by targeting "a number of individuals [and entities] … who benefit from the Putin regime and play a key role in advancing Russia's malign activities." These sanctions indicate a refined organizational appreciation, but successful deterrence will also require the West to understand how Putin exercises power and the degree to which the networked, patrimonial Collective Putin influences strategic decision-making.

Anne-Marie Slaughter noted that "the traditional definition of power rests on the ability to achieve your goals either on your own or by getting someone … to do what you want them to do that they would not otherwise do." Hierarchical organizations traditionally view power through a transactional or coercive mindset, while networked organizations acquire and manage power through the volume and strength of connections between network nodes. Putin's governance structure internally employs the hard power of coercion and the soft power of attraction through a mixture of command, agenda-setting and preference-shaping strategies. While the patronal system is predicated on positional and coercive power, it is strengthened by a network mindset where information, communication and material flow between network actors. The modular hierarchical network model from Slaughter's book provides a viable characterization of what a network model of the contemporary Russian state would look like [Figure 1]. A central node connected to other nodes in a descending hierarchy of centrality and connectedness; everyone is connected but not for every purpose, creating system resilience through a combination of nodal diversity, modularity and redundancy. Taking from Galeotti's article "Controlling Chaos: How Russia Manages its Political War in Europe," the presidential administration represents the central node "and perhaps the most important single organ within Russia's highly de-institutionalized state." While the presidential administration holds a central network position, the underlying patronal system necessitates Putin's personal arbitration of interagency conflict and involvement in decisions of strategic significance.

Putin's ability to build, gatekeep, adapt and scale his patronal network operationalizes Joseph Nye and Suzanne Nossel's concept of "smart power." Putin blends elements of hard and soft power through the selective employment of every tool available to leverage influence across a grid of allies, institutions and corporations, maintaining internal stability while achieving strategic objectives. Russia's employment of smart power and maskirovka make a fitting national strategy, given a convergence of Russian history steeped in patrimonial power networks, burgeoning NSA influence, the ambiguity and deniability necessary to compete when constrained by a lack of soft power, and challenging demographic and economic conditions.

Figure 1

The modular, hierarchical network



Source: Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World*

Harmonizing of Deterrence and Compellence

Putin's hybridization of the Russian state began the day then-President Boris Yeltsin appointed him prime minister and granted him the authority to coordinate all power structures. But Putin's power structure is not vertical in a dictatorial sense, rather, it is an adaptable construct which he balances based on his central role as arbiter and moderator of the switching functions between competing patronal groups. His overarching objective is regime protection, but the objectives of the patronal conglomerate vary. Putin's fulfillment of the disparate objectives of critical network nodes preserves internal stability while affording him access to a wide array of conglomerate-generated, subconventional effects for internal and external use.

The structural changes Putin has put in place have moved the character of Russian governance along a continuum from unitary to hybrid state, generating strength, but also creating exploitable vulnerabilities. The strength and weakness of Putin's hybrid state springs from nodal interdependencies — the ability of individual nodes to obtain their objectives by generating purpose-fulfilling value, or effects, for the network. The Collective Putin is principally a business network built upon mutual-trust relationships, fueled by the exchange of power, resources and information brokered by *kurators*, who gatekeep and manage the connections between different networks. The factors that maintain elite cohesion and the power of Putin's kurators are also the primary network vulnerability, in the sense that removing highly interconnected nodes can damage or even destroy the entire network. Exploiting Putin's network vulnerabilities, and therefore shaping the perceptions of Russia's NSAs, demands that the West embrace a more offensive, overt and dynamic compellence construct to complement ongoing deterrence efforts.

If the purpose of deterrence is to dissuade unwanted action, the West must view Russia not as a mirror-imaged unitary state, but as a hybrid state. Hybrid state deterrence requires the simultaneous deterrence of the normative state and compellence of the networked actors who guide, support, and finance its nonstate entities. Deterring an HSA therefore requires dedicated focus, persistence and analytical rigor to map the network, its players, their relationships and objectives, and the opportunities inferred by emergent vulnerabilities. Inadequate network understanding will inadvertently inform actions that produce incomplete network disruption and allow rapid reconstitution of malign capabilities. The West must indirectly remove Putin's strategic options by shaping the perceptions of critical network players, making it clear that their interests and the patronal network itself are at risk. Accomplishing this end requires that NATO fundamentally challenge its assumption that Russia acts as a unitary state and create an attribution network resembling U.S. Army Gen. Stanley McChrystal's team-of-teams approach to defeating al-Qaida in Iraq, but on a supranational level.

An effective attribution network would see the entirety of Russia's malign influence in real time, understand the network's switching mechanisms, and grasp the casual relationships between deterrent actions and nodal responses, thereby informing a harmonized policy approach to defense, deterrence and dialogue. NATO, its members and its societies already maintain a loose network of ad hoc partnerships and organizations of Russia watchers, but neither the Alliance nor its members comprehensibly detect nor fully appreciate noncontiguous threats due to information stovepiping. Solving attribution ownership requires the creation of a standing international, intergovernmental and intersocietal organization, fashioned in the image of the U.S. National Counterterrorism Center or the European External Action Service's Intelligence Center. An organization incorporating Celina Realuyo's critical elements of collaborative models for security and development: "political will, institutions, mechanisms to assess threats and deliver countermeasures, resources, and measures of effectiveness" could ostensibly meld the existent web of Russia watchers with the hierarchical structures of NATO and the governments it defends. This approach has significant sovereignty, agency and fiscal limitations, but there may be a more expedient path to holistic attribution.

NATO already leverages a loose constellation of input networks spanning military, law enforcement, civil defense

Ukrainian troops rappel from an Mi-8 helicopter during the Clear Sky 2018 joint exercises with the United States and other NATO countries on the Starokostyantyniv Air Base in western Ukraine. Military preparedness is one way to deter hybrid state aggression. AFP/GETTY IMAGES and academia. Broadening the participation in these groups, and clearly articulating their mandate, could garner significant attribution capability and capacity. Additionally, NATO should consider broadening the mission, manning and capabilities of the Multi-National Corps and Divisional Headquarters to include greater joint, interagency and intergovernmental partners to maximize individual alliance member expertise to inform more rapid and synchronized responses, whether they be multi-, bi- or unilateral. Networked structures such as these would embody the essence of former U.S. Secretary of Defense James Mattis' approach to long-term strategic competition outlined in the summary of the 2018 U.S. National Defense Strategy, and are necessary to ensure "the seamless integration of multiple elements of national power — diplomacy, information, economics, finance, intelligence, law enforcement and military," as well as providing a permanent point of interface with academia, nongovernmental organizations and corporations with interests jeopardized by Russian aggression.

Sobelman asserts that, "in theory, deterrence succeeds when a potential challenger, having received a credibly perceived threat, calls off an intended action." While the West has taken some deterrent actions, Russia's continued subconventional activities offer stark evidence that Putin and his network are undeterred. While NATO rightfully improves military capability, interoperability and strategic mobility, it must also account for Sobelman's assessment that "military capabilities will not necessarily deter a challenger that believes that is has devised an effective way to offset their impact or escape them." Credible military capability is an indispensable component of deterrence, but deterring Russia requires a collaborative attribution network built upon McChrystal's twin pillars of "shared consciousness" and "empowered execution." Formulation of effective deterrence and compellence measures requires an understanding of a hybrid state's network, its internal decision dynamics and the interests of its actors. In the case of a revanchist Russia, greater network understanding will not only inform Western deterrence efforts, but also offer insight into the branches and sequels of the post-Putin era.

Chief of the Russian General Staff Gen. Valery Gerasimov noted in 2013 that "no matter what forces the enemy has, no matter how well-developed his forces and means of armed conflict may be, forms and methods for overcoming them can be found. He will have vulnerabilities and that means that adequate means of opposing him exist." While debate continues as to the intent of Gerasimov's comment, Galeotti notes that there is nothing "conceptually novel about current Russian practices," as they include "using all kinds of nonkinetic instruments to achieve its ends." The West already possesses adequate means to oppose the illicit actors and tactics constituting Russia's array of subconventional aggression, for they are already in use, albeit desynchronized in their execution and informed by the unchallenged assumption that Russia acts as a unitary state.

While improved conventional deterrence and holistic resilience efforts are indispensable components of a revised deterrent construct, a successful Alliance strategy must necessarily embody structural and organizational changes that facilitate cross-government, civil-military cooperation. Development of a functional collaboration network will illuminate the linkages and vulnerabilities of Russia's opaque network of malign influence facilitators. Deterring a hybrid Russian state requires a construct that harmonizes unitary-state deterrence and NSA compellence, incorporating denial of objectives and punishment of actions, facilitated by specific and credible dialogue.

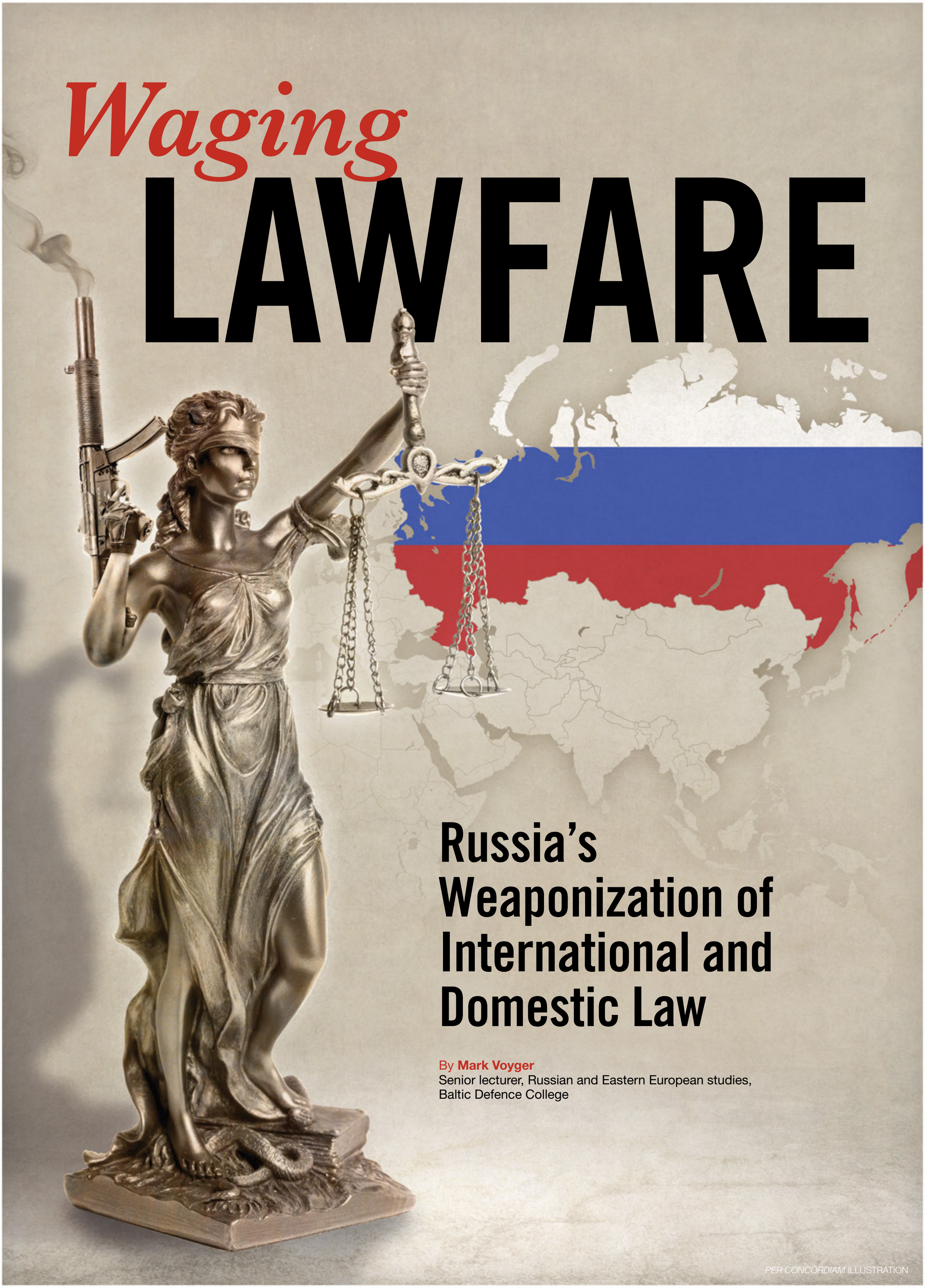
Ukrainian activists block construction of a huge shopping mall in Kyiv belonging to Russian oligarch Boris Rotenberg, a figure close to President Vladimir Putin.

AFP/GETTY IMAGES

Embracing a Revised Mindset

Traditional deterrence constructs fail to substantively address the asymmetric actors increasingly employed by revisionist states. Challenges posed by relatively weak but highly networked NSAs continue to confound Western governments, undoubtedly informing adversarial strategies. Western adversaries' takeaways from this are threefold: 1) the West effectively initiates but ineffectively responds to subconventional competition; 2) direct Western conventional competitive advantage can be indirectly countered through the introduction of subconventional actors that are ambiguous and deniable in nature; and 3) hybridized governance structures confuse Western policy responses, creating opportunities to block, disrupt and spoil Western initiatives.

As a result, agenda-setting and effective competition in a highly networked environment will require states to embrace a deterrent mindset shift, thus informing innovative approaches to achieve desired policy outcomes. As Gen. Mark Milley, chief of staff of the U.S. Army stated, "The nature of war — the use or threat of violence, as an extension of politics, to compel the enemy … is immutable. However, the character of war … changes due to unique geopolitical, social, demographic, economic and technological developments interacting, often unevenly, over time." While the nature of warfare is immutable, the character of the actors engaged in geopolitical competition is changing, requiring the West to operationalize U.S. Adm. James Stavridis' "whole of international society approach" to counter hybrid state adversaries. The distinct implications of the hybrid state actor necessitate that deterrence thinking evolve or risk failure. □



Waging LAWFARE

Russia's Weaponization of International and Domestic Law

By **Mark Voyger**
Senior lecturer, Russian and Eastern European studies,
Baltic Defence College

PER CONCORDIAM ILLUSTRATION

Russia's attempts to assert its hegemonic ambitions against Ukraine and other countries in its "near abroad" — what Moscow perceives as a region of its privileged interests — have posed serious challenges not only to the security of the region, but to the international order. During its ongoing comprehensive hybrid warfare campaign against Ukraine, the Kremlin has employed a full range of nonmilitary tools (political, diplomatic, economic, information, cyber) and military ones — conventional and covert. Given the prominent role of Russia's information and cyber warfare, those two hybrid warfare domains have received most of the public attention and analytical effort so far.

However, there is a third pivotal element of Russia's hybrid toolbox — "lawfare" (legal warfare), which is critically important and equally dangerous, but has remained understudied by the analytical community and is effectively still unknown to the public. Given lawfare's central role in Russia's comprehensive strategy, Russia's neighbors, NATO and the West must develop a deeper understanding of this hybrid warfare domain and design a unified strategy to counter this major challenge to the European security architecture and the entire world order.

Definitions of lawfare

The term lawfare was first coined by retired U.S. Air Force Maj. Gen. Charles Dunlap, a former deputy judge advocate general and now a professor of international law at Duke University. His 2009 paper "Lawfare: A Decisive Element of 21st-Century Conflicts?" defined lawfare as "a method of warfare where law is used as a means of realizing a military objective." He broadened the definition in a 2017 article for *Military Review* to include "using law as a form of asymmetrical warfare." Those original definitions focus on the exploitation of the law primarily for military purposes, which is understandable, given that the term hybrid warfare did not enter Western political parlance until the summer of 2014 with its official adoption by NATO. Given the prevalence of nonmilitary over military means (not only in an asymmetric military sense) in Russian Gen. Valery Gerasimov's new generation warfare model, presented in February 2013, it is necessary to revisit and broaden the original definition of lawfare in a holistic fashion to place it in its proper context as one of the pivotal domains of Russian hybrid warfare. In Gerasimov's 2016 update in the *Military-Industrial Courier* to his original model (based on Russia's military experiences in Syria), he stated, "Hybrid Warfare requires high-tech weapons and a scientific substantiation." In that regard, Russian lawfare's primary function is to underpin those efforts by providing their legal foundation and justification. To be precise, the term lawfare itself does not exist in Russian, but the 2014 Russian military doctrine recognizes the use of legal means among other nonmilitary tools for defending Russia's interests.

Russian lawfare is the domain that intertwines with and supports Russian information warfare, thus providing (quasi) legal justifications for Russia's propaganda claims and aggressive actions. To provide further granularity, the legal domain of Russian hybrid warfare can be understood in its entirety only through the comprehensive analysis of the intersection of the areas of the law with the various other military and nonmilitary domains of hybrid warfare.

Russian lawfare's imperial origins

Russia has been using international law as a weapon since at least the 18th century. The roots of this type of conduct can be found in the history of Russian and Soviet interactions with the international system of nation states known as the "Westphalian order." At various times in its history Russia has either been invited to join the concert of major European powers or invaded by some of those powers. In its formative centuries, the nascent Russian Empire did not deal with neighboring states as equals, but took part in their partition (the Polish-Lithuanian Commonwealth) and the division of Eastern Europe into spheres of influence. It also regularly acted to suppress ethnic nationalism within its own territories, while at the same time encouraging Balkan nationalism and exploiting the ethno-religious rifts within the Ottoman Empire throughout the 18th and 19th centuries. International law was pivotal for Russia's expansionist agenda because it claimed that the 1774 Treaty of Kucuk-Kaynarca with the Ottomans had granted it the right to intervene diplomatically and militarily in the Balkans as the sole protector of Orthodox Christians. Based on that fact, 1774 should be regarded as the birth year of Russian lawfare. This method for justifying imperial expansionism thrived during the Soviet era as the Soviet Union partitioned states, annexed territories, and launched overt aggressions and clandestine infiltrations across national borders in the name of protecting and liberating international workers, but really to impose its limited sovereignty doctrine on its satellite states.

This twisting and permissive reinterpretation of history to justify *ex post ante* Russia's acts of aggression against its neighbors was codified on July 24, 2018, when the Russian Duma adopted a law recognizing officially April 19, 1783, as the day of Crimea's "accession" to the Russian Empire. Catherine the Great's manifesto proclaiming the annexation of Crimea is a diplomatic document that had an impact far beyond the borders of Russia and throughout the centuries that followed, and it has regained relevance in present-day

Russian strategy. It is unique also in that Empress Catherine II employed arguments from all domains of what we nowadays refer to as hybrid warfare — political, diplomatic, legal, information, socio-cultural, economic, infrastructure, intelligence and military (both conventional and clandestine) — to convince the other Great Powers of Europe, using the 18th century version of strategic communications, that Russia had been compelled to step in to protect the local populations in Crimea. In that regard, April 19, 1783, can be regarded as the official birthdate of Russian hybrid warfare, in its comprehensive, albeit initial form, enriched later by the Soviet traditions of clandestine operations, political warfare and quasi-legal justifications for territorial expansionism.

It is noteworthy that the Russian word “*принятия*” [*prinyatiya*] used in the text of the 2018 law literally means “to accept,” and not “to annex” or “incorporate.” The authors expressed their confidence that setting this new commemoration date affirms the continuity of Crimea and the city of Sevastopol as part of the Russian state. This legal reasoning contravenes the fact that, in territorial terms, the Russian Federation of today is the successor of the Russian Soviet Federative Socialist Republic (RSFSR) as a constituent part of

Figure 1: Russian lawfare among the Russian hybrid warfare domains

Source: Mark Voyger

LAW AREAS

HYBRID WARFARE DOMAINS	Legal Theory	Customary International Law	Humanitarian Law	Constitutional Law
Political	Uphold ethnic self-determination over state sovereignty in target states.	Emphasize the fluidity of international law over peremptory legal norms.	Assert Russia’s “responsibility to protect” its compatriots in “near abroad.”	Assert supremacy of Russian constitution over international law.
Diplomatic	Assert Russia’s right to “spheres of interest,” blur boundaries between peace and war.	Derecognize neighboring states’ governments to justify Russian invasions and annexations.	Create new ethnic realities on the ground through Russian passports.	Claim the transfer of Crimea to Ukraine contradicted Soviet constitution.
Socio-Cultural	Use history to legalize interventions and annexations.	Assert Russian “cultural values” over individual rights.	Provide Russian citizenship on historical grounds.	Close ethnic minorities’ institutions; accuse them of separatist propaganda.
Information	Claim Russia’s status as the Soviet Union’s legal successor when beneficial.	Portray existing international order as West-centric and unfair toward Russia.	Claim Russian minorities are oppressed and denied language rights.	Claim dissolution of Soviet Union was “unconstitutional” under Soviet law.
Economic/ Financial	Set the legal groundwork to dominate Eurasian economic integration.	Expropriate foreign assets to compensate for assets frozen by the West.	Exert pressure on EU through migration flows.	Subject economic entities to state interests in wartime.
Energy/ Infrastructure	Assert Russian state sovereignty over energy resources.	Oppose Western sanctions against Russia’s energy infrastructure.	Destroy energy infrastructure to justify humanitarian convoys.	Vest the Russian National Guard with the rights to protect infrastructure.
Cyber	Assert Russian state sovereignty over the cyber domain.	Oppose U.S. sanctions for meddling in U.S. elections.	Target Western humanitarian organizations.	Launch cyber attacks on Western electoral systems.
Intelligence	Define Western legal concepts as foreign and subversive to Russia.	Oppose Western sanctions for chemical attacks on U.K. soil.	Collect intelligence during reconciliation campaigns.	Legalize the supremacy of Russia’s security apparatus over individuals’ rights.
Military	Assert Russia’s right of preemptive actions abroad.	Assert right to military exercises within Russia’s borders.	Target civilians to trigger humanitarian crises.	Define Russian military as a pillar of Russia’s domestic order.

the Soviet Union, and not of the Russian Empire, and that the RSFSR only incorporated Crimea from 1922 until 1954.

After the Soviet collapse, the use of lawfare allowed Russia to justify its involvement in Moldova (that enabled the creation of a separatist Transnistria) in 1992, the 2008 and 2014 invasions of Georgia and Ukraine respectively, and the 2014 annexation of Crimea, not to mention Russia's involvement in Syria in 2016, because these were all presented as essentially humanitarian peacemaking efforts. In all those cases, Russia claimed that friendly local populations or governments had turned to it for help, and that Russia felt compelled to answer that call and take those populations under its "protection," thus also assuming control over their ethnic territories and domestic politics. The successful operationalization of this lawfare tool poses serious future dangers for all of Russia's neighbors because it codifies a quasi-legal justification for Russia's "peacemaking operations" that no longer requires only the presence of ethnic Russians or Russian speakers for the Russian state to intervene — it can also be employed to "protect" any population that has been declared Russia-friendly, regardless of its ethnic origin.

All these examples clearly demonstrate how Russia has been trying to amalgamate international and domestic law with categories often as vague and contested as history and culture for the purposes of implementing the Russian hybrid expansionist agenda. While these are nothing more than elaborately fabricated pretexts for Russian aggression, the fact that they have been allowed to stand de facto enables Russia to continue employing them against its various nation-state targets.

21st-century lawfare

International law dealing with conflict between states has evolved to prevent war through negotiations and agreements, regulate the right to go to war and set the rules of engagement,

Russian sailors vote in Russian parliamentary elections in 2016, held illegally on the territory of Russian-occupied Crimea. REUTERS

and normalize postwar relations through cease-fires, armistices and peace treaties. International law, in its modern interpretation, was not intended to sanction and justify the invasion and annexation of territories the way it is being used by Russia against Ukraine. The main systemic challenge that Russian lawfare poses is that customary international law is not carved in stone because it also derives from the practices of states, and thus in many ways is ultimately what states make of it. This fluid, interpretative aspect of international law is being used by Russia extensively and in the most creative ways to assert its numerous territorial, political, economic and humanitarian claims against Ukraine, as well as to harass regional neighbors in its perceived post-Soviet sphere of influence. So far, the existing international system based on treaties and international institutions has failed to shield Ukraine from the aggressive resurgence of Russian hegemony. Ukraine has submitted claims against Russia at the International Court of Justice on the grounds that Russia's activities in Donbas and Crimea support terrorism and constitute racial discrimination, but it has not been able to challenge Russia on the fundamental issues of Crimea's occupation and illegal annexation, and the invasion of Donbas.

While Russia does not have full control over the international legal system, and thus is not capable of changing its rules *de jure*, it is definitely trying to erode many of its fundamental principles de facto. The primary one is the inviolability of European national borders that were set after World War II, codified at Helsinki in 1975 and recognized after the end of the Cold War, including by the Russian Federation. Another legal principle that Russian lawfare severely challenges is the obligation to adhere to international treaties, *pacta sunt servanda*, although the Russian leadership constantly pays lip service to it and regularly accuses other signatories of international treaties and agreements (the United States, Ukraine) of violations or noncompliance. The full domestic and international sovereignty of nation states that is the cornerstone of the existing Westphalian international system is yet another fundamental principle eroded by Russia's actions. To compound things, the universally recognized right of self-determination is used by Russia to subvert Ukraine's unity as a nation state by elevating the status of the ethnic Russian and Russian-speaking Ukrainian citizens in Crimea, Donbas and elsewhere to that of separate "peoples."

Georgians wave their national flag in protest of Russia's de facto annexation of Georgia's South Ossetia region.
AFP/GETTY IMAGES

Russian lawfare actions range from strategic to tactical, depending on specific objectives at any point in time. Some specific examples since the beginning of the Russian aggression against Ukraine include a draft amendment to the law on the admission of territories into the Russian Federation that would have allowed Russia to legally incorporate regions of neighboring states following controlled and manipulated local referenda. This particular draft law was removed from the Duma agenda on March 20, 2014, by request of its authors following the Crimea referendum of March 16, 2014. Nevertheless, the fact that it was submitted to the Duma on Friday, February 28, 2014, barely a day before "little green men" — masked soldiers in unmarked green army uniforms and carrying modern Russian military weapons — appeared in Crimea and its subsequent occupation indicates the high level of coordination between the military and nonmilitary elements of Russian hybrid efforts, especially in the lawfare and information domains.

The legislative onslaught continued in April 2014 with a draft amendment proposing to grant Russian citizenship based on residency claims dating back to the Soviet Union and the Russian Empire, because it was targeting primarily Ukrainians. The annexation of Crimea and the invasion of eastern Ukraine in the spring of 2014 enabled Russia to expand another subversive practice — giving away Russian passports to boost the number of Russian citizens in neighboring states (aka "passportization"). This lawfare technique was used against Georgia to portray the Russian occupation and forced secession of Georgia's Abkhazia and South Ossetia territories as legitimate actions in response to the will of local "Russian citizens," coupled with the newly redefined Russian right of "responsibility to protect." The scope and definitions of that particular right have proven to be extremely flexible since it was proclaimed in the Medvedev Doctrine of 2008. The initial intent to protect Russian citizens abroad later expanded to include the protection of ethnic Russians in Crimea, and then of Russian speakers in eastern Ukraine in 2014. Then in June 2014, Russian President Vladimir Putin postulated the concept of the "Russian World" (*"Russkiy Mir"*) — a supranational continuum composed of people outside the borders of Russia who are to be bound to it not only by legal and ethnic links, but by cultural ones, too. Thus, Russia proclaimed its right to tie an affinity for the Russian culture writ large (Russian poetry, for example) of any category of people to their right to legal protection by the Russian state, which would be understood as a Russian military presence.

In the military sphere, the exploitation of loopholes within the existing verification regime set by the Organization for Security and Co-operation in Europe (OSCE) Vienna Document of 2011 has proven to be particularly advantageous for Russia and difficult for NATO to counter effectively. The most notorious lawfare technique that Russia has been applying since 2014 is the launching of no-notice readiness checks (snap exercises) involving tens of thousands of Russian troops. Such military activities obviate the Vienna Document and run contrary to its spirit and the intent to increase transparency and reduce tensions in Europe. Paradoxically, this is made possible by the loophole contained in Provision 41, which stipulates: "Notifiable military activities carried out without advance notice to the troops involved are exceptions to the requirement for prior notification to be made 42 days in advance." In this case, the Russian modus operandi involves a major Russian news agency issuing a communique on the morning of the exercise stating that President Putin had called Minister of Defense Sergei Shoygu in the early hours of that morning to order him to put the Russian troops on full combat alert — a simple but very powerful technique combining lawfare with information warfare. Russia has also been circumventing the requirement to invite observers to large exercises by reporting lower numbers than the observation threshold of 13,000 troops (the number it provides to the OSCE always curiously revolves around 12,700) or by referring to Provision 58, which allows participating states to not invite observers to notifiable military activities that are carried out without advance notice to the troops involved unless these notifiable activities have a duration of more than 72 hours. In those cases, Russia simply breaks down the larger exercise into separate smaller ones of shorter duration.

Russia has also long been exploiting international law through organizations, such as the United Nations and the OSCE, for a range of purposes, such as blocking adverse U.N. resolutions through its veto power, garnering international support for its actions, or portraying itself as a force of stability and a peacemaker in Ukraine and the Middle East. Russia also reportedly uses those structures for influence operations or for intelligence gathering, for example, by having the Russian observers in the OSCE provide reconnaissance of the Ukrainian military's disposition in the Donbas. Other examples include Russian attempts in 2014 to use the U.N. Security Council to sanction the opening of "humanitarian corridors" in the Donbas; presenting Kosovo and Libya as legal precedents for Russian actions; the sentencing of high-ranking Ukrainian officials in absentia by Russian courts; and multiple Russian allegations that Ukrainian authorities have triggered a humanitarian catastrophe in the Donbas, in an attempt to justify the overt deployment of Russian troops under the guise of "peacekeepers."

Vulnerable areas and relevant responses

Areas that continue to be vulnerable to the effects of Russian lawfare are primarily the territories in Ukraine under Russian occupation, such as Crimea and the Donbas, but also the so-called frozen conflicts in Transnistria, Abkhazia, South Ossetia and Nagorno-Karabakh. They all contain multiple, intertwined and often mutually exclusive historical narratives based on complex socio-cultural realities that provide fertile ground for Russia's presence and involvement under the quasi-legal pretext of stabilization efforts.

Ukraine has also recognized the power of historical narratives as a counter-lawfare tool. According to an August 2018 poll of Ukrainian public opinion by the Rating Group of Ukraine, more than 70% of Ukrainians believe that Ukraine, and not Russia, is the rightful successor of the Kievan Rus. The Ukrainian state must capitalize on those social trends to develop a coherent strategy targeting domestic and international audiences and institutions to counter Russia's malicious exploitation of Ukrainian history for the purposes of disinformation and lawfare-based expansionism.

Similar cultural claims have been used as pretexts by Russia to put pressure even on its traditional allies, such as Belarus. The 2014 Russian military doctrine refers to it as "Belorussia," its Russian imperial and Soviet name, and the Russian military has been pushing to expand its presence in Belarus by requesting additional bases on its territory. Most Belarusians use the Russian language for daily interactions and communication. In the age of Russian hybrid warfare, when culture is used to fabricate legal pretexts, the Belarusian leadership has recognized that very real threat and is taking steps to improve the population's cultural awareness and language skills.

Unresolved border disputes with Russia also pose potential threats because Russia can exploit those to infiltrate NATO territory or to claim that NATO troops are provocatively close to its territories. Russia has been using border negotiations as tools of influence against its neighbors, particularly Estonia. After more than two decades of negotiations, the Russian Duma announced that it would ratify the bilateral treaty on February 18, 2014, less than two weeks before Russian forces infiltrated and occupied Crimea, and likely an attempt by Russia to secure its Western borders with NATO prior to launching its operation in Ukraine. The issue of the Russian-Estonia border was raised again in the summer of 2018, when Russia reneged on its commitment to ratify the treaty, explaining it as a result of Estonia's "anti-Russian" attitudes.

Russia, of course, does not enjoy free reign in the sphere of international law, and it can prove to be a double-edged sword when the targets of Russian lawfare, in particular the Baltic states and Ukraine, decide to use the law proactively to defend themselves. The recent announcement by the ministers of justice of both Estonia and Latvia that they are exploring legal options to demand compensation from Russia — as the legal successor of the Soviet Union — for damages from the Soviet occupation is a timely example of how this internationally recognized Russian legal status can also be leveraged for counterclaims.

Apart from history and culture, Russian lawfare has also integrated and used skillfully the domain of science in the Arctic and the High North, particularly geology, chemistry and oceanography. The 2014 Russian military doctrine clearly identifies "securing Russian national interests in the Arctic" as one of the main tasks of the Russian Armed Forces in peacetime. After ratifying the United Nations Convention on the Law of the Sea in 1997, Russia began to exploit the loophole provided by Article 76 to push for the expansion of its exclusive economic zone from 200 to 350 nautical miles, based on the claim that the Lomonosov Ridge that stretches for 1,800 kilometers under the Arctic Ocean is a natural extension of Russia's continental shelf. The legal and scientific debates over the geological definition and chemical composition of that shelf could have huge ramifications. If Russia's claim ultimately succeeds, according to Eric Hannes in a March 2017 *U.S. News and World Report* article, it would add more than 1.2 million square kilometers, with vast hydrocarbon deposits, to Russian Arctic sovereignty. While waiting for the legal case to be adjudicated by the U.N., Russia has gradually expanded its military presence in the Arctic in a clear attempt to combine legal and lethal arguments in its ongoing quest to dominate this strategic region, as the effects of global warming open its sea routes to navigation.

Tracking Russian lawfare

Lawfare provides numerous advantages to Russia. So far, it has proven to be less recognizable than its counterparts in the information and cyber domains. It successfully exploits the loopholes of international legal regimes, uses diplomatic negotiations as a delay tactic, and can create dissent and confusion among allies by exploiting legal ambiguities. On the other hand, by observing the patterns of Russia's weaponization of the law as an element of its hybrid strategy against target nations, such as Ukraine, Georgia and Moldova, NATO can identify early signs of similar actions targeting other countries in its neighborhood, in particular its Baltic member states. The primary utility of tracking and analyzing Russian legal maneuvers is that acts of lawfare, by default, cannot remain completely secret. They are meant first and foremost to justify Russia's actions in the international arena, and therefore, they must be employed overtly — either as a Russian legal claim, as a new law promulgated by the Russian parliament, as a decree issued by the Russian presidency, or as a troop deployment request approved by the Russian senate.

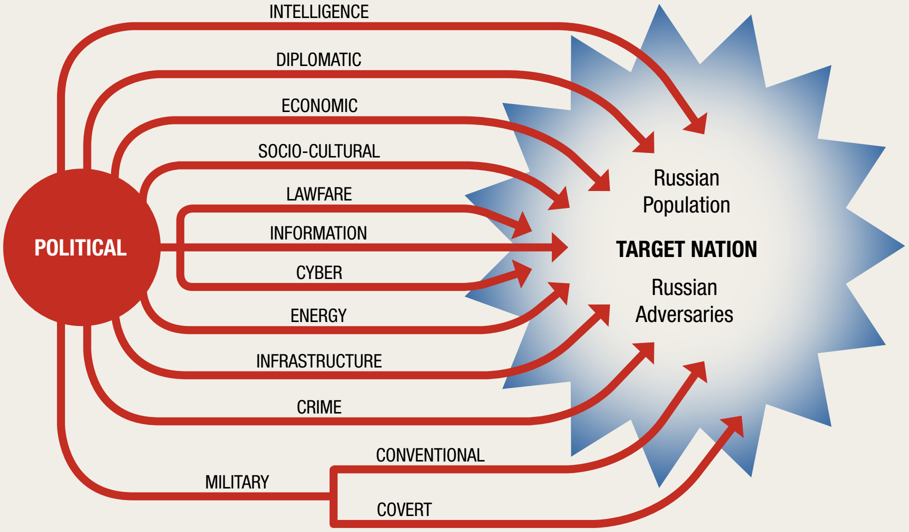
While such overtness may appear paradoxical for a society such as Russia's, where secrecy and conspiracies have traditionally substituted for public policymaking, when it comes to the legal preparation of the battlespace, secret laws cannot serve the Russian leadership to defend their aggressive moves internationally or in mobilizing domestic support. In addition, since the preparation of those highly creative legal interpretations and pushing draft bills through the Russian legislature requires certain procedural efforts, if identified sufficiently early, the process can serve as an advance warning indicating the direction of future Russian political or military steps, both domestically and internationally. To achieve this, the Western analytical community would have to clearly recognize lawfare as a domain of Russian hybrid warfare, and track and analyze Russian legal developments on a continuous basis. The expansion of the DIME model (diplomatic, information, military and economic) of national power to DIMEFIL by adding financial, intelligence and legal, is definitely a step in the right direction, but "L" also should be added to the PMESII (political, military, economic, social, information and infrastructure) analytical framework that describes the effects of the comprehensive preparation of the environment/battlefield through DIMEFIL actions.

Defending against Russian lawfare, of course, is not solely the task of analysts. A comprehensive strategy to counter its tools and impact can only be elaborated on and applied successfully by the coordinated efforts of political and military

Russian-backed rebels march in Ukraine's breakaway city of Luhansk on May 9, 2019, in celebration of the Soviet Union's victory over Nazi Germany in World War II. REUTERS leaders, legal and academic experts, and the institutions they represent across borders and multiple domains. This would require constant and firm emphasis to be placed on upholding and strengthening the peremptory norms of international law at all levels — from the U.N. level through the international courts system to various university law departments. The political leadership and the media organizations of NATO and partner nations must constantly seek to expose proactively (hand-in-hand with the experts in countering Russian information warfare) the ulterior motives and aggressive purposes behind Russia's "peacemaking" campaigns; vehemently oppose Russia's claim to its "responsibility to protect" in its self-perceived sphere of interest; incessantly seek opportunities to close existing loopholes in international agreements that Russia exploits; and as a rule of thumb, always approach negotiations with Russia as a multidimensional chess game that requires constant awareness that Russia's moves look many steps ahead and across all domains.

Figure 2: The intersection of the areas of the law with the PMESII* analytical framework

Source: Mark Voyger



*Political, military, economic, social, infrastructure and information systems

Lawfare Defense Network

Given that lawfare is a pivotal element of Russia's hybrid warfare strategies against Ukraine and the West, the response must be holistic and comprehensive in nature. It would require the building of a network of lawfare study programs (a Lawfare Defense Network) at various universities and think tanks — first and foremost in Ukraine, but also throughout Eastern, Central and Southern Europe, in countries such as Estonia, Latvia, the Czech Republic, Serbia and Georgia, as well as in the U.S. and the United Kingdom. This network's ultimate goal would be to generate interest and support among NATO and EU member states' legislators, political leadership and publics to establish a Lawfare Center of Excellence, just like the ones dealing with strategic communications (Riga, Latvia), cyber defense (Tallinn, Estonia) and energy security (Vilnius, Lithuania). It could be based in a NATO or a European Union member state or in an aspirant country such as Ukraine. Regardless of the future location, Ukraine and the Baltic states must be at the forefront of this initiative, morally, given that they have been the primary target of Russian lawfare for centuries, and practically, by performing the main body of research and analysis of ongoing Russian lawfare activities. Once these programs are established and fully operational at various think tanks and universities, they can focus on their specific country's lawfare challenges to better leverage their national capabilities. The future Lawfare Center of Excellence will then compile and analyze all the national input and provide practical, feasible recommendations to national governments and NATO.

Conclusion

The continuous evolution of Russian lawfare is proof of Russia's legal creativity in bending and reinterpreting international law to achieve its strategic objectives. While Russia publicly demonstrates ostentatious respect for international law, it has undoubtedly espoused a revisionist view of international law based on the concept of Great Powers' spheres of influence and a self-proclaimed right of intervention that challenge the main tenets of security arrangements in Europe and beyond. If its lawfare activities continue unchecked, Russia will be emboldened to continue applying those methods to justify its expansionist and interventionist policies in all areas that it regards as legitimate spheres of interest. Quite inevitably, other great and regional powers have already followed suit and are resorting to lawfare tools to lay claims on contested areas (China) or justify their presence in volatile regions (Iran). The Middle East, Africa and Asia are particularly vulnerable to the application of lawfare, given the disputed, even arbitrary, nature of many state borders there. But some NATO members are also not immune, especially those with sizable Russian-speaking populations or unresolved border disputes with Russia. Russia's use of lawfare as a primary domain of its comprehensive hybrid warfare strategy poses structural challenges to the stability of the international security system and the foundations of the international legal order and, therefore, a cohesive Western response is needed to successfully counter it. □

This article is excerpted from the Baltic Defence College publication, *NATO at 70 and the Baltic States: Strengthening the Euro-Atlantic Alliance in an Age of Non-Linear Threats.*

SHADOW WARS

HYBRID WARFARE IN THE LEGAL AND STRATEGIC GRAY ZONE

By **Lt. Douglas Cantwell,** Judge Advocate General's Corps, U.S. Navy

The best way to boil a frog, the adage goes, is to turn the heat up slowly enough so the frog does not realize it is being cooked. If the perpetrators hacked the stove's software, denied their culpability, and bombarded bystanders with fake news before annexing the kitchen, one might have a workable analogy for hybrid warfare.

Alternately termed nonlinear war, active measures or conflict in "the gray zone," hybrid warfare has no single, agreed upon definition. In the abstract, a state engaging in hybrid warfare foments instability in another state's domestic affairs, prioritizing nonkinetic military means such as cyber and influence operations in concert with economic pressure, support for local opposition groups, disinformation and criminal activity. It may involve the covert deployment of unmarked troops or irregular combatants, though hybrid warfare's reliance on cyber capabilities and nonstate proxies is distinctive. The strategic benefit of hybrid warfare is to obscure the involvement of an aggressor state. Even the thinnest veneer of deniability may delay or fragment opposition to actions that otherwise would invite a vocal, sometimes forceful, international response.

Hybrid warfare is most often associated with aggressive Russian foreign policy over the past decade. Russia's embrace of hybrid warfare has been credited to Valery Gerasimov, chief of the general staff of the Russian armed forces. In 2013, Gerasimov articulated his view of hybrid warfare as an asymmetrical response to the spread of liberal democracy in a globalized world, although Russian writings, including Gerasimov's, do not actually use the term hybrid warfare but rather "nonlinear" or "new generation" warfare. It is a corollary to Carl von Clauswitz's conception of war as politics by other means. Gerasimov observed "the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness." Consequently, he advocated the "broad use of political, economic, informational, humanitarian, and other nonmilitary measures — applied in coordination with the protest potential of the population," to be "supplemented by military means of a concealed character."

Observers may disagree about which cases should be classified as hybrid war. Russia's 2008 invasion of Georgia and the resulting de facto annexation of Abkhazia and South Ossetia, its actions in 2014 to seize and annex Crimea, and its deployment of "little green men" leading to the

A U.S. Navy photo shows a Russian Sukhoi Su-24 attack aircraft making a low pass by the guided missile destroyer USS Donald Cook in the Baltic Sea in April 2016. Two Russian warplanes flew near the destroyer in what one U.S. official described as an aggressive interaction.
REUTERS

declaration of the Donetsk People's Republic and Luhansk People's Republic in eastern Ukraine are the clearest examples of Russian hybrid warfare applied to full effect. However, hybrid war need not result in the annexation of territory. A disinformation campaign fomenting anti-government riots followed by a cyber attack crippling Estonia's digital infrastructure in 2007, orchestration of elaborate coup attempts in Macedonia in 2016 and Montenegro in 2017, support for right-wing political parties in France and Germany, and interference in the 2016 United States election all fit within Gerasimov's description of hybrid warfare. Rather than merely a descriptor for isolated cases or a constellation of tactics, hybrid warfare is better understood as a grand strategy aimed at destabilizing the existing liberal order.

Conceptually, framing hybrid warfare as an innovation in international affairs has drawn criticism. All states engage in some forms of covert action and nonmilitary measures constitute essential tools of diplomacy. Additionally, hybrid warfare resembles operations undertaken by both opposing blocs during the height of the Cold War and by many modern states under the heading of irregular warfare. Skeptics have therefore questioned whether, aside from the introduction of cyber capabilities and the name itself, there really is anything novel about hybrid war. States on the front lines facing the particular hybrid threat posed by Russia have answered that question in the affirmative, investing in strategic thinking on how best to counter hybrid warfare techniques. In April 2017, a group of 11 NATO and European Union member states signed a joint memorandum of understanding in Finland, establishing the European Centre of Excellence for Countering Hybrid Threats in Helsinki. The center, inaugurated in October 2017, engages in strategic dialogue, research, training and consultation to illuminate vulnerabilities to hybrid measures and improve resilience against hybrid threats.

Chief of the General Staff of Russian Armed Forces Valery Gerasimov, credited with initiating Russia's hybrid warfare strategy, sits next to Russian President Vladimir Putin during a visit to the National Defence Control Centre in Moscow to oversee the testing of a new Russian hypersonic missile in December 2018. REUTERS

Hybrid war under international law

Understanding the relationship between hybrid warfare and international law governing the use of force is central to countering hybrid threats. Hybrid measures have been employed, with increasing success, to undermine existing international protections for the territorial integrity and political independence of states. Foremost is the ban on aggressive war. Hybrid warfare has created a new vehicle for aggression, identified as the "supreme international crime" in 1946 at the International War Crimes Tribunal at Nuremberg. Outlawed by the Kellogg-Briand Pact, enforced during the tribunals at Nuremberg and Tokyo, prohibited in the United Nations Charter, and reaffirmed in the Kampala amendments to the Rome Statute of the International Criminal Court, states endorse with near unanimity the general principle that aggression violates international law.

The rub lies in attempting to define aggression and enforce its prohibition in particular cases. Incorporation of a defined crime of aggression under the jurisdiction of the International Criminal Court represents measured but uncertain progress. Aggression has not been enforced judicially since Nuremberg. States continue to disagree about the definition of aggression and powerful states that are not party to the Rome Statute — including the U.S., India, China and Russia — have not committed to the particular definition codified in the amendments. However, states, both unilaterally and multilaterally, have acted to counter aggression. Formation of an international coalition to expel Saddam Hussein's forces from Kuwait in 1990-91 stands as the high-water mark of marshaling collective will to forcefully counter aggression. But modern cases of aggression rarely involve a blitzkrieg of tanks and uniformed forces rolling across an international border to take a neighboring state's capital. Few have drawn such a swift and forceful response as Operation Desert Shield and Operation Desert Storm. In cases where an act of aggression may be less immediately apparent or where the status of either the victim or aggressor state discourages a forceful response, nonforceful measures such as economic sanctions, diplomatic censure and verbal condemnation may be employed. Such was the case following Russia's actions in Georgia and later in Crimea and eastern Ukraine. That there was widespread

A Latvian border guard keeps watch at the border with Russia, near Pasiene in eastern Latvia. A large proportion of Latvians are ethnic Russians targeted by Russia's disinformation war. AFP/GETTY IMAGES international condemnation of Russia bolsters the general prohibition against aggression. That the international response has not resulted in a return to the status quo places Russia's actions in Georgia and Ukraine among a handful of instances where a state has redrawn post-1945 borders with force, not simply occupying but annexing territory. As such, it is important to situate hybrid measures within the existing law they seek to circumvent.

The U.N. Charter prohibits aggression through its ban on uses of force without legal justification. Article 2(4) guarantees the right of states to be free from any threat or use of force against their territorial integrity or political independence. Prohibited uses of force encompass, but need not reach, the level of an armed attack, the basis for self-defense under Article 51 of the U.N. Charter (as well as the collective defense provision contained in Article 5 of the Washington Treaty of 1949 establishing NATO).

Unlawful uses of force that violate Article 2(4) generally require forces engaging in military activities, whether traditional armed forces and nonstate armed groups, as detailed in International Court of Justice (ICJ) rulings, including a 1986 decision regarding U.S. actions in Nicaragua and a 2005 decision regarding Uganda's actions in the Democratic Republic of the Congo. This framework has proven capable of accounting for changes in the means through which states wage war. For example, in the context of cyber operations, the Tallinn Manual, a treatise on the application of existing international law to cyber space drafted by an international group of experts, affirms that cyber operations may constitute unlawful uses of force if they are attributed to the armed forces of a state or if their effects mimic those of traditional military operations. In theory then, the U.N. Charter's prohibition on the use of force is sufficient to account for hybrid threats when they resemble traditional military activities — for example, when unmarked troops engage in hostilities — but also when a state employs cyber capabilities in a hybrid war campaign to damage or disable infrastructure in a way that resembles the use of bombs and bullets.

In practice, hybrid measures are designed to avoid being identified as clear violations of the Charter, even when they do constitute an unlawful use of force. One way this is achieved is through an emphasis on covert action. States have long engaged in covert operations that may run afoul of Article 2(4)'s prohibition on nonintervention, as Alexandra H. Perina argues in a 2015 article in the *Columbia Journal of Transnational Law*. While reasons for engaging in covert action vary and are often mixed, uses of force may be done covertly at least in part to honor international law in the breach. Maintaining public deniability limits the establishment of *opinio juris* for acts that blatantly violate the

Pro-Russian fighters withdraw from the village of Petrovske, 50 kilometers from Donetsk, Ukraine, as part of a demilitarization accord in October 2016.
AFP/GETTY IMAGES

charter — important for maintaining an international system that has prevented major power war since 1945. In the context of hybrid warfare, such benevolent motivations should not be assumed. Covert means are crucial to a hybrid warfare strategy not because covert actions may discourage open violations of the charter by others, but because it exploits the weakness of an international enforcement regime where the status quo is often inaction, particularly in those cases where aggressor states have sown doubt as to attribution or the legality of their behavior.

Other hybrid measures are simply not accounted for by the charter's prohibition on the use of force. For example, economic measures traditionally do not violate Article 2(4). Disinformation and criminal activity generally also fall below this threshold. However, actions not constituting use of force may still be unlawful as a form of interference. Sovereign noninterference is implicit in the doctrine of sovereign equality, enshrined in Article 2(1) of the charter. The U.N. General Assembly has opined on the concept. In a 1965 declaration, the assembly described interference as "the subordination of the exercise of [a state's] sovereign rights" up to and including the violent overthrow of a state's government. In a 1970 declaration, the assembly highlighted the ban on intervention in the internal or external affairs of any other state along with "all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements."

Interference may be understood as a lesser-included offense of intervention. The controlling expression is contained in the ICJ landmark 1986 Nicaragua decision. In Nicaragua, the court emphasized the right of all states to decide issues inherent to state sovereignty, to include a state's political, economic, social and cultural system and the formulation of its foreign policy. When those choices are influenced by methods of coercion, including through subversion or indirect force, that constitutes unlawful interference.

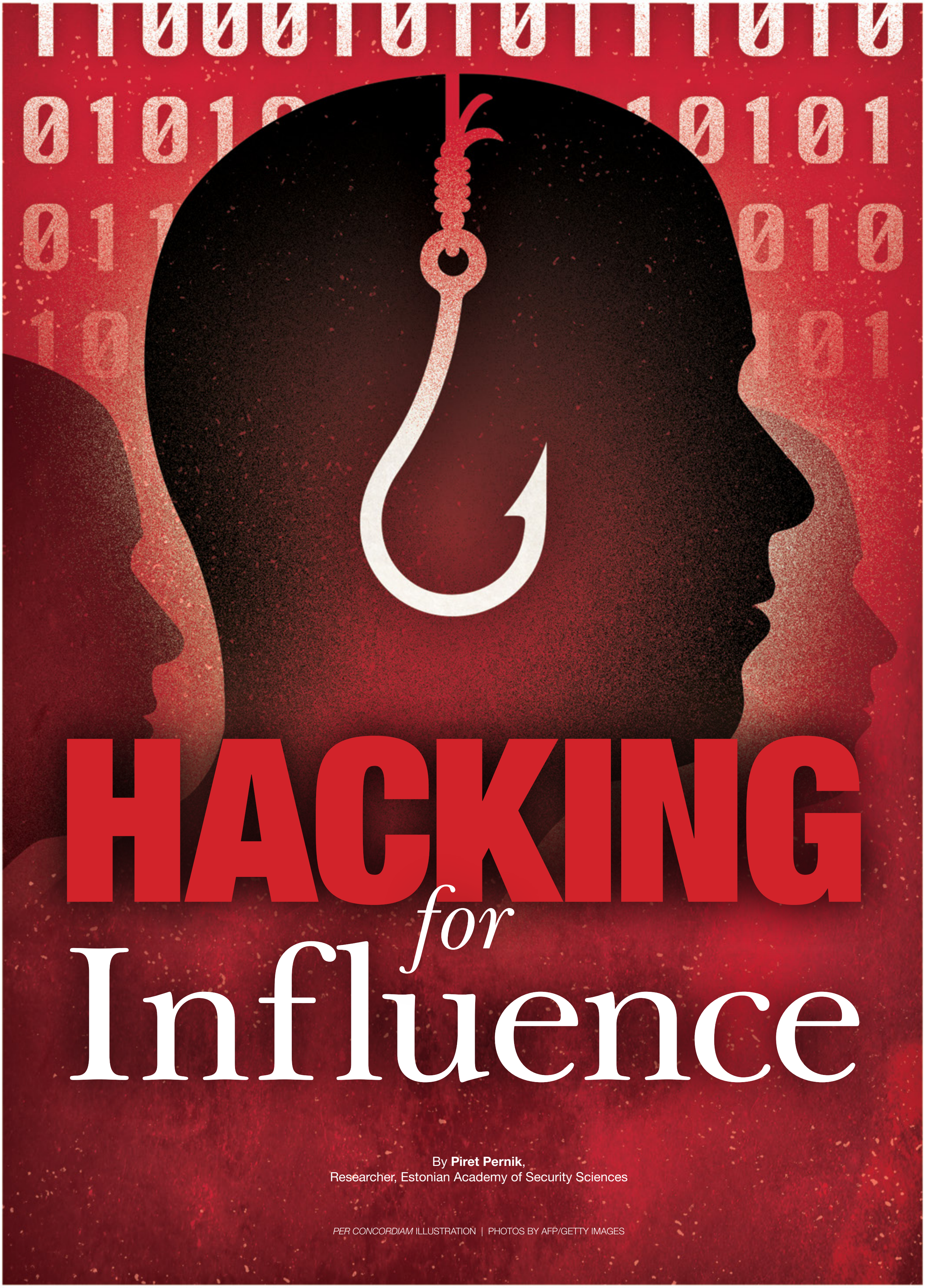
The charter framework, therefore, is at least conceptually sufficient to address hybrid measures short of the use of force. However, as Tom J. Farar wrote in a 1985 paper for the *American Journal of International Law*, since Nicaragua the contours of what constitutes coercive interference have remained murky. Lack of clarity and a threshold that has placed interference nearly on par with intervention have left gaps that hybrid measures may exploit. No single element of a hybrid campaign may present a clear case of coercive interference when viewed in isolation. However, constant, coordinated interference intended to destabilize a government may violate the spirit, if not the letter, of the charter's protections for the political independence of states. While a state with robust civic institutions may be able to withstand a trumpet blast of false news stories, riots and strategic leaks of information intended to undermine elections, smaller states in particular may find themselves overwhelmed. As such, it is important that coercive acts be recognized, scrutinized, and subject to a swift and coordinated response where necessary by those states and international and nongovernmental institutions seeking to uphold protections on political independence enshrined in the charter. Likewise, coercive acts must be distinguished from actions taken transparently and lawfully by states, which may exert diplomatic pressure without it constituting illegal interference.

Ukrainian naval ships seized by Russia's Federal Security Service are anchored in Crimea in November 2018.
REUTERS

Conclusion

A complete understanding of hybrid war as a strategic concept requires that it be properly situated within the existing regime governing the use of force under international law. Addressing legal aspects of hybrid conflict in turn requires proper acknowledgment of hybrid campaigns that amount to aggression and more robust theorizing on what hybrid measures constitute coercive interference. In that sense, efforts such as the establishment of the European Centre of Excellence for Countering Hybrid Threats are a welcome development. Its supporters should ensure that the growing body of work around hybrid warfare incorporates the established lexicon of international law, an important step toward clearing the fog of war in the gray zone. □

The views expressed are those of the author and do not represent the U.S. Navy, the Department of Defense or the U.S. government. A version of this article appeared in the American Society of International Law publication, *Insights*.



HACKING *for* Influence

By **Piret Pernik**,
Researcher, Estonian Academy of Security Sciences

PER CONCORDIAM ILLUSTRATION | PHOTOS BY AFP/GETTY IMAGES

Cyber attacks are key to Russian information warfare

In recent years, liberal democracies have found themselves increasingly subjected to nonkinetic attacks from authoritarian countries, especially in cyberspace. All nation states — democratic and authoritarian — have traditionally used cyber capabilities to gather intelligence in foreign countries, but today low-intensity political warfare in cyberspace has become more prominent. Unfortunately for democratic countries, cyberspace is an ideal environment in which to undermine democratic processes and institutions using diverse covert activities.

Authoritarian states and their proxies use cyber attacks in support of other influence activities. In cyberspace, the major state adversaries to democratic countries are China, Russia, Iran and North Korea. Among them, China and Russia have developed mature information warfare and information operation strategies and tactics, and Iran is effectively copying their activities. While the focus here is on Russian theory and practice in using cyber attacks for soft subversion, it should be emphasized that China's approach is similar. Both see free information and foreign technologies as threats to their "cyber sovereignty" and seek to control cyberspace and the information contained within. Similarly, neither distinguishes between peacetime and wartime information-related activities. They have long traditions of strategic thinking about the role of information in projecting national power and holistic understandings of the information space. It is unlikely that China's or Russia's strategies will change remarkably any time soon.

Russian and U.S. viewpoints

Russia's primary strategic documents (the Military Doctrine of the Russian Federation of 2014 and the Russian Federation's National Security Strategy of 2015) identify the use of information and communications technology for political and military purposes as a main security and military threat. They depict Russia's information counterstruggle as a defensive measure and a strategic priority in peacetime and wartime alike. Moscow perceives European Union and NATO enlargement and the "color revolutions" in former Soviet republics as threats to Russia's geopolitical interests and national security. Information of Western origin is consequently perceived as a security threat and the information environment as a domain of operations.

> Russia regards its information warfare against the West as a "threat-neutralizing measure" to deter what it perceives as hostile activities.

Against this backdrop, Russia regards its information warfare against the West as a "threat-neutralizing measure" to deter what it perceives as hostile activities. In this way, information freedom and its medium, the free and open internet, become Russian targets. This view, which may seem paranoid to some, is expressed frequently by senior Russian government officials and key leaders. For example, President Vladimir Putin's spokesman, Dmitry Peskov, claimed that

Russia is "in a state of information warfare with the trendsetters in the information space, most notably with the Anglo-Saxons, their media." Sergey Kislyak, the former Russian ambassador to the United States, claims that the U.S. runs "a massive propaganda campaign … with the purpose of undermining the internal political atmosphere in Russia." According to journalist and author Andrei Soldatov, the Kremlin genuinely believes it is under attack from the West, and Russia's strategic activity is, therefore, always reactive. However, according to Dmitry Adamsky in a 2015 paper for the French Institute of International Relations, in the Russian view, deterrence in the information space can coerce an opponent's behavior in the other domains of operations.

The Russian concept of information warfare can be described as *informatsionoye protivoborstvo* (information confrontation or counterstruggle). The Russian defense ministry defines its purpose as "to inflict damage on [an] opponent by means of information in [the] information sphere." The main mechanisms to cause harm are divided into information-psychological and information-technical tools. Technical tools are low-level cyber attacks (for instance, unauthorized access to information resources). The end goal is a change in the strategic behavior of an adversary, which is achieved by manipulating their picture of reality and consciousness through technological and psychological components of the counterstruggle.

> "For Russia, the objective of psychological activities is to affect the will, behavior and morale of the adversary, and the more subtle emotions that impact rational thinking." ~ V.A. Kiselyov, *Military Thought*

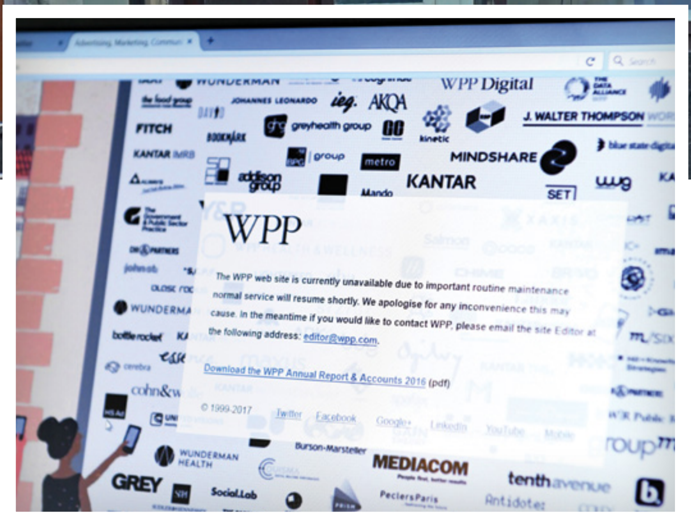
Psychological measures encompass anything that can be used to influence the general population and armed forces personnel. V.A. Kiselyov, in a 2017 article for the Russian journal *Military Thought*, tells us that, for Russia, the objective of psychological activities is to affect the will, behavior and morale of the adversary, and the more subtle emotions that impact rational thinking. Adamsky describes this activity, known as reflective control, as a state attempting to predetermine an adversary's decisions in such a way that the adversary believes it is behaving in its own interests. According to Russia's military doctrine, information warfare in modern conflicts does not solely target an adversary's key decision-making, but extensively uses "the protest potential of the population." U.S. military doctrine is much less nuanced in the area of psychological influence on the population. It states simply that the aim of information operations is to create doubt, confuse and deceive, and to influence decision-makers, militaries and various other audiences, but it is silent on the need to manipulate the sentiments of the population. According to Adamsky, Russia views the main battlefield as human consciousness, perceptions and strategic calculations. Prominent Russian information warfare expert Sergei Modestov says there are no borders in the battlefield of the cognitive domain. The borders are blurred between war and peace, tactical, operational and strategic levels of operations, forms of warfare (offensive and defensive) and coercion.

Two key aspects distinguish Russia's understanding of the information confrontation from the U.S. military's view of information operations. In the Russian view, it is first conducted constantly during peacetime and, secondly, it is a strategic-level activity executed by a whole-of-society response that recalls the Soviet-era concept of total defense, according to which all the resources of civil society were used for national defense. Russia expert Mark Galeotti, in a 2016 article for the European Council on Foreign Relations, described how the Kremlin carries out this holistic approach by outsourcing the policy implementation to volunteers, organized-crime groups, business, the Russian Orthodox Church, government-organized nongovernmental organizations, the media and other actors in the deployment of various active measures. By contrast, the U.S. military perceives information operations as a wartime activity executed by designated authorities whose action is legally constrained by their mandates. For the U.S., this activity is conducted at the operational level.

In several respects, the U.S. and Russian views also display similarities. For Russia, Kiselyov asserts, violent physical acts, such as "kidnapping adversary officials" and "physical destruction of adversary assets and targets," are also psychological tools. Likewise, the U.S. includes physical destruction among information operations tools. Accordingly, actions in the domains of operations (land, air, sea, space and cyber) can have psychological effects. Both countries reckon that cyber attacks are part of the information warfare toolkit, and that information-related activities are to be conducted simultaneously in the cyber and physical spaces. Both countries include defensive activities (e.g., operational-level security, and protecting their own infrastructure, networks and forces) as part of information warfare, and they agree that the ultimate objective of information warfare is information superiority. Russia emphasizes information-psychological capabilities because the control of information, including internet content and physical infrastructure, is seen as security for the survival of the regime. In contrast, the U.S. emphasizes information-technological capabilities.

Asymmetric measures

Russian foreign policy instruments can be divided into six broad categories: governance, economics and energy, politics and political violence, military power, diplomacy and public outreach, and information and narrative warfare, as outlined by Robert Seely in a 2017 paper for *RUSI Journal*. In addition to the traditional tools of national power, Russia uses a mix of covert influence tools referred to as active measures. In a way, the Kremlin has weaponized every factor of modern life at the personal, organizational, nation-state and global level — culture, history, nationalism, information, media and social media, the


WPP

The WPP web site is currently unavailable due to important routine maintenance normal service will resume shortly. We apologise for any inconvenience this may cause. In the meantime if you would like to contact WPP, please email the site Editor at the following address: editor@wpp.com.

Download the WPP Annual Report & Accounts 2016 (pdf)

© 1999-2017 Twitter Facebook Google+ LinkedIn YouTube Mobile

Customers try to enter a closed branch of Oschadbank in Kyiv, Ukraine, in June 2017. A wave of cyber attacks wreaked havoc on government and corporate computer systems as it spread to Western Europe and across the Atlantic.

The homepage of British advertising giant WPP is pictured after it became one of several multinational companies targeted in a cyber attack that started in Russia and Ukraine before spreading to Western Europe in June 2017.

internet, business, corruption, electoral processes and globalization. In this struggle, information has been rendered a target, disinformation a weapon, and the internet a battlefield.

One of the principal threats posed by a democratic worldview to the Russian model of governance is the principle of freedom of expression, including its manifestation in a free and open internet. The internet can whip up protests and uprisings — the color revolutions, for example — and the Kremlin fears that an Arab Spring-like upheaval in Russia could sweep it from power. The Kremlin's fear of a free and open internet was expressed by Putin in 2014 when he claimed it was a "CIA project" from which Russia needed to be protected. For this reason, a multistakeholder internet governance model is perceived by Russia and many other authoritarian countries as inherently dangerous. These governments intend to increase their control over cyberspace content and physical infrastructure, as well as software and hardware. Whether for defensive or offensive purposes, or a mixture, Russia has used cyberspace to conduct political influence activities at the strategic level against many EU and NATO member states, as well as in the Western Balkans, the South Caucasus and Central Asia.

Each country is vulnerable to Russian active measures in different ways. Galeotti distinguishes seven types of Russian influence strategies that seek to exploit specific weaknesses and allegiances in individual countries. For example, Bulgaria and Greece have two types of vulnerabilities: a Russia-friendly political and business elite and weak democratic institutions. Russia cultivates a strategy of "state capture" by attempting to make these countries Trojan horses within the EU and NATO. Hungary, Romania and Montenegro also have weak institutions, but their affinity to Russian interests

> "The beginning of wisdom is to understand that the Russian pursuit of influence is a continuous, background effort not confined to 'influence operations.' It is labour as well as resource intensive, built on local knowledge, the cultivation of individuals and the long-term development of networks."
>
> ~ James Sherr, foreign policy expert

is moderate. Russia therefore seeks to influence them only on specific issues (e.g., EU sanctions) by cultivating a strategy that targets the state.

The remaining strategies are, according to Galeotti, exploitation (in the United Kingdom), demonization (in Estonia and Poland), disruption (in France, Germany, the Netherlands and Sweden), influencing (in the Czech Republic, Italy, Latvia and Lithuania), and social capture (in Slovakia). In the information environment, Russia has likewise cultivated specific memes and narratives to influence different countries. It has used social media bots to influence public opinion in the U.S., the U.K., the Netherlands and Spain. In Hungary, the Czech Republic and Austria, it used a multitude of local political, economic and disinformation actors, according to the 2017 paper "Does Russia Interfere in Czech, Austrian and Hungarian Elections?" Russian disinformation practices in Europe show that specific influence tools are chosen after considering particular strengths (e.g., free speech) and vulnerabilities to be exploited and the expected effects. Russia deemed social media to be an effective medium for covert disinformation activities in the U.S. That enabled it to target selected demographic groups in certain geographic areas over great physical distance with low risk of escalation. In several Central and Eastern European countries, physical influence activities (corruption and cultural, national and other allegiances) yielded better strategic-level effects than the abuse of social media platforms would have achieved.

Hence, Russia exacerbates various socio-economic and ideological grievances in Western societies related to processes such as globalization, technological innovation, nationalism, fundamentalism, immigration and climate change. In addition

A Russian aircraft arrives at Dulles International Airport outside Washington, D.C., in December 2016 to pick up Russian diplomats expelled as part of sanctions imposed on Russia for suspected cyber attacks during the United States elections.

to country-specific vulnerabilities, it exploits the openness and freedom of democratic systems. In the words of James Sherr, an expert on Russian foreign policy, "attributes of the liberal polity that normally are a source of strength, e.g., 'fairness,' can also be used to undermine liberal democracy and advance hostile objectives."

He writes: "The beginning of wisdom is to understand that the Russian pursuit of influence is a continuous, background effort not confined to 'influence operations.' It is labour as well as resource intensive, built on local knowledge, the cultivation of individuals and the long-term development of networks."

Many experts take the view that Russia's approach to the information confrontation has been constantly evolving, developing and adapting, and others believe that in the process it has become refined and tailored.

To sum up, the Soviet-era experience in the use of active measures and intimidation has been adapted and elaborated for modern use. Asymmetric tools that can be outsourced to various actors are attractive for projecting Russian national power due to their low cost and wide availability, a degree of anonymity and stealth, a low risk of escalation and great destabilizing potential, as described in a 2017 Atlantic Council report. What perhaps distinguishes Russia, according to Seely, is that asymmetric activities are highly integrated with one another and coordinated with conventional operations in early and defining phases of military conflict (e.g., kinetic operations in Georgia and Crimea).

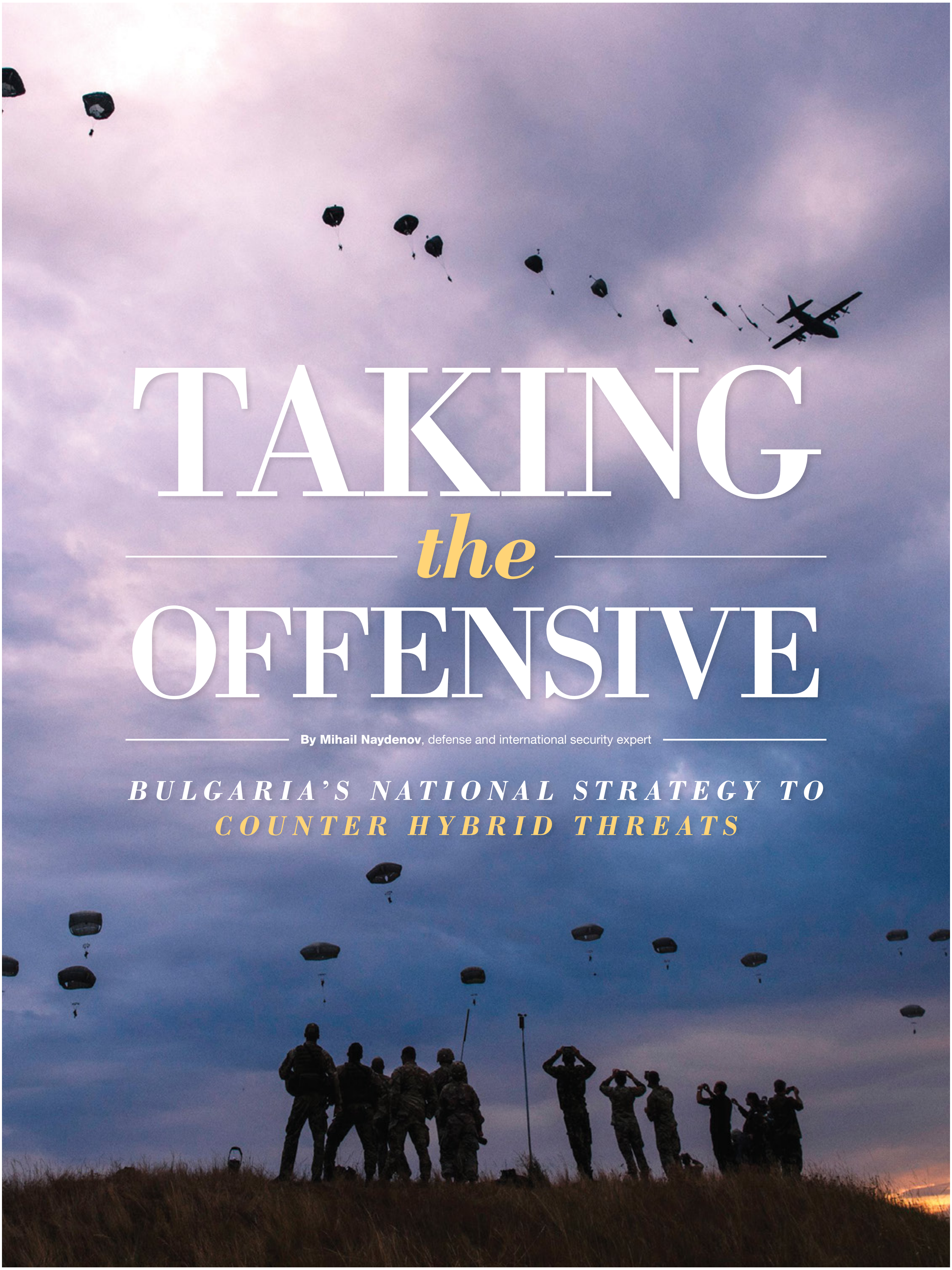
The prison jacket of Enn Tarto, an Estonian former political prisoner who spent years in Soviet jails, hangs in the hall of Tallinn's Occupation Museum as a reminder of Russia's past subjugation of its neighbors.

Conclusion

The unique nature of cyberspace makes it an ideal domain for gray zone cyber attacks and other cyberspace-enabled political influence activities. Cyber capabilities differ from kinetic weapons in many respects, and conventional concepts fail to account for the dynamics in this complex domain. Cyber espionage seems to have strategic effects, while low-end cyber attacks tend to produce tactical and operational effects; however, together with psychological operations, they can have strategic effects on national security. Armed forces use cyber attacks in kinetic conflicts and also outside a conflict zone against civilian targets. They are conceived as force multipliers in support of operations in other domains and sometimes replace the kinetic use of force. In some cases, cyber attacks likely have psychological effects of their own, but there is still little understanding about the scope of possible impacts. There is also little understanding about the strategic effects of cyber attacks for national security and interstate relations. For this reason, past cyber attacks deserve better scrutiny.

Russia does not apply a uniform cyber-attack strategy across all targets but considers various opportunities innovatively as they emerge. Cyber attacks are ideal weapons for authoritarian states to project national power and support other political influence activities. They can be used for deterrence and coercion, but a better international relations theory for cyberspace should be developed to explain how cyber attacks translate into deterrent or coercive effects. Quantitative and qualitative methods, and operational and strategic level analysis, should be combined to develop a new theoretical and conceptual framework for understanding this fast-evolving domain and how authoritarian states are exploiting it. □

This is an abbreviated version of an article published by the International Centre for Defence and Security in Estonia.



TAKING the OFFENSIVE

By **Mihail Naydenov**, defense and international security expert

BULGARIA'S NATIONAL STRATEGY TO COUNTER HYBRID THREATS

The Kremlin's hybrid warfare campaign against NATO and the European Union — in particular the subversive activities against Eastern European members — is the most substantial challenge to allied and Bulgarian security. Bulgaria, being a NATO and EU eastern-flank member state, is significantly exposed to Moscow's systematic subversion strategy aimed at obstructing the building of a strong national security and defense system. This is detrimental to Bulgaria's efforts to become a strong security provider within NATO and the EU.

To quickly and effectively remedy this perilous state of affairs, Bulgaria must immediately embark upon a coherent program to strengthen the institutional capacity to counter hybrid threats, regardless of the source. As a first step, Bulgaria should — as soon as possible — write and adopt a national strategy for countering hybrid threats. This document should be fully harmonized with the NATO and EU documents in this sphere of growing relevance, especially with the Alliance's strategy for countering hybrid warfare (2015) and the EU's "Joint Framework on countering hybrid threats - a European Union response" (2016).

The good news is that in 2018 Bulgaria updated its 2011 National Security Strategy, and hybrid threats have been duly incorporated, coupled with a sound reassessment of the external security environment after Russia's illegal annexation of Crimea in 2014. The ongoing shift in the geostrategic and military balance of power in the Black Sea region is also taken into consideration. Moreover, Sofia updated its National Defense Strategy in 2016 to better enable its defense organization to meet the growing challenges of hybrid war. Nonetheless, these steps are not enough, given the gravity of today's challenges. Therefore, it is necessary for Bulgaria to have a new strategic document that explicitly addresses hybrid threats.

A NATIONAL STRATEGY

It is high time for a Bulgarian national strategy for countering hybrid threats. It should support the implementation of the updated National Security Strategy. Being focused on countering hybrid threats, this strategy would guide all national policies in this field. It should serve as a key enabler, making national efforts for countering hybrid threats well-coordinated, effective and efficient. The document should make a realistic analysis of existing national weaknesses and identify the right ways and means to deal with hybrid threats, taking into consideration the resources available. This strategy must make unambiguously clear what the problem is and how to solve it.

NATO paratroopers jump from a U.S. Air Force Hercules during the Swift Response 17 joint airborne military exercise at Bezmer airfield in Bulgaria. Bulgaria is integral to the defense of NATO's eastern flank. AFP/GETTY IMAGES

Writing this strategy should be an interagency effort, bringing together all the relevant Bulgarian institutions under the general coordination of the Council of Ministers. The participation of people from various structures, such as the ministries of defense, interior, foreign affairs, finance, economy, energy and transport, and the intelligence and counterintelligence agencies, and other relevant bodies, would support improved interagency coordination. NATO and the EU should be consulted to incorporate the best practices and lessons learned to date. The document should be approved by the government and endorsed by parliament. Bulgaria has begun a review of its national security protection system and strategic defenses. This is the time to create such a document and to fix the existing gaps in the national security system regarding countering hybrid threats.

A man protests Russia's invasion of Ukraine in March 2014 as he stands in front of the Soviet Army Monument in Sofia, Bulgaria, with a sign equating the Soviet Union with Nazi Germany. Bulgaria, a former Warsaw Pact Soviet client state, is uniquely vulnerable to Russian hybrid warfare tactics. AFP/GETTY IMAGES

The first aim of this effort is to address strictly national Bulgarian weaknesses. This is the reason why its text should be centered on the most demanding existing domestic vulnerabilities that are now, or could possibly be, exploited by external hostile powers. In this respect, its table of contents should contain the following topics at a minimum:

The introduction must first answer the question of why the strategy is critically needed. It should make crystal clear what it aims to achieve. A concise description of hybrid war and hybrid threats should be given, without delving too deeply into theoretical and academic details. Most important, it should emphasize that hybrid war is not "declared," and that it is already being fought,

NOWADAYS, MANY COUNTRIES IN EUROPE ARE VULNERABLE TO HYBRID THREATS, PRIMARILY DUE TO THEIR INABILITY TO UNDERSTAND THE NATURE AND TIMING OF THE ATTACK, OR EVEN THAT THEY ARE UNDER ATTACK AT ALL.

A Bulgarian military honor guard attends a flag-raising ceremony in 2014 in the capital, Sofia, to mark the 10th anniversary of Bulgaria joining NATO. REUTERS

a practical lesson to be learned, the sooner, the better. Nowadays, many countries in Europe are vulnerable to hybrid threats, primarily due to their inability to understand the nature and timing of the attack, or even that they are under attack at all. Therefore, they are not able to assess what is really happening and hence, to effectively organize their defenses. As hybrid war is above all a war of perceptions, if a country is under hybrid attack and its leaders are unable to comprehend that they are de facto in an undeclared war, then defeat is only a matter of time. Such a strategy helps decision-makers understand as early as possible whether their country is under hybrid attack through the monitoring of specific indicators.

A realistic analysis of the fundamentally changed European security environment since 2014 should be incorporated, focusing on: Bulgaria's regional perspective and especially on Black Sea regional security in the context of Russian aggression against Ukraine, frozen conflicts, the militarization of Crimea, the buildup of Russian naval forces, and growing Russian anti-access/area denial capabilities. Based on an analysis of the strategic environment, this document should explicitly spell out the main sources of hybrid threats to Bulgaria.

A detailed chapter with solid evidence should be dedicated to concrete national vulnerabilities to hybrid threats. This means spotlighting specific areas of hybrid activity against Bulgaria. This could be a difficult analysis and at some point might be politically sensitive. But its inclusion in the strategy is a necessity if the document is to have teeth and deliver results. Without claiming to cover all potential areas, this chapter should contain at a minimum the following topics:

- The penetration by external powers of internal Bulgarian political processes, and the national decision-making and internal political actors supportive of foreign hybrid intrusions.
- The activities of foreign intelligence services in Bulgaria.

- Media manipulation — the use of the internet and social media for manipulating public opinion, spreading fake news, and promoting anti-EU, anti-NATO, anti-Western and pro-Russian narratives.
- The concentration of, and lack of transparency about, media ownership and the potential to launch media projects that can be used for hybrid activity.
- Energy dependence on Russia as a key enabler of hybrid activity against the state and Bulgarian society.
- The use of economic relations to influence political decision-making.
- The rule-of-law deficit as a breeding ground for hybrid activity.
- Corruption and organized crime as tools that could be exploited for hybrid war purposes.
- Subversive Russian actions against building a strong Bulgarian defense system.
- The existence and functioning of pro-Russian paramilitary groups.
- Critical infrastructure vulnerabilities.
- Cyber attacks as a hybrid warfare tool.
- The risk of illegal migration and the potential for external powers to use it as a tool to carry out hybrid activity.

Another chapter should be dedicated to providing specific recommendations and options for bridging identified gaps. This would help strengthen national resilience to hybrid threats. Resilience is understood as the capacity to prevent a threat from materializing and, if it nonetheless does, the ability to rapidly recover and return to normal. The NATO vision for dealing with hybrid threats focuses efforts in three main directions — preparation, deterrence and defense. As a NATO ally, Bulgaria should use this strategy to translate the NATO vision into actions on the national level.

To be successful in countering hybrid threats requires putting due emphasis on cooperation and coordination. This is a two-tier activity, having internal and external dimensions. This should be the content of the next chapter of the strategy. The first tier is developing and improving internal, interministerial and interagency coordination in tackling hybrid threats. The strategy should propose measures to make interaction among national-level institutions effective and rapid, emphasizing the improvement of early-warning and quick-reaction capabilities. Designating a state-level coordinating body, most logically a structure under the prime minister, together with adopting strict procedures for effective interinstitutional interaction, should also be taken into consideration at this juncture. The second tier consists of integrating more into NATO and EU processes, procedures and structures. Working more closely within NATO and EU frameworks, and thus sharing best practices and seeking joint solutions, would be of critical importance to successfully dealing with the challenges of today and tomorrow. A good step forward for Bulgaria would be to join the European Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland, which helps participating countries build capabilities and enhances EU and NATO cooperation in countering hybrid threats.

Another chapter of the strategy should be dedicated to the resources needed to effectively deal with hybrid threats and, in particular, the requirement to ensure sufficient financing of the national security sector, including the military. To this end, NATO allies have committed to spend 2% of their gross domestic product on defense.

Lastly, the strategy must be a living document, open to periodic review, so that evolving security challenges are taken into account. The timeline of the document (at least five years) and the mechanism for reviewing and updating it should be recorded in the final chapter.

CONCLUSION

The process of developing a Bulgarian National Strategy for Countering Hybrid Threats would simultaneously serve a number of valuable purposes. First, this process would help spot existing national vulnerabilities to hybrid threats and identify ways and means to overcome them, better preparing Bulgarian institutions to tackle them.

Bulgaria, which has been under the Kremlin's subversive hybrid influence for many years, provides a good analytical subject for conducting an in-depth case study. The lessons learned could be quite useful not only nationally, but also for NATO, the EU and their member countries. Developing the strategy would support such an analysis. This would also provide a good opportunity to exchange relevant, up-to-date experiences with NATO, the EU and key allies, as well as to develop practical cooperation in this field.

Finally, initiating the process of writing and officially endorsing this strategy would provoke negative reactions from some politicians. This political opposition would make transparent the internal Bulgarian actors who are against Bulgaria being a robust, resilient, effective and more integrated NATO ally and EU member state. Furthermore, this state of play, together with the quality of the document that would finally be approved, would serve as a perfect chance to shed light on the actual scale and depth of the Kremlin's penetration of Bulgaria's political system. □

The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the minister of defense of Bulgaria or the Bulgarian government.

PER CONCORDIAM ILLUSTRATION

A LATVIAN CASE STUDY

CROSS-DOMAIN COERCION AND RUSSIA'S EFFORTS TO WEAKEN NATO'S EASTERN FLANK

By **Cmdr. Roslaw Jezewski**, Polish Navy and national military representative at the Supreme Headquarters Allied Powers Europe

Russian President Vladimir Putin has said he wishes the Soviet Union had not collapsed. For Putin and many Russians, this was a geopolitical disaster that removed Eastern Europe from Russian hegemony. The fact that the Baltic countries and the states in the former Soviet zone of influence in east-central Europe now belong to NATO annoys the Russian leadership. The Kremlin has been bombarding them with fake news, accusing them of fascism and hoping to find a weak point in the structure of the Alliance. NATO's eastern flank is not homogenous, especially when it comes to the Baltic states.

But which of the three countries is most vulnerable? A quantitative analysis of a few indexes helps to answer this question. The European Quality of Government Index for 2017, which focuses on the public's perception of corruption and the quality of government services, ranks Estonia 90th among the 202 regions in Europe surveyed, Lithuania 114th, and Latvia 142nd. In another indicator, the Human Development Index, Estonia again is positioned best among the Baltic states (30th), followed by Lithuania (35th) and Latvia (41st). The same sequence was observed in two other indexes: the Social Justice in the EU Index for 2016 and the Social Cohesion Index for 2017. Several qualitative indicators help to explain Latvia's rankings: 26% of the Latvian population is ethnic Russian, many residents are noncitizens, and the society is troubled and still recovering from the 2008 financial crisis. These factors make Latvia especially vulnerable to the security challenges posed by hybrid warfare techniques known as "new generation" warfare or cross-domain coercion, which aims to influence an adversary's behavior through nonmilitary means.

Russia, which resents Latvia's membership in NATO, attempts by all means below the threshold of active military hostilities to undermine the country's stability and affect the cohesion of its population, hoping also to weaken NATO unity in the process. The National Security Concept, approved by Latvia's government in 2015, recognizes that in this pursuit Russia will use coercion in all accessible domains, especially social, economic and military ones.

Examples of Russian coercion in Latvia are the derogatory propaganda from Russia-sponsored mass media, Russia's live-fire drill within the Latvian Exclusive Economic Zone in April 2018, and the activity of Russia-based organized crime. These are difficult to counter because Russia seeks to undermine Latvian societal cohesion and stability without provoking a conflict that would create an Article 5 scenario. The employment of new-generation warfare techniques against Latvia will probably stop short of provoking conventional war. Russia prefers to employ "raiding tactics" against NATO that are cheap and efficient forms of warfare and that cross many domains (cyber, informational, financial), include infiltration and surprise attacks, leverage agility and help achieve the desired political results. This approach can successfully target every vulnerability in Latvian society, undermine the government's credibility and weaken societal cohesion.

ТЫ ПОДПИСАЛСЯ
С 1 по 30 ноября по всей Латвии пройдет второй этап сбора подписей за признание русского языка вторым государственным.
ЗА РУССКИЙ ЯЗЫК?
Vladimirs Lindermans:
"Nepiedalies krusta karā pret krievu valo
BEZ KRIEV
P

A leader of the Mother Tongue movement holds leaflets supporting a referendum in 2012 to make Russian the official second language of Latvia. Nearly three-quarters of the country's voters rejected the measure.

THE ASSOCIATED PRESS

A significant vulnerability is the large share of ethnic Russians in the population. Many of them are noncitizens who are deprived of voting rights and cannot own property. This makes them vulnerable to Russian psychological operations (with Russian propaganda taking the lead) designed to convince them that Latvia does not protect their rights. A second vulnerability is Russia-based organized crime. It is suspected that organized crime organizations work in close cooperation with the Kremlin to launder money during covert operations against Latvia's society and government. The scope and size of this threat is not publicly disclosed, but it has a profound effect on Latvian security. Third, the country faces grave social problems, such as income inequality, an aging population and emigration.

This qualitative study explores the questions: Is the Russian minority in Latvia a threat to the country's cohesion? What is the impact of Russia-based organized crime on Latvia's stability? Are there countermeasures that can be employed? To find the answers it is necessary to start with a survey, without which it would be difficult to determine the cohesiveness of Latvia's population, the societal gaps and vulnerabilities. The survey assesses the susceptibility of the Latvian population to exploitation by Russian propaganda, the attitude of the Russian minority, and the threat perceptions of both Latvians and ethnic Russians.

LATVIAN VULNERABILITIES

Latvia's population is estimated to be 1.95 million, with a labor force of slightly more than 1 million. Latvians represent 62% of the population, and Russians represent 25.4%, the country's largest ethnic minority group. Many of the Russians live in the Latgale region in eastern Latvia and contribute to the presence of a Russian diaspora that dates from the Soviet-era occupation. Latvia identifies two major groups in the country: Latvian speakers and non-Latvian speakers. Among the Russian-speaking minority are ethnic Russians, Belarussians and others.

Inside the Russian minority there are about 242,000 noncitizens with relatively low status because of their poor command of the Latvian language and an inability to obtain good jobs. Latgale has a troubled economy, and available jobs are largely in the transportation or construction sectors. At the same time, Latvia is experiencing a serious demographic decline. Forecasts for 2060 suggest a population of only 1.2 million. An aging

An election placard supports Harmony, the pro-Kremlin Social Democratic Party, in front of Russia's embassy in Riga, Latvia, ahead of the 2019 European Parliament elections.

AFP/GETTY IMAGES

population and emigration, particularly among those under 30 years of age, are driving the decline. It is estimated that this intensive emigration will continue until at least 2030. There could be a negative impact on national security if adverse elements begin operating in depopulated areas.

The National Defence Academy of Latvia report, "The Possibility of Societal Destabilization in Latvia: Potential National Security Threats," describes a divided society with people neither socially nor politically active and a serious distrust of the government. The 2016 report claims that participation in public issues is low. A summary of Latvian cohesion is supplied by the EU Social Justice Index 2017, which places Latvia 19th among the 28 European Union members (and last among the Baltic states). The education system, however, was rated well, though with caveats for an urban-rural quality gap and for the limited provisions for students with special needs.

The economy, despite positive trends, also has significant vulnerabilities. It is a small and open economy that is dependent on broader global trends. Business and development are focused on Riga, while the rest of the country remains underdeveloped. This is the reason why 30% of native Latvians declare their readiness to leave the country. There is significant disparity in the unemployment rate, with the lowest rate in Riga and the highest in Latgale. The percentage of elderly facing social exclusion is rising. These factors affect the whole Latvian population, and consequently the attitude of the Russian minority.

ETHNIC RUSSIAN ATTITUDES

Studies on the matter give the impression that the Russian minority is not a significant security threat; about 80% of Russian speakers declare loyalty to the nation, according to Aleksandra Kuczyńska-Zonik's

2017 report in the *Baltic Journal of Law & Politics*. Additionally, the Russian diaspora is moderately integrated within Latvian society, although, according to James K. Wither in a 2018 Small Wars Journal article, there is antipathy toward active participation in the national defense system. The government's anticipated language reform policy is also problematic and may create feelings of discrimination among ethnic Russians. However, half of noncitizens do not support Russian narratives, according to a National Defence Academy report, and the older generation expresses the greatest level of loyalty to Latvia because they enjoy life in Latvia compared to life in Russia. Nevertheless, a majority claims that they do not plan to obtain Latvian citizenship because of difficulties communicating in the Latvian language, easy travel to Russia (no visas are necessary) and, for some, plans to obtain Russian citizenship.

Interviews with ethnic Latvian representatives provide further insights. One expressed rather negative feelings toward noncitizens, claiming that their existence is a real problem for the country. According to the interviewee, these people love Russia but live in Latvia. Some have problems with alcohol and drugs, especially the younger generation (of noncitizens), and the older generation accuses the Latvian population of Nazism. But there was also a more positive side to the conversations. One interviewee said that much depends on parents in the noncitizen diaspora because there are examples of noncitizens trying to learn the Latvian language and integrate with society. Another Latvian representative stated that those noncitizens wanting to emigrate to Russia had already gone, and that the majority of the remaining ethnic Russians had no plans to leave. Older people feel some sentiment toward Russia, but only because of their ethnicity. They definitely do not want to emigrate, especially to Russia, because they know that the living conditions in Russian do not compare favorably with those in Latvia.

There are also noncitizens who act against Latvia and create problems for national security because they can be used as tools by the Kremlin. Analysis by the NATO Centre of Excellence in Riga demonstrates that Russia remains a trusted source of information for minorities in the Baltic states. A 2017 report by the Latvia Security Police paints an alarming picture of Russian Latvians involved in Russia's information campaigns targeting Latvia's internal problems. This part of the Russian minority may be leveraged by Russia to exploit Latvia's internal vulnerabilities. The Latvian Security Police have already warned hostile pro-Russian activists about their behavior. One tool of provocation may be Russia-based organized crime, which has penetrated the Russian diaspora and is directly connected to the Kremlin.

> ***"RUSSIA'S INFLUENCE IN LATVIA'S INFORMATION ENVIRONMENT STILL CONSTITUTES ONE OF THE MOST IMPORTANT LONG-TERM THREATS TO THE SECURITY OF THE LATVIAN STATE."***
>
> **– Latvia's Constitution Protection Bureau**

Research concerning the perception of the threat to Latvia's security from the Russian minority proved surprising. In Latgale, for example, 78% of people who speak the Latgalian dialect claim they would support Latvia against Russian aggression. According to a Latvian government official, they are ready to fight for Latvia's freedom if necessary. For the Latvian population as a whole, the biggest threat is not Russia but the troubled domestic situation (low wages, declining population, inefficient health care system, corruption and crime). As for the interviewees, all consider Russia a threat. They also expressed a belief that Russia could attack without warning. Latvia's National Security Concept lists Russia as the main threat to Latvia's national security. Other parts of that document outline the ways cross-domain coercion or hybrid warfare methods aim to gradually weaken the country.

Based on these insights, it is possible to conclude that the Russian diaspora in Latvia is not homogenous. It differs in its opinion of the government and has different perspectives regarding the threat to national security. Therefore, this issue requires further study, including further interviews because the current posture of noncitizen and compatriot diasporas are not well-reflected in the literature. This can also be said of the presence of Russia-based organized crime.

HOW RUSSIA CAN WEAPONIZE LATVIAN SOCIETY

Latvia's National Security Concept addresses the ways countries try to influence the unity of Latvian society. Russia uses a hybrid warfare strategy known as "raiding," an easy and effective alternative to expensive and dangerous conventional warfare methods. In the information sphere, raiding coerces the enemy by shaping public perception. As in every aggression, the intruder targets an opponent's center of gravity. And in Latvia, that center is likely to be public perception. Derogatory messages penetrating the Latvian information space try to create a positive image of Russia in the eyes of the Russian minority and to undermine trust toward the Latvian government. There is music, there is culture — and in between there are fake news and lies; one example is the lie that Latvia was not occupied by Russia.

Russian media find it easy to raid the Latvian information sphere, which hosts media in the Latvian and Russian languages. TV, radio and troll farms targeting social media transmit Russia's soft power messages. Russia is playing on national sentiment in Russian minority populations to influence the domestic and foreign policies of neighboring countries. According to the NATO Strategic Communications Centre of Excellence, "the (alleged) violation of the human rights of Russia's compatriots abroad may be used as justification for the violation of sovereignty, as was the case during the war with Georgia and crisis in Eastern Ukraine." If Russia wants to provoke unrest in a country, the Russian minority could be a very useful tool.

Latvia's Constitution Protection Bureau emphasized the danger in 2016, warning that "Russia's influence in Latvia's information environment still constitutes one of the most important long-term threats to the security of the Latvian state." Russia's broadcasts target all vulnerabilities that exist within society and use any pretext to get their messages across. In this stream of messaging, Russia presents itself as the defender of old sentiments, criticizes NATO and Latvia's language policy, and repeats offers to grant Russian citizenship and pensions for compatriots. It is especially directed toward the part of the population that only consumes Russian-language media. In 2015, a survey by Latvia's National Defence Academy found that "46% of Russian speakers do not obtain any information from the Latvian language media. ... Approximately one-fifth of Latvian society cannot be reached through media in the state language."

Belarussian tanks participate in war games with Russia near Latvia in 2017. Among the Russian-speaking minority in Latvia are Belarussians and others that Russia attempts to influence.

THE ASSOCIATED PRESS

However, easy access to the Latvian media space does not guarantee victory for Russia in the information war. A survey by NATO's Centres of Excellence clearly shows that Russia's efforts are not as effective as they have hoped since "national media in the surveyed countries is perceived as more trustworthy ... [than] the Russian media outlets." For example, 54% of respondents to a 2017 survey disagree with the statement that Russian-speaking people in Latvia are being discriminated against. In addition, 45% fully disagree with the statement, "NATO is a threat to Russia." It means that the audience makes judgments about Russian broadcasting and compares it to other sources.

The potential weaponization of Latvian society is not limited to the information sphere, according to the Centres of Excellence. Russia has been searching for countries or regions with poor governance to gain influence through corruption. Heather Conley, in the book *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*, writes that this process is at the forefront of new generation warfare, which tends to influence a system, penetrate it and weaken it from inside. Russia then pumps its influence inside the country through established economic connections and tries to capture the state and amend national decisions. A 2018 Reuters article reported on suspected Russian money kept in the Latvian banking system and used to interfere in the internal affairs of European countries. The financial assets were reportedly delivered from Russia and used to finance hybrid activities that undermine political systems in other countries. Also in 2018, Bloomberg reported on suspicious Russian financial transactions in Latvia between 2010 and 2014, and on a significant flow of Russian deposits into Latvia beginning in 2012.

Even more alarming is a plot confirmed by Finland's security services in 2018. According to these reports, ethnic Russians (some with double nationality) were buying or constructing expensive houses in southwest Finland close to vital communication routes and security installations. According to some accounts, military surplus fast boats were purchased, and there were frequent helicopter flights between Finland and Latvia. It prompted Finland to consider measures that would reduce the ability of foreigners to buy land or property in Finland. Similar measures should be introduced in Latvia, where it is possible to gain five-year permanent residency by fulfilling one of three conditions: buying property, making investments or opening a bank account. Special attention should also be paid to the Russian indoctrination of young ethnic Russians living in Latvia, which is taking place in paramilitary camps inside Russia. These are the places that infect young brains with propaganda. Russia's investment in the younger generations may one day result in pro-Russian leaders in Latvia.

In response to Russian aggression, Latvia strives to unite the nation into a cohesive society able to repel adversarial actions. It is official national policy that it is the "duty of each citizen to defend their country and to resist an aggression in an active or passive manner." Apart from Latvian uniformed formations, the core of the deterrence system is the presence in Latvia of NATO units, which conduct exercises as a show of force to demonstrate NATO's commitment. According to Latvia's Ministry of Defence, at the national level, deterrence capabilities are based on the potential to "rapidly increase the extent of the (regular armed forces) to the level required for the deterrence or warfare." Does that mean one of the factors determining the resilience of Latvia's defense system is the aging population? If the answer is "yes," Latvia faces a problem. A report on the Defence Ministry website states: "the Baltic States face a common demographic challenge as efforts to expand the size and capacity of territorial forces may be thwarted by a shortage of young, skilled recruits, especially as seems likely, members of the large ethnic Russian minorities in Estonia and Latvia are unwilling to take part."

FUTURE IMPLICATIONS

In the short term, the composition of the Latvian government will decide Latvia's future. The elections in October 2018 brought an end to a coalition of right-wing parties. The pro-Russian Harmony party received about 20% of the vote. Of the two populist parties, KPV received 14%, and the New Conservative Party received slightly less than 14%. Support for Harmony does not mean that Latvia is turning toward Russia; the party has many Latvian members and public support is decreasing, from 28% in 2011 to slightly less than 20% in 2018. Therefore, the good news for the populist parties is that people simply grew tired of the scandals, corruption and the lack of progress.

In the long term, the demographic decline might hit Latvia the hardest. A decrease in the population could be catastrophic: Scarcely populated areas will become depopulated, and Latvia may turn into a country of old people and huge economic disparities. A lack of young people will also contribute to this gloomy picture: Who will work? Who will defend the country? These are the questions that the government, regardless of political orientation, will have to address. Is there any remedy for this trend? Most important is to restore the birthrate to at least 2.1 children per couple to sustain the population and reverse the emigration trend. The current Russian minority will probably integrate more into

Latvian society simply because there is no other option, and the noncitizen diaspora will diminish due to mortality and the naturalization of the youth. This will require a tough but open stance by the Latvian government toward Russia to fight derogatory messaging and fake broadcasting. These efforts are on the way. In Latgale, where powerful Russian signals dominate the airwaves, Latvian TV stations are erecting transmitting stations and broadcasting Latvian-made Russian programs to address the eastern part of the country.

CONCLUSIONS

The Russian minority in Latvia — especially after the October 2018 elections — constitutes a base that Russia could use to undermine the country's cohesion. However, this threat should not be overstated because the Russian minority is not homogenous; it contains pro-Latvians as well as pro-Russians. Also, the potential vulnerabilities in the Russian diaspora are not clear-cut. There are Latvian Russians with a clear understanding of the different living conditions in Latvia compared with Russia and who do not believe Russian propaganda or fake news. The Latgalians, especially, should not be perceived as a pro-Russian group; there are pro-Russian citizens and there are patriots who do not fear Russia and are ready to fight to defend Latvia. One thing must be clear, the Russian diaspora does not pose a threat for now. But if provoked from outside, perhaps by Russian coercion, the diaspora may react against Latvian society. Russia, if it decides to intervene in Latvia, will not do it to protect the diaspora, but will do it because of strategic choices, and the Russian minority will be just a tool to that end.

Russia-based organized crime may emerge as one of the most effective and covert means of coercion in Latvia. It has been deep inside Latvia since Soviet times and will be difficult to erase from society. Its existence should be analyzed together with its direct connection to the Kremlin, the Russian economic footprint and the problems affecting the Latvian banking system. It is likely that organized crime will be heavily involved in Russian attempts to incite unrest, bribe politicians and gather intelligence. Fighting this threat will require a national and international response.

Russia has been practicing extensive, hostile cross-domain coercion in Latvia for years, hoping to weaken the cohesion of NATO's eastern flank. The most spectacular cases are the Zapad 17 exercise, cyber attacks, derogatory propaganda from state-owned TV stations, and the radicalization of ethnic Russian youth in training camps. These efforts may evolve into more aggressive measures, and direct warfare cannot be ruled out. The good news is that the self-esteem of the Latvian population is growing as people compare information from a wider range of sources and learn to identify fake news. This suggests that Russian propaganda is becoming an obsolete tool, and that Russia will try to engage through other domains. This would probably involve cyber operations, which are relatively cheap, effective and borderless.

Russia has been testing NATO's eastern flank for years, a practice that can be expected to continue. Those efforts may now expand beyond the Baltic states to other "promising" targets. Divisions in society are also dangerous for Latvia's national security. Social inequality is a serious obstacle to national cohesion. Distrust of the government is unfortunately justified in the face of corruption and social inequality, especially in rural areas. Societal gaps need to be eliminated as soon as possible because they work against the cohesion and resilience of Latvia.

There is evidence that, apart from money laundering, Russian organized crime is involved in espionage and intelligence gathering for the Russian government and is cooperating with criminal groups on the border. This means that despite the surprisingly positive resilience of the Russian diaspora in Latvia, Russia has an opportunity to infiltrate the country and exert cross-domain coercion from the inside. Other concerns that demand greater attention include the overall status of the Latvian population, cooperation with other Baltic states regarding Russian minorities, and the structure and characteristics of the Russian minority in Latvia.

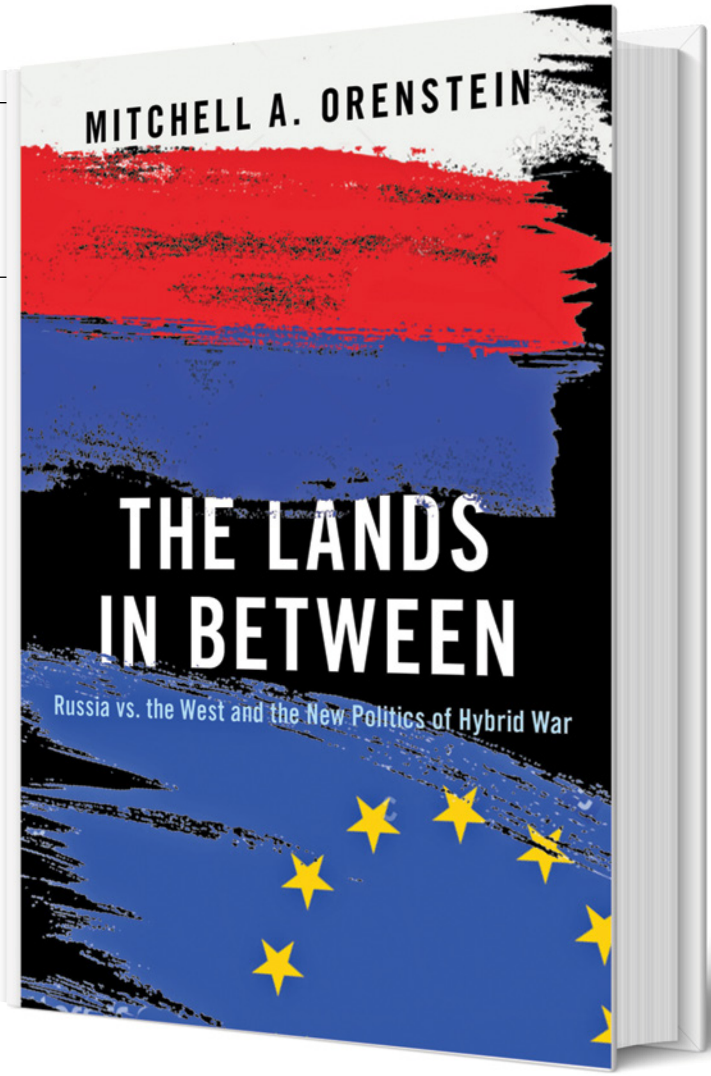
Latvia's case illustrates clearly that the cohesion and unity of a nation is of the utmost importance when opposing cross-domain coercion. □

Latvians mark their ballots at a polling station in Riga in 2018. The elections brought an end to a coalition of right-wing parties, though the pro-Russian Harmony party received about 20% of the vote.

THE ASSOCIATED PRESS

Hybrid War IN THE LANDS IN BETWEEN

BOOK AUTHOR: Mitchell A. Orenstein
PUBLISHED BY: Oxford University Press, 2019
REVIEWED BY: *per Concordiam* Staff



Mitchell Orenstein assures us that his book, *The Lands in Between: Russia vs. the West and the New Politics of Hybrid War*, is not just about the small, poor countries nestled in between Russia and the European Union. There is much more at stake because these "lands in between" are on the front lines of what he describes as a geopolitical conflict fought with conventional and unconventional tools, such as cyber warfare, hacking, money laundering and the threat of nuclear war.

Orenstein is well-placed to explain this assault in his short, compelling and easy-to-comprehend treatise. He is a leading scholar of the political economy and international affairs of Central and Eastern Europe, and he is a professor and chair of Russian and East European studies at the University of Pennsylvania and senior fellow at the Foreign Policy Research Institute. His premise is that former Soviet republics and satellites in Central and Eastern Europe and Western/Central Asia face "civilizational pressures" from Western democracies and the Russian behemoth.

Although the Soviet Union is dead, Orenstein explains that for a Russian government determined to win back the former Soviet empire, the very existence of NATO and its security guarantees to member states constitute a threat. An enlarged NATO alliance threatens Russia's attempts to [re]establish itself as a great power with a legitimate sphere of influence — whether or not the lands in between acknowledge or accept that influence.

Or, to put it in more plain terms, "where the West sees democracy promotion as a strategy for promoting peace in Europe, Putin sees it as an act of war against Russia and his regime in particular. … Russia regards the battle for influence in the lands in between as a zero-sum game, to be won or lost." This conflict of visions has led to a conflict in reality as Russia conducts hybrid war and operates in a gray area, daring Western nations to stop it.

Russia calls its actions a campaign of "strategic deterrence," "reflexive control" or "new generation warfare." But Orenstein notes, "Russia's objectives are to polarize, disable, and ultimately destroy the European Union and NATO without incurring too great a reaction from the West." In this largely covert hybrid war, Russia has used a wide range of tools: spying, cyber warfare, funding for anti-EU political parties, media campaigns and disinformation, support for nongovernmental organizations and pro-Russia paramilitary organizations, and military interventions against countries signing association agreements with the EU, such as Ukraine.

The author calls out the West as a whole for reacting so slowly to this nonkinetic aggression: "Western countries faced powerful economic incentives to improve and deepen relations with Putin's Russia. Few in the West wanted to acknowledge the existence of a hybrid war that would disrupt business and force countries to increase military expenditures." Given this stubborn fact, is it any wonder that some regional leaders seek to cut deals with Russia to maintain freedom to maneuver as sovereign nations?

Despite the seeming value of such flexibility, following this path is both shortsighted and dangerous. Of course, having endured the Russian boot for nearly 50 years, one cannot imagine why Hungary, Moldova or, until 2014, Ukraine, should not wholeheartedly and unreservedly embrace the liberal democratic and economic institutions of the West. This is not so easy, however, when one resides on the geographic doorstep of an irate Russia angered at its reduced influence within what it considers to still be its domain.

Orenstein looks with understanding, if not agreement, at the Hungarian and Moldovan leaders and the flexibility they have employed in balancing competing interests. In the lands in between, the geopolitical environment seems to demand it. "In countries where mass politics is extremely polarized — fought out between media and political forces that are fiercely pro-EU or pro-Russia — the greatest power and wealth flows not to ideological partisans, whose gains are often partial and transient, but to the power brokers who position themselves to profit from the enormous passions and insecurities of both sides." It is the task of the EU and NATO to persuade these leaders that their countries' best interests are with the West and not with an unreliable and self-interested Russia.

Orenstein also looks at Belarussian President Alexander Lukashenko and observes: "Lukashenko embodies the political paradoxes that haunt the lands in between. Caught between two powerful neighbors pulling in different directions, politics in these countries has become sharply, intensely polarized." Lukashenko has made flexible choices that perplex, frustrate and, in some cases, infuriate not just leaders in Russia, but conversely, leaders in the West who had imagined he was taking his nation on a path toward Western liberalization.

Orenstein sums it up succinctly: The main issue in national politics within the region is whether to join Soviet Union 2.0 or to achieve national independence within an EU framework.

> "The lands in between can choose closer relations with the EU, a huge and successful market characterized by rule of law, freedom of speech, anticorruption campaigns, visa-free travel, educational opportunities, and a path toward Western prosperity, but at the risk of high inequality and increasing internationalism. On the other, they can choose to be part of the new Russian empire, where they share a common culture and history, speak the same language [or, at least understand Russian], and benefit from long-standing trade and employment ties, but also suffer from a top-down system of corruption, a weaker economy, and a state propaganda machine that feeds a debilitating belief in conspiracy theories."

Regional leaders, known for their flexibility, have not conceded the unsurmountable contradictions here. They ought to consult with the people of Ukraine. "Prior to 2014, the median voter in Ukraine wanted closer relations with the EU and Russia simultaneously and did not worry if these goals were mutually exclusive. Ukrainians simply wanted good relations with both sides," Orenstein writes. However, "when Russia grabbed Crimea and Eastern Ukraine in order to prevent Ukraine from joining the EU, it pushed a majority of Ukrainians into the pro-EU camp and made them see Russia as an enemy. Geopolitical orientation and nationalism became firmly aligned." Ukraine today enjoys a national identity and nationalist patriotism previously inert. This is not necessarily the West's doing; it has been nurtured through hard experience with Russia's heavy-handed and dismissive treatment of Ukraine as a sovereign country.

Orenstein believes these nations inevitably must choose a side. The lands in between need firm assistance and reasons why they should reject Soviet Union 2.0. The West can provide this by rearticulating the values of political liberalism, equality before the law, protection of minorities, and the benefits of democracy, all values that are under attack — in both the lands in between and in the West. They are the values the Marshall Center promotes so successfully. "It may be a long struggle," Orenstein writes, "but the West needs to put up a vigorous defense in the face of an onslaught from domestic populists and foreign spoilers." □

Resident Courses

Democratia per fidem et concordiam
Democracy through trust and friendship

Registrar
George C. Marshall European Center
for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
Telephone: +49-8821-750-2327/2229/2568
Fax: +49-8821-750-2650

www.marshallcenter.org
registrar@marshallcenter.org

Admission
The George C. Marshall European Center for Security Studies cannot accept direct nominations. Nominations for all programs must reach the center through the appropriate ministry and the U.S. or German embassy in the nominee's country. However, the registrar can help applicants start the process. For help, email requests to: registrar@marshallcenter.org

PROGRAM ON APPLIED SECURITY STUDIES (PASS)

The Marshall Center's flagship resident program provides graduate-level education in security policy, defense affairs, international relations and related topics such as international law and counterterrorism. A theme addressed throughout the program is the need for international, interagency and interdisciplinary cooperation.

PASS 20-19

Sept. 9 -
Nov. 24, 2020

September

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

October

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

November

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

PROGRAM ON COUNTERING TRANSNATIONAL ORGANIZED CRIME (CTOC)

This resident program focuses on the national security threats posed by illicit trafficking and other criminal activities. The course is designed for government and state officials and practitioners who are engaged in policy development, law enforcement, intelligence and interdiction activities.

CTOC 20-07

Mar. 17 -
Apr. 8, 2020

March

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

April

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

CTOC 20-16

July 8 - 30, 2020

July

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

PROGRAM ON TERRORISM AND SECURITY STUDIES (PTSS)

This program is designed for government officials and military officers employed in midlevel and upper-level management of counterterrorism organizations and will provide instruction on both the nature and magnitude of today's terrorism threat. The program improves participants' ability to counter terrorism's regional implications by providing a common framework of knowledge and understanding that will enable national security officials to cooperate at an international level.

PTSS 20-05

Feb. 11 -
Mar. 12, 2020

February

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

March

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

PTSS 20-18

Aug. 6 -
Sept. 3, 2020

August

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

September

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

PROGRAM ON CYBER SECURITY STUDIES (PCSS)

The PCSS focuses on ways to address challenges in the cyber environment while adhering to fundamental values of democratic society. This nontechnical program helps participants appreciate the nature of today's threats.

PCSS 20-02

Dec. 3 - 19, 2019

December

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

SEMINAR ON REGIONAL SECURITY (SRS)

The seminar aims at systematically analyzing the character of the selected crises, the impact of regional actors, as well as the effects of international assistance measures.

SRS 20-03

Jan. 14 -
Feb. 7, 2020

January

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

February

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

SENIOR EXECUTIVE SEMINAR (SES)

This intensive seminar focuses on new topics of key global interest that will generate new perspectives, ideas and cooperative discussions and possible solutions. Participants include general officers, senior diplomats, ambassadors, ministers, deputy ministers and parliamentarians. The SES includes formal presentations by senior officials and recognized experts followed by in-depth discussions in seminar groups.

SES 20-15

June 22 - 26, 2020

June

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Alumni Programs

Christopher Burelli
Director, Alumni Programs
Tel: +49-(0)8821-750-2706
christopher.burelli@marshallcenter.org
Languages: English, Slovak, Italian, German

Alumni Relations Specialists:

Drew Beck
Western Balkans,
Francophone Africa

Languages: English, French

Tel: +49-(0)8821-750-2291
ryan.beck@marshallcenter.org

Christian Eder
Western Europe

Languages: German, English

Tel: +49-(0)8821-750-2814
christian.eder@marshallcenter.org

Marc Johnson
Eastern Europe, Caucasus,
Central Asia;
Cyber Alumni Specialist

Languages: English, Russian, French

Tel: +49-(0)8821-750-2014
marc.johnson@marshallcenter.org

Frank Lewis
Visegrád Four, Baltics, Middle East, South and East Asia;
Counterterrorism Alumni Specialist

Languages: English, German

Tel: +49-(0)8821-750-2112
frank.lewis@marshallcenter.org

Donna Janca
Americas, Anglophone Africa,
Eastern Balkans, Mongolia;
CTOC Alumni Specialist

Languages: English, German

Tel: +49-(0)8821-750-2689
nadonya.janca@marshallcenter.org

mcalumni@marshallcenter.org

Contribute

Submit articles and feedback to the Marshall Center at **editor@perconcordiam.org**

Subscribe

For more details, or a **FREE** subscription to *per Concordiam* magazine, please contact us at **editor@perconcordiam.org**

Find us

Find *per Concordiam* online at:
Marshall Center: **www.marshallcenter.org**
GlobalNET Portal: **https://members.marshallcenter.org**
Digital version: **https://perconcordiam.com**

The George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany

MARSHALL CENTER