PRISM

VOL. 10, NO. 4 | 2024

Managing Chaos in a Disordered World

PRISM
VOL. 10, NO. 4, 2024

ISSN 2157- 0663

ABOUT

PRISM is National Defense University's (NDU) flagship journal of national and international security affairs. PRISM's mission is "To provide unique insight for current and future national security leaders on emerging security challenges beyond the strictly military domain of the joint force, including transnational, multi-domain threats, gray zone conflict, the technological innovation challenge, and geoeconomic competition among the great powers."

COMMUNICATIONS

PRISM welcomes unsolicited manuscripts from policymakers, practitioners, and scholars, particularly those that present emerging thought, enduring insight, or best practices related to the emerging national security environment. Publication threshold for articles and critiques varies but is largely determined by topical relevance, continuing education for national and international security professionals, scholarly standards of argumentation, quality of writing, and readability. To help achieve threshold, authors are strongly encouraged to recommend clear solutions or to arm the reader with actionable knowledge. Our review process can last several months. The PRISM editorial staff will contact authors during that timeframe accepting or regretfully rejecting their submission. If the staff is unable to publish a submission within four months of acceptance, PRISM will revert publication rights to the author so that they may explore other publication options. Constructive comments and contributions are important to PRISM. We also welcome Letters to the Editor that are exclusive to PRISM—we do not publish open letters. The PRISM editorial staff will contact authors within two months of submission if they accept the letter for publication. Please direct all comments and submit manuscripts in electronic form to prism@ndu.edu. Hard copies may be sent to the address listed below and should include a note that provides a preferred email address and phone number for feedback: PRISM does not return original hard copy submissions. National Defense University, PRISM Editor, 260 Fifth Avenue, S.W., Building 62, Suite 212, Fort Lesley J. McNair, Washington DC 20319

DISCLAIMER

"Managing Chaos in a Disordered World"

FEATURES

BOOK REVIEWS

Managing Chaos

By Michael Miklaucic

"Things fall apart; the centre cannot hold;
Mere anarchy is loosed upon the world,
The blood-dimmed tide is loosed, and everywhere
The ceremony of innocence is drowned;
The best lack all conviction, while the worst
Are full of passionate intensity."

(W.B. Yeats, The Second Coming, 1921)

If it seems like the world is descending into chaos the feeling is justified. Thirty-five thousand dead in Gaza. Nearing 300,000 killed in Ukraine. War in the Red Sea. Jihadist insurrectionists in the Sahel. Nuclear saber-rattling by the Kremlin. North Korea and Iran threatening their neighbors and everyone else. Escalating Chinese intimidation of Taiwan. Complete breakdown of Transatlantic relations with Russia. Partial breakdown of U.S. relations with China. The world seems to be coming unglued. The rules-based global order that set the norms and more-or-less governed behavior between states for the past nearly 80 years is frayed—possibly beyond repair. Citizens everywhere are exhausted, barraged relentlessly by the 24/7 news cycle with constant reportage so grim as to be anaesthetizing.

Global order is a universal public good, however it is neither self-executing nor auto-emergent. It emerges from the struggle—sometimes violent—of competing principles of governance, often but not exclusively manifested by states. Those principles are expressed by a specific conceptual vocabulary and constitute a paradigm.

Michael Miklaucic is a Senior Fellow at National Defense University and the Editor-in-Chief of PRISM.

It is permanently in flux. Today we are experiencing a paradigm shift and global order cannot be taken for granted. We are veering toward chaos.

The defining principles of the liberal, rules-based global order originated in Europe, but while never attaining universality rapidly spread to the Western Hemisphere, to Asia and South Asia, and elsewhere. They were elegantly articulated and reached their apogee in the immediate post-World War II era with the Charter of the United Nations, the Universal Declaration of Human Rights, and a substantial body of international law. Today autocratic regimes are set on replacing the liberal, rules-based global order with an alternative more conducive to authoritarian governance based on pervasive surveillance, social and political control, and rigid regime dominance.

Geopolitical concepts such as deterrence, containment, international law, development, sovereignty, alliances, and cooperative multilateralism, among others made the post- World War II world somewhat predictable and manageable, if not always copacetic. They helped prevent great power conflict, organized international relations, promoted prosperity, and mobilized resources for the benefit of both the populations recovering from the devastation of World War II as well as those emerging from colonial legacies. That order, however, has reached entropy; each of the fundamental concepts underlying the post-World War II system has dramatically weakened and lost its ordering power.

The dissipation of the post-World War II paradigm leaves a profound vacuum in our conceptual framework and understanding of the global security environment. A new constellation of ordering principles must be discovered to replace the anachronistic principles of past order. Absent a new set of guiding principles and the collective will to implement them the current, fading order will dissolve into chaos, or worse, into a future order based merely on brute force and violence. Russia has shown us that future with its unprovoked invasion of and explicit intention of eradicating Ukraine.

In this era of entropy and disorder what are the options for preserving the principles of the liberal, rules-based global order? One ever-present option is to stick with the status quo; however, this option cedes the initiative to adversaries that are relentless and committed to overturning that order and achieving regional if not global hegemony. The status quo entails a shrinking core of liberal states consumed with destructive internal dynamics, fratricidal disputes amongst themselves about market shares, incremental erosion of global influence, and paralysis in the face of a concerted strategic assault by authoritarian adversaries. A more aggressive option is to attempt to counterattack and reclaim recently lost ground in the global competition for influence. However, absent a reversal or at least mitigation of recent geopolitical and geoeconomics trends favoring the authoritarian coalition this option will be a struggle likely to fall short in the near-term. A third option—less ambitious, but within reach—is to accept the reality of decoupling from the authoritarian coalition and consolidate the "Core" of liberal states committed to a rules-based global order by strengthening their bonds of alliance and partnership, increased burden-sharing, and, importantly, reinforcing their respective institutions of liberal, rules-based governance.

What is "the Core?" It is neither the West nor the East nor the North nor the South. "Consolidating the core" is neither containment nor imperial expansionism. The core consists of those states committed to the liberal, rules-based global order embracing human liberty, social justice, and the norms of international behavior articulated in the UN Charter and the Universal Declaration of Human Rights. The core is not frozen nor exclusive. Between the core and the authoritarian coalition exists a large number of hedging states unwilling or unready to commit to one or the other visions of

global order or the coalitions advancing them. These are contested states that might continue to hedge or lean toward or join one group or the other. They are not insignificant, and the competition over their allegiance will be intense. To win the alignment of the hedging states the Core must have "a better deal" to offer in terms of the sharing of power, wealth, and prosperity. To those contested states the Core must offer incentives and real potential to reach their aspirations. The disastrous Washington Consensus must be abandoned.

Policies based on anachronistic principles can have little hope of effectively shaping desired outcomes. For example, policies based on the principle of sovereignty have over-estimated the governance capability of fragile and failing states. The prevailing understanding of development has not been successful in accomplishing the aspirations of the post-World War II architects, and the institutions built to foster development have under-performed at great cost. Deterrence, while it may have been successful at the strategic level, has proven ineffective in preventing sub-strategic violence and conflict. To achieve relevance both policy and practice must be built upon principles that accurately reflect the evolving global environment.

Identifying and articulating the principles that will govern the trajectory of the future global order implies the creation of a new vocabulary to define the evolving global paradigm. The old vocabulary has become a limiting function undermining both policy and practice. The new vocabulary will emerge through an intellectual fusion with contributions from thought leaders and practitioners from the international security, statecraft, technology, and development communities. Insight from the private sector (finance, manufacturing, commerce, etc.) will also be critical to creating a policy-relevant vocabulary.

Today, the core states are poised in an existential struggle against a powerful coalition of authoritarian, elite-controlled, surveillance states intent on shaping the future to be conducive to rigid, autocratic domination. This struggle will determine who will set the rules of behavior and governance for the 21st century. PRISM

Examining the Value of a "Soft Power" Net Assessment

Comparing Chinese and U.S. Power Projection in Africa

By Michael J. McNerney, Oluwatimilehin Sotubo, and Daniel Egel

The Chinese Communist Party (CCP) has entered an era in which it is no longer willing to be second fiddle to the United States. After many years of quietly growing China's economy, following Deng Xiaoping's guidance to "hide your strength and bide your time,"[1] the CCP and President Xi Jinping are overseeing a plan for a more assertive China that uses its political and economic power to influence international relations.

Underpinning China's more assertive approach is a new concept that Xi has called *zonghe guoli* or "comprehensive national power." This is a concept that seeks to describe "China's combined military, economic, and technological power and foreign policy influence,"[2] particularly as it compares to that of the United States and its allies.[3] Xi's conclusion, it seems, is that China's *zonghe guoli* has grown such that China no longer needs to stand in America's shadow.

The United States is well-aware of the challenge posed by China. The 2022 National Security Strategy emphasized that China "is the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it."[4] Given such high stakes, it should be no surprise that the U.S. government's strategy argues for including "all elements of national power" in "out-competing China."[5]

Competing effectively against China requires a nuanced understanding – a net assessment – of the relative strengths of China and the United States.[6] There are now robust U.S.-China net assessments focused on military capabilities,[7] key emergent technologies,[8] defense industrial base,[9] and overall national competitiveness.[10]

But how effective are the non-military components of U.S. efforts to project power abroad in comparison to those of China? Comparable analyses of America's "soft power" vis-à-vis China are far more limited.[11]

Mr. Michael J. McNerney is a former Senior Researcher at RAND. **Mr. Oluwatimilehin Sotubo** is a Researcher at RAND. **Dr. Daniel Egle** is an Senior Economist at RAND.

This article explores the potential value of a net assessment for understanding the relative strengths and weaknesses of U.S. and Chinese soft power. After describing the rise of China's soft power, this article examines the concept of a "soft power net assessment" through a focused look at the continent of Africa, an area of historical and future strategic consequence. It is also a continent where the CCP has made significant investments to strengthen its influence and leverage that influence to undermine the international rules-based order.[12] While the article is primarily meant to explore the concept of a soft power net assessment, we include some analysis in the form of a rudimentary net assessment to illustrate the idea.

Our illustrative net assessment suggests that China may be gaining on America's soft power leadership in Africa and in some cases could now have an edge. U.S. influence in Africa has been stagnant in many ways over recent years, whereas China's influence is clearly growing. But the CCP, which prides itself on taking the long view, also faces serious headwinds over the next few decades, as it tries to steer an aging and disgruntled post-pandemic China through an international environment that is increasingly suspicious of it.

The United States needs its own comprehensive plan to implement its National Security Strategy successfully. Such a plan might benefit from comparative "whole of society" net assessments that identify and act upon relative U.S. and Chinese strengths and vulnerabilities. U.S. citizens would benefit from more public analysis with stronger involvement by the intelligence community and federal departments like State, Treasury, Commerce, Energy, and Education.

THE RISE OF CHINA'S SOFT POWER

China's economic growth over the past 45 years has been meteoric. In the decades following Chairman Deng Xiaoping's policy of "reform and opening" in 1978,[13] China transformed from a largely agrarian society to a global industrial power.[14] Its unprecedented, sustained growth since its "opening up" in the late 1970s saw China's economy grow from 2 percent of global GDP in 1978 to 18 percent of global GDP in 2021.[15] Figure 1 below shows U.S. and Chinese GDP between 1978 and 2021 both in dollar terms and as a share of global GDP.

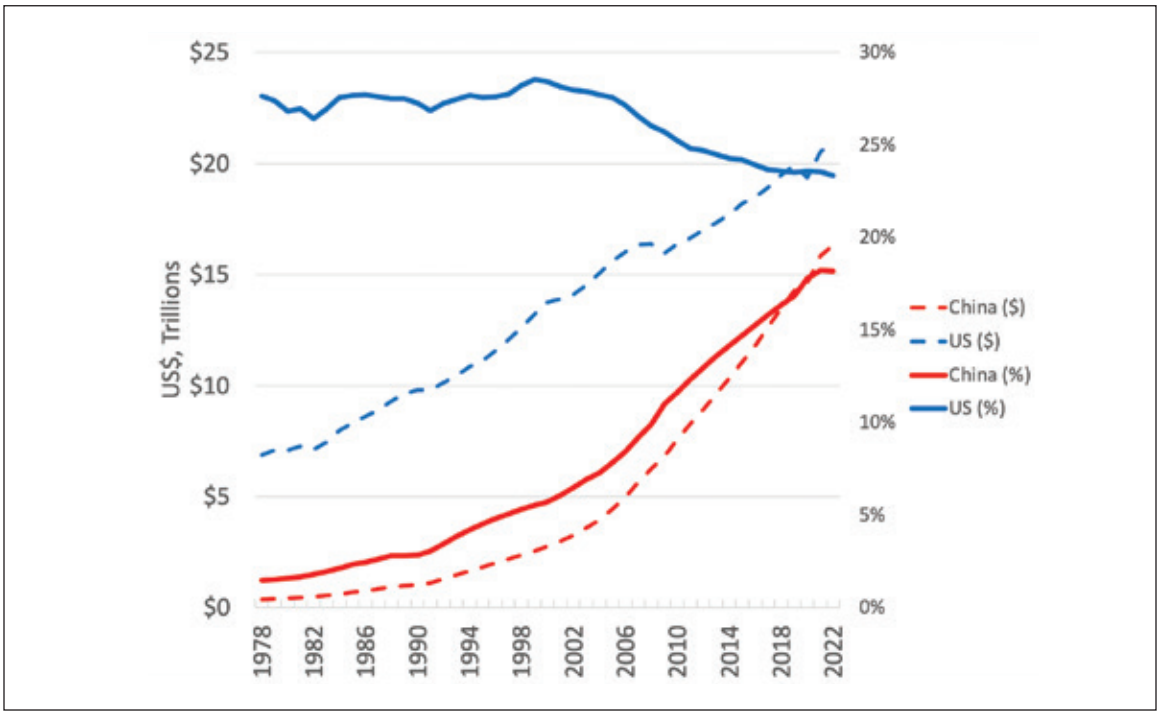
As China's economic power has grown, it has sought to play a more assertive political role on the global stage. This includes the CCP's continuing efforts to incentivize and pressure countries to cut their diplomatic ties with Taiwan, with China undermining the "checkbook diplomacy" that Taiwan has depended on for decades.[16] The CCP has also used its political power to facilitate the acquisition of dual-use ports[17] and to strengthen access to the natural resources like oil and rare earth elements needed to sustain Chinese high-tech manufacturing and economic growth.

This section describes the key components of Chinese soft power that are enabling it to achieve its strategic ambitions. The economic components are aimed at creating a virtuous cycle of political power strengthening economic power which further strengthens political power. The informational components are aimed at influencing opinions of elites and citizens internationally, especially in terms of how China is perceived. The geo-strategic components are aimed at advancing CCP political and security goals in places like the South China Sea and in countries with key natural resources. And the educational component is focused on building long-term influence by training future world leaders and expanding the prestige of its higher-education institutions.

Economic

The CCP exerts tight control over the Chinese economy. In the 1980s, at the beginning of the economic opening under Deng Xiaoping, the

Figure 1. U.S. and Chinese GDP from 1978-2021



Source: World Development Indicators, "GDP (constant 2015 US$) – China, United States, World" World Bank, 2023.

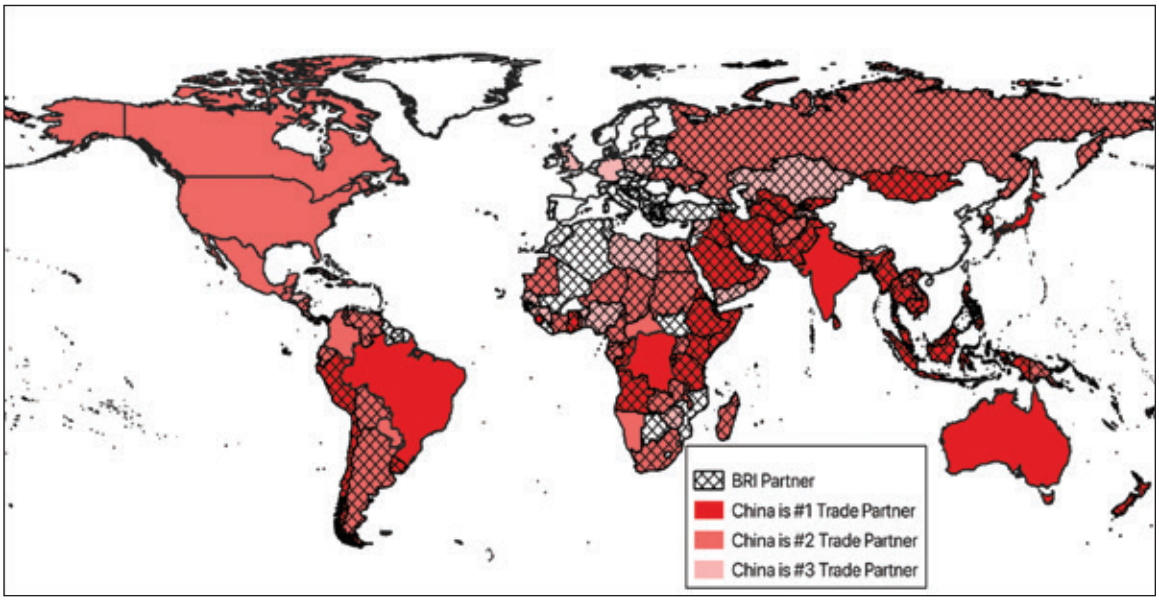
Chinese described the Chinese market economy as a bird in a cage: Market forces require some limited freedom to be effective, but the bird is never intended to fly free.[18] The CCP under President Xi has been making the cage smaller in recent years, strengthening its control over the private sector in order to better harness its political power. In a February 2023 speech, Xi said the CCP would "step up party-building work" in Chinese companies, as part of a larger set of structural reforms to China's financial and commercial sectors, with particular emphasis on technology.[19]

This control over the economy gives the CCP a potent tool to project soft power abroad. And the CCP is deliberate in how it leverages its massive domestic market and its ability to deploy financial capital to build influence in capitals and boardrooms across the globe.

China's economy is now second to only the United States, having passed the European Union in 2021, and China surpassed the United States in 2017 to become the second largest importer in the world (and is now second to only the European Union).[20] This makes China a critical economic partner for countries across the globe. This is true for developing countries that are seeking markets for both raw and manufactured goods[21] and for Western or multinational firms that want to sustain access to China's large consumer market.[22]

As the map above shows, China is now among the top three trading partners for 121 countries, making it second only to the European Union (which is in the top three for 151 countries) in terms of diversity of engagement. It is the primary partner for 47 countries – a 15-fold increase from 2001 when it entered the World Trade Organization (WTO)[23]

Figure 2. China's Global Economic Engagement: Trade and BRI



Notes: Authors' estimates based on aggregate trade data from 2018-2022 from IMF Department of Trade Statistics and BRI data from the Council on Foreign Relations.[24]

– and the second most important trading partner for an additional 47 countries.

And China has shown a willingness to use this position to influence its trading partners,[25] which U.S. Trade Representative Katherine Tai has described as the "weaponization" of trade by China.[26] In recent years, China has overtly leveraged its trade dominance in efforts to achieve political objectives in Australia,[27] Japan,[28] and Mongolia,[29] among others.

The Chinese government has similarly leveraged its large consumer base to make steep demands of foreign companies that desire access to the Chinese market. Foreign companies are pressured to maintain a local business presence in China and to make political statements favorable to the Chinese government.[30] Requisite partnerships with Chinese firms to access the domestic market also often require the Western company to transfer technology to its Chinese partner (and thus the Chinese government) as the price for accessing China's consumer base, while in other cases intellectual property was simply stolen.[31]

Foreign direct investment and financing are the second major set of tools China uses to promote its economic power. Many countries in the developing world lack necessary infrastructure and China has both the capacity and the willingness to provide it. This is one of the appeals of the Belt and Road Initiative (BRI), which has grown to include nearly 150 countries, as illustrated in Figure 2. Countries outside the BRI, especially African countries, have also approached China to secure infrastructure and financing.[32]

The Chinese government has also deployed heavy subsidies and easy financing to sell and install advanced capabilities around the world, like Huawei's 5G telecommunications systems or Chinese facial recognition platforms.[33] While this support from China is welcomed by many nations

Figure 3. China's Cinematic "Wolf Warriors" Liberating Africans

Image from Wolf Warrior 2. Source: https://qz.com/africa/1052857/chinas-wolf-warrior-2-in-war-ravaged-africa-gives-the-white-savior-complex-a-whole-new-meaning

that would otherwise lack the ability to deploy advanced systems, it creates both commercial challenges for competing Western companies (such as Cisco, Nokia, and Ericsson) and national security challenges because of the systems' potential uses for cyber espionage.[34]

China also tries to promote its economic power through international institutions. China has tried to achieve this through both Western-created institutions such as the World Bank and the United Nations, as well as the relatively newer institutions it has created, such as the Asian Infrastructure Investment Bank and the Shanghai Cooperation Organization. There have also been reports about China's efforts to set standards at the International Telecommunication Union.[35] These efforts have not been successful; however, one can imagine that if they had been successful, China would have created a niche for itself in the sale of telecommunications equipment and thus increased its economic influence.

Informational

The informational component of the CCP's plan for political power can be understood by studying the "Three Warfares" concept: public opinion warfare, psychological warfare, and legal warfare. Public opinion warfare is used to promote intense nationalism and other CCP values at home and positive impressions of China and CCP policies abroad. Psychological warfare focuses on influencing the policies of foreign government officials and the perspectives of elites. Legal warfare focuses on shaping domestic and international law to provide

justifications for CCP actions.[36] "Sharp power" is another useful concept for understanding how powers like China and Russia limit free expression within their countries and "distort political environments in democracies while simultaneously shielding their own domestic public spaces from democratic appeals coming from abroad."[37]

The film industry offers an important example of how the CCP is engaging in public opinion warfare. One component of this is the promotion of Chinese honor and strength and the degradation of adversaries, like the United States. This is demonstrated most clearly with Wolf Warrior 2, in which a Chinese soldier liberates Africans from white mercenaries while using taglines like this: "Anyone who offends China will be killed no matter how far the target is."[38]

A second component of this approach via the film industry leverages China's domestic market to pressure foreign companies to boost China's image. American movies from *X-Men: Days of Future Past* to *Independence Day: Resurgence* inserted Chinese stars into heroic roles, while Hollywood studios and actors were blacklisted for movies depicting China in a negative light.[39]

Figure 4. Bomber Jacket with and without Japan and Taiwan Patches

This led to an insidious self-censorship in Hollywood that culminated in 2022 with the producers of *Top Gun: Maverick* removing the Taiwanese and Japanese flags from Tom Cruise's iconic, patch-laden bomber jacket to avoid potential blowback from China.[40] But perhaps messing with Tom Cruise and Top Gun was a bridge too far.

The media alerted the American public to this last-minute editing before the film's release, and the producers ultimately restored the patches. The movie was never released in China, but – more important – Americans were beginning to wake up to the CCP's efforts at public opinion warfare. In a final, ironic twist to the story, a similar, but reportedly inferior, Chinese-produced movie about fighter pilots was grounded, because "the Chinese version risked ridicule in comparison."[41]

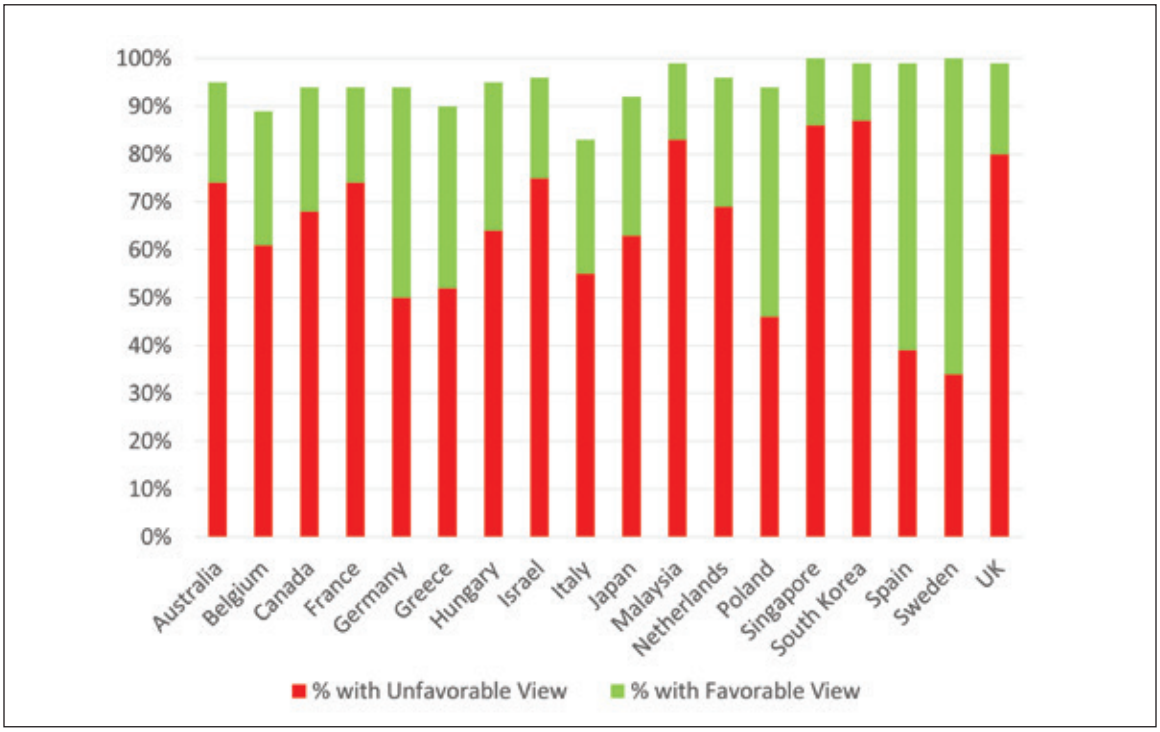
So, is the CCP's information warfare working? Is global public opinion growing more favorable toward China? No. In fact, in democratic countries, quite the opposite is unfolding.

A 2022 Pew poll of citizens in 19 democratic countries showed that the median view of China was 68 percent unfavorable and 27 percent favorable, illustrated in Figure 5. Unfavorable opinions of China were at or near historic highs in most of the 18 countries for which trend data was available.[42] By comparison, the median view of the United States among the same set of countries was 35 percent unfavorable and 61 percent favorable.[43]

But the CCP is unlikely to give up so easily. The information space is multifaceted, and setbacks in some areas—for example influencing public opinion in wealthy democracies—could perhaps be offset by advances in other areas.

Many leaders in developing or autocratic countries heap praise on China and turn a blind eye to human rights abuses. Leaders of countries like Saudi Arabia, Turkey, and Iran frequently present themselves as defenders of Muslim rights around the world, but at times mistreat their own citizens. China's economics-centric, values-neutral engagement avoids criticizing such abuses, thereby creating a reluctance for these leaders to criticize

Figure 5. International Perspectives of China in 2022



Source: Authors' analysis based on Pew Research Center, Spring 2022 Global Attitudes Survey, June 29, 2022.

the CCP's mistreatment of Uyghur Muslims. In a 2021 interview, Pakistani Prime Minister Imran Khan even denied any CCP mistreatment and stated, "China has been one of the greatest friends to us in our most difficult times, when we were really struggling."[44]

Geo-Strategic

The geo-strategic components of the CCP's plan are aimed at exerting political and military power around the world, securing access to natural resources, and – most concerningly – the domination of authoritarianism in international politics. The CCP uses both bilateral and multilateral approaches to achieve these ends.

Echoing the Cold War struggle between the free world and global communism, the CCP is marketing its autocratic political model as a direct competitor to the democracies of the United States and its allies. Arguing that Western democracy has "caused wars, chaos, and human displacement around the world and promoted its own governance model,"[45] the CCP is offering its political model as an evolved form of democracy that is "process-oriented" and "results-oriented."[46] This approach – which emphasizes stability and domestic order rather than human rights and civil liberties touted by the U.S.-led rules-based order – is appreciated among many political elites in fragile or pseudo-democracies.[47]

China has increased its diplomatic presence around the world. It has 172 embassies around the world (compared to America's 163) and deploys and receives official delegations at a robust pace.

President Xi has nurtured a new generation of aggressive "Wolf Warrior" diplomats empowered to respond to concerning policies or perceived slights by their host nation with extreme rhetoric and coercive threats. The COVID-19 pandemic set CCP engagement activities back—for example, President Xi made no trips outside of China from February 2020 to August 2022—but diplomacy ramped up again after that, including a visit by President Xi to Moscow in March 2023.

The CCP has engaged in conflict management in places like Afghanistan, Myanmar, Mali, and Sudan with an emphasis on promoting stability and strong rulers, as well as its own access to markets and natural resources.[48] Its role in the March 2023 deal between Saudi Arabia and Iran to restore relations has helped the CCP make the case that China is a responsible and influential great power. On the other hand, the CCP has struggled to play a constructive role in the conflict between Russia and Ukraine. Regardless, its recent diplomatic efforts have made it clear that the CCP sees itself as a global player rather than a regional one.

The CCP has used multilateral fora like the United Nations to criticize the United States and Western democracy, promote its governance model, and use Lawfare to shape behavior in the international body. Empirical evidence suggests that Chinese financing influences voting patterns of UN member states.[49] The CCP has also established its own multilateral fora, including the Shanghai Cooperation Organization, Forum on China-Africa Cooperation, and the Global Security Initiative to serve as a counterweight to U.S.-led institutions.

In an example of using Lawfare to further isolate Taiwan, the CCP in June 2022 asserted that the Taiwan Strait is not international water. Should the CCP begin to administer the strait as an Exclusive Economic Zone, it could become more difficult for the U.S. military to operate in those waters and deter a Chinese attack against Taiwan.[50]

Educational

The United States has long prioritized higher education as a means of projecting its national power.[51] And there are clear indications that China is paying attention and is beginning to explore how it can best leverage education as a tool of cultural soft power.

The Chinese government is now providing tens of thousands of scholarships to international students to study in China,[52] likely in part to compete against U.S. leadership in educating future world leaders. The potency of this approach as a diplomatic tool was highlighted by Secretary of State Colin Powell, who indicated that "I can think of no more valuable asset to our country than the friendship of future world leaders who have been educated here."[53] Indeed, many of those educated in the United States have gone on to promote U.S. interests and values abroad. Aleksandr Yakovlev, who influenced Mikhail Gorbachev's liberalization policies, and Lee Teng-hui, nicknamed "Mr. Democracy," who oversaw the complete democratization of Taiwan, offer two potent examples.[54]

China is also actively trying to build the prestige of its highest-end institutions, in a bid to compete against U.S. and European universities. Spending on higher education by the Chinese Ministry of Education almost doubled from $92 billion to $179 billion in the past decade,[55] and top Chinese universities—such as Fudan University, Peking university, Tsinghua University, and Zhejiang University, among others—have government funding comparable to the annual operating budget of top U.S. universities such as Harvard, MIT, and UC Berkeley.[56] Chinese universities have also succeeded in attracting top talent from Western universities. Recent investigations in the United States have revealed ties between American academics and Chinese universities. In addition, Chinese universities have established research collaboration and exchange programs with reputable Western universities, with a deliberate eye toward increasing their international appeal.

A U.S.-CHINA SOFT POWER NET ASSESSMENT FOR AFRICA

Chinese political influence is growing significantly in Africa and by some measures may surpass that of the United States. An example of this influence was offered in 2021 when only two African countries, Liberia and Eswatini, signed the UN communique condemning China's activities in Xinjiang.

This section examines the sources of Chinese soft power influence in Africa through an analysis of the four domains of China's soft power analyzed above. The intent is not to provide a comprehensive

Table 1. Illustrative comparison of U.S. and Chinese non-military power in Africa.

DIMENSION	U.S.	CHINA
Economic Power	• Important trade partner, but dwarfed by China despite a tripling of U.S.-Africa trade from $20 billion in 2002 to $62 billion in 2021. • African countries openly criticize the U.S. with less fear of economic retaliation.	• China-Africa trade grew from $11 billion in 2002 to $251 billion in 2021. • African countries do not antagonize China publicly because of its ability and willingness to use economic coercion.
Informational Power	• U.S. messaging about China has had limited effectiveness in Africa, though U.S. cultural influence (via films, music, etc.) remains strong. • Perception that U.S. is only seeking to compete with China and promote its interests in Africa without regard for African interests.	• Increasingly effective in portraying itself as promoting African interests, while overall cultural influence is still relatively weak.
Geostrategic Power	• U.S. government support for diplomatic presence on continent languishing in recent years. • Inconsistent levels of interaction between African leaders and senior U.S. leaders in recent years. • Africa perceived as being low on U.S. priority list. • Some African leaders express concern about U.S. "lectures" on governance.	• Growing Chinese diplomatic presence on the continent. • Robust engagement between Chinese leaders and African leaders. • China signals that it prioritizes Africa. The Chinese foreign minister's first international trip has always been to Africa since 1991. • China calls its engagement with Africa a partnership of equals.
Educational Power	• Investments have languished in recent years and are not widely publicized.	• China dramatically increasing numbers of scholarships to African students annually. • Confucius Institutes in Africa are reaching 100,000s of students with language and cultural programs.

assessment, but to illustrate the importance and value of a net assessment. Table 1 provides examples of U.S. and Chinese soft power in Africa for each component and the rest of the section describes each in more detail.

Economic

China is an important economic partner for Africa, both as a trade partner and a source of financing for infrastructure. And there is growing evidence that China may be using this economic influence to promote its political goals.

This economic power has been explicitly linked to African support for China in international political bodies. As an example, the lack of African support for the UN's censoring of China over Xinjiang has been attributed to "China's economic clout … most African countries simply don't want to 'pick a fight' over Xinjiang, which, to many, seems far away."[57]

In addition, there is some evidence of an economic quid pro quo from China; for instance, a study by AidData found that aid to African countries increased by about 86% when they voted in support of China at the United Nations.[58] Whereas China induces African countries with economic incentives, there is a perception that the United States reaches more often for the "gun instead of the purse in its foreign policy."[59]

There have also been claims that China is exerting a form of economic coercion in Africa called "debt trap diplomacy," in which Chinese-held debt is used to extract concessions from African nations. However, African leaders have rejected these claims, as have several academic studies.[60]

Informational

Three channels have been identified through which China influences the information and media space in Africa: training African journalists, purchasing controlling shares in African media outlets, and selling technology to Africa that provides African governments with control over the information space.[61]

As a result of these activities, many African media professionals are now promoting China's narratives.[62] These media professionals "deflect criticism of China and its African partners,"[63] and Africans who consume these positive media reports about China have been found to hold more positive views of China.[64] Although China has been successful in creating a positive image of itself in Africa, this has not been at the detriment of the United States. Afrobarometer has found that Africans hold similarly positive views of both China (59%) and the U.S. (58%).[65]

American cultural influence and U.S. government public diplomacy efforts in Africa have contributed to positive perception of the United States among Africans. However, its messaging about China has been less effective, partly because while China has "demonstrated that it has a lot to offer," the United States "appears to offer only criticism."[66] For instance, the United States has tried to dissuade African leaders from using Huawei's 5G equipment without providing a feasible alternative.[67] South African president Cyril Ramaphosa considers the U.S. messaging about Huawei to be driven by competition with China and a desire to punish Huawei because it's 5G advances are ahead of the U.S. technology.[68]

There is also growing concern among African nations that U.S. interests in Africa are mostly about contesting China and not about helping the nations of Africa.[69] For evidence, analysts point to the robust anti-China messaging that the United States has been promoting, some of which has been misleading or heavy-handed.[70]

Geostrategic

China has several geostrategic advantages over the United States in Africa. Foremost among these is that the Chinese diplomatic engagement in Africa is

robust,[71] while that of the United States is—simply said—not. U.S. embassies in Africa are understaffed, with some embassies lacking an ambassador.[72] This does not communicate that Africa is a priority. The contrast between the Forum on China-Africa Cooperation (FOCAC) and the U.S-Africa summit in Washington in December 2022 demonstrates this dramatically: while Xi took the time to meet with these leaders, few African heads of state had an opportunity to discuss their interests with President Biden.

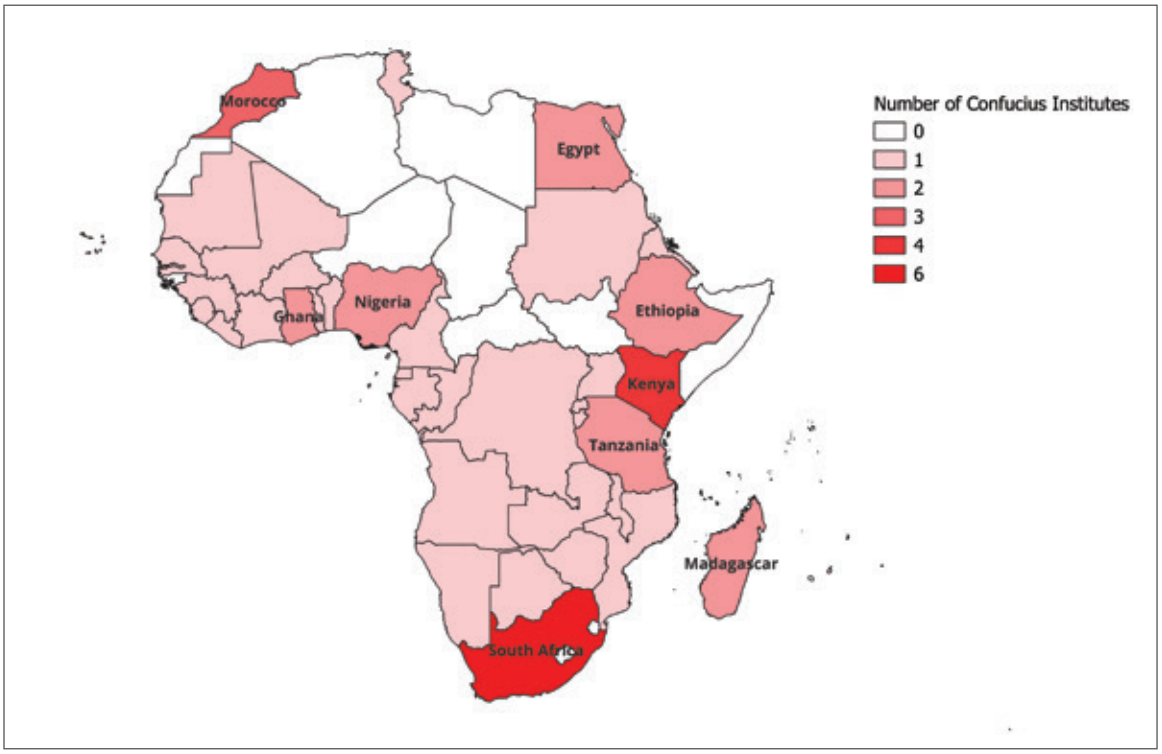
While the United States emphasizes good governance in its political engagements with African leaders, China sees this as interference in the internal affairs of another country. China believes each country should be allowed to pursue its interests in the way it sees fit. In addition, China postures itself as a leader for Global South countries, promoting their interests. This has allowed China to build goodwill among African leaders by opposing external critiques on human rights, corruption, and other sensitive issues.

This makes them susceptible to messaging from China which appears to promote their developmental interests, and which regularly reminds African leaders that China has "no history of colonialism in Africa" and should therefore be trusted.[73] Some African countries have now espoused China's view of "development without democracy," which pursues growth and industrialization without prioritizing democracy, because of China's record of growth.[74] For instance, Paul Kagame of Rwanda has stated that "because African countries have different histories, cultures and contexts, democracy may not fit African countries."[75]

Figure 6. Chinese and Rwandan Leaders Meet at a FOCAC Summit in 2018

Source: https://africacenter.org/spotlight/focac-forum-china-africa-cooperation-21-where-to-next/.

Figure 7. Confucius Institutes and Confucius Classrooms in Africa as of 2018



Source: Author's analysis based on Statista, "Number of Confucius Institutes in Africa as of December 2018, by country," December 31, 2018, Statista.

Educational

No country has trained more foreign leaders than the United States.,[76] but with China's growing cultural and education diplomacy efforts, this may change. Analysts have documented a "gradual increase in the number of African government officials and business leaders with exposure and ties to China,"[77] concluding that "we can expect stronger bridges with China to be built by the rising numbers of future African leaders studying here [in China]."[78]

China's deliberate efforts to educate African students has contributed to this. At the last couple of FOCAC meetings, China has pledged tens of thousands of scholarships and training opportunities for Africans. In addition, China had 61 Confucius Institutes and 48 Confucius classrooms across the continent in 2021,[79] reaching upwards of 150,000 students annually in Africa.[80] The U.S. government does not have a comparable program for scholarships and training.

WHAT SHOULD THE UNITED STATES DO?

President Xi is assertively exercising all components of China's soft power around the world. China's future challenges on the economic, political, and educational fronts, however, may prove to be a series of body blows that undermine Xi's plan. Some have already argued that China is a declining power facing serious headwinds ranging from resource scarcity, demographic trends, centralization of

power at the expense of economic prosperity, and an increasingly hostile external environment.[81]

Nevertheless, China's power remains a force to be reckoned with and should not be underestimated. The United States and its allies are not predestined to win this competition. The rules-based international order is under threat from China, from other autocratic powers, and from within.

Toward the end of the Cold War, many experts stepped back to reflect on America's strengths relative to the Soviet Union and other communist countries. A central conclusion that emerged from this reflective process was that the "enormous investments in education, industry, science, technology, and the infrastructure to link these elements together" were critical to "strengthening the foundations of American global power."[82]

Employing this Cold War "playbook" requires prioritizing investments at home while efficiently and effectively employing non-military power overseas. Much is already being done. But there remain many opportunities for additional initiatives, as well as the need for a more coordinated campaign.

Systematic U.S.-China soft power net assessments could serve as the foundation for such a campaign. Several organizational and policy changes could enable the development and pursuit of these proposed campaigns:

First, America's civilian agencies—most notably the State, Treasury, Commerce, and Education departments—could be given clearer mandates to prioritize efforts that strengthen America's economic, political, and educational competitiveness with China. These mandates would have explicit domestic and international measures of effectiveness to help guide and assess government efforts to get America's own house in order while also more effectively engaging allies, partners, and competitors overseas.

Second, given that so much of America's competitiveness relies on state and local agencies and the private sector, the federal government and Congress could take steps to incentivize public-private "strategic competition partnerships" at both the national and regional levels. There are pockets of excellence across the U.S. government supporting effective partnerships—for example, the Export-Import Bank's China and Transformational Exports Program and DOD's Defense Innovation Unit—that could serve as models for other initiatives.

Third, the National Security Council could establish an Office of Net Assessment to complement and incorporate the rigorous work done by DoD into a wider range of U.S. government analysis. Given the short-term focus of the National Security Council, an alternative could be a standing commission modeled on the congressionally-mandated U.S.-China Economic and Security Review Commission, but with more extensive resources and authority to draw on analysis by agencies across the U.S. government.

Finally, just as the 1947 National Security Act created a Joint Chiefs of Staff to improve coordination among America's military services, the United States could create a civilian equivalent to help coordinate departments with a role in U.S.-China competition, including State, Commerce, Treasury, and Education.[83] Each of these departments could have a net assessment office with policies that mandate systematic monitoring and evaluations of economic, political, and educational developments within the United States and China and developments in their competition internationally. Such a "Civilian Joint Staff" could also develop a competition strategy and implementation plans that set clear objectives and identify ways and means to achieve them.

President Xi and the CCP are executing a comprehensive plan to strengthen China domestically, exert its power overseas, and weaken America's leadership around the world. The United States has a National Security Strategy that acknowledges this competition but needs its own plans to compete more effectively. Developing structures and

procedures to conduct sophisticated U.S.-China net assessments could improve understanding of the relative strengths, weaknesses, and trajectories of U.S. and Chinese development. America would then be far better positioned to reinforce its strengths, address its vulnerabilities, and counter Chinese efforts to undermine its leadership of the rules-based international order. PRISM

Notes

[1] Charles Clover, "Xi Jinping signals departure from low-profile policy," *Financial Times,* October 20, 2017, https://www.ft.com/content/05cd86a6-b552-11e7-a398-73d59db9e399.

[2] Kevin Rudd, "The World According to Xi Jinping," *Foreign Affairs*, November/December 2022, https://www.foreignaffairs.com/china/world-according-xi-jinping-china-ideologue-kevin-rudd.

[3] Kevin Rudd, "Rivals Within Reason?" *Foreign Affairs*, July 20, 2022, https://www.foreignaffairs.com/china/rivals-within-reason.

[4] White House, "The National Security Strategy," October 12, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[5] White House, "The National Security Strategy," October 12, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[6] Andrew F. Krepinevich Jr., "Measures of Power: On the Lasting Value of Net Assessment," Foreign Affairs, April 19, 2019, https://www.foreignaffairs.com/articles/china/2019-04-19/measures-power.

[7] Eric Heginbotham et al., *The U.S.-China Military Scorecard*, RAND, 2015, https://www.rand.org/pubs/research_reports/RR392.html; Michael D. Swaine et al., *China's Military & The U.S.-Japan Alliance in 2030: A Strategic Net Assessment,* Carnegie Endowment for International Peace, 2013, https://carnegieendowment.org/files/net_asses_exec_summary.pdf; Center for Global Security Research, *Net Assessment and 21st Century Strategic Competition*, Lawrence Livermore National Laboratory, 2021, https://cgsr.llnl.gov/content/assets/docs/NetA_Workshop_Summary.pdf.

[8] P.J. Maykish, Abigail Kukura, and Will Moreland, *A Memo for the President on U.S. Technology Competitiveness,* Special Competitive Studies Project, November 22, 2022, https://scsp222.substack.com/p/a-memo-for-the-president-on-us-technology.

[9] Thomas G. Mahnken and Tai Ming Cheung, *The Decisive Decade: United States–China Competition in Defense Innovation and Defense Industrial Policy in and Beyond the 2020s*, Center for Strategic and Budgetary Assessments, May 22, 2023, https://csbaonline.org/research/publications/the-decisive-decade-united-state-schina-competition-in-defense-innovation-and-defense-industrial-policy-in-and-beyond-the-2020s.

[10] Michael J. Mazarr, The Societal Foundations of National Competitiveness, RAND, 2022, https://www.rand.org/pubs/research_reports/RRA499-1.html.

[11] Anthony Cordesman, *Major Powers and Strategic Partners: A Graphic Net Assessment*, Center for Strategic and International Studies, October 18, 2022, https://www.csis.org/analysis/major-powers-and-strategic-partners-graphic-net-assessment.

[12] White House, *U.S. Strategy Toward Sub-Saharan Africa*, August 2022, https://www.whitehouse.gov/wp-content/uploads/2022/08/U.S.-Strategy-Toward-Sub-Saharan-Africa-FINAL.pdf.

[13] Jacques Delisle and Avery Goldstein, China's Economic Reform and Opening at Forty, *The Brookings Institution*, 2019, https://www.brookings.edu/wp-content/uploads/2019/04/9780815737254_ch1.pdf.

[14] Yi Wen, *China's Rapid Rise: From Backward Agrarian Society to Industrial Powerhouse in Just 35 Years*, Federal Reserve of St. Louis, April 11, 2016, https://www.stlouisfed.org/en/publications/regional-economist/april-2016/chinas-rapid-rise-from-backward-agrarian-society-to-industrial-powerhouse-in-just-35-years.

[15] World Development Indicators, "GDP (current US$) - China, World," World Bank, 2023, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=CN-1W.

[16] Rocio Fabbro and Robbie Gramer, "Taiwan Isn't Playing Dollar Diplomacy Anymore," *Foreign Policy*, April 24, 2023, https://foreignpolicy.com/2023/04/24/taiwan-china-competition-dollar-diplomacy/.

[17] Isaac B. Kardon and Wendy Leutert, "Pier Competitor: China's Power Position in Global Ports," *International Security*, Vol. 46, No. 4, 2022, https://direct.mit.edu/isec/article-abstract/46/4/9/111175/Pier-Competitor-China-s-Power-Position-in-Global.

[18] Aaron L. Friedberg, *Getting China Wrong*, Polity, 2022, 86.

[19] Jacob Gu and Xiao Zibang, "Xi Boosts Party Control of China's Economy with Vast Changes," *Bloomberg*, February 28, 2023, https://www.bloomberg.com/news/articles/2023-02-28/xi-preps-china-for-intensified-overhaul-of-government-agencies.

[20] Authors' estimate based on World Bank and IMF data. Data on imports for China includes both Mainland China and Hong Kong.

[21] Xuefeng Qian, Kalsoom Rafique, and Yingna Wu, "Flying with the Dragon: Estimating Developing Countries' Gains from China's Imports," *China & World Economy*, September 30, 2020, https://doi.org/10.1111/cwe.12338.

[22] Bonny Lin, Howard J. Shatz, et al., *Bridging the Gap: Assessing U.S. Business Community Support for U.S.-China Competition*, RAND, 2022, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA1417-1/RAND_RRA1417-1.pdf.

[23] China was the top trading partner for only Mongolia, Myanmar, and Uzbekistan in 2001.

[24] James McBride, Noah Berman, and Andrew Chatzky, *China's Massive Belt and Road Initiative*, Council on Foreign Relations, February 2, 2023, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative. The approach for visualizing China's role in trade (i.e., ranking as a trade partner) is inspired by Xiaoxue Martin and Jonas Lammertink, *New Map of the Belt and Road Initiative*, Clingendael, March 5, 2021, https://www.clingendael.org/publication/new-map-belt-and-road-initiative.

[25] Mark A. Green, "China Is the Top Trading Partner to More Than 120 Countries," *Wilson Center*, January 17, 2023, https://www.wilsoncenter.org/blog-post/china-top-trading-partner-more-120-countries; Anders Sundell, "Visualizing Countries Grouped by Their Largest Trading Partner (1960-2020)," *Visual Capitalist*, February 11, 2022, https://www.visualcapitalist.com/cp/biggest-trade-partner-of-each-country-1960-2020/.

[26] Sam Kim, "Biden's Trade Chief Slams China for 'Weaponizing' Trade Against Partners," Bloomberg, March 31, 2023, https://www.bloomberg.com/news/articles/2023-03-31/biden-s-trade-chief-slams-china-for-weaponizing-trade-against-partners.

[27] The Economist, "Australia has faced down China's trade bans and emerged stronger," May 23, 2023, https://www.economist.com/asia/2023/05/23/australia-has-faced-down-chinas-trade-bans-and-emerged-stronger.

[28] Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *New York Times*, September 22, 2010, https://www.nytimes.com/2010/09/23/business/global/23rare.html.

[29] Brahma Chellaney, "China's Weaponization of Trade," Project Syndicate, July 26, 2017, https://www.project-syndicate.org/commentary/china-weaponization-of-trade-by-brahma-chellaney-2017-07.

[30] US-China Business Council, *USCBC 2022 Member Survey*, June 2022, https://www.uschina.org/reports/uscbc-2022-member-survey.

[31] Jim Duffy, "Cisco sues Huawei over intellectual property," *Network World*, January 23, 2003, https://www.networkworld.com/article/2339463/cisco-sues-huawei-over-intellectual-property.html.

[32] In Africa, traditional lenders do not prioritize hard infrastructure projects, causing African countries to borrow significant sums from China to fill this gap. Zainab Usman, *What Do We Know About Chinese Lending in Africa?* Carnegie Endowment for International Peace, June 2, 2021, https://carnegieendowment.org/2021/06/02/what-do-we-know-about-chinese-lending-in-africa-pub-84648.

[33] Martin Beraja, Andrew Kao, David Y. Yang, and Noam Yuchtman, *Exporting the surveillance state via trade in AI*, The Brookings Institution, January 2023, https://www.brookings.edu/wp-content/uploads/2023/01/Exporting-the-surveillance-state-via-trade-in-AI_FINAL-1.pdf.

[34] Noah Berman, Andrew Chatzky, and Lindsay Maizland, *Is China's Huawei a Threat to U.S. National Security*, Council on Foreign Relations, February 8, 2023, https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security.

[35] Matt Sheehan and Jacob Feldgoise, *What Washington Gets Wrong About China and Technical Standards*, Carnegie Endowment for International Peace, February 27, 2023, https://carnegieendowment.org/2023/02/27/what-washington-gets-wrong-about-china-and-technical-standards-pub-89110.

[36] Peter Mattis, "China's 'Three Warfares' In Perspective," *War on the Rocks*, January 30, 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/.

[37] Christopher Walker, "What is `Sharp Power'?" *Journal of Democracy*, Vol. 29, No. 3, July 2018, https://www.journalofdemocracy.org/articles/what-is-sharp-power/.

[38] BBC News, "Wolf Warrior 2: The nationalist action film storming China," August 4, 2017, https://www.bbc.com/news/blogs-china-blog-40811952.

[39] Erich Schwartzel, *Red Carpet: Hollywood, China, and the Global Battle for Cultural Supremacy*, New York: Penguin Press, 2022.

[40] Alison de Souza, "Hollywood used to bend over backwards for China. Top Gun: Maverick shows it might not any more," *South China Morning Post*, August 28, 2022, https://www.scmp.com/week-asia/lifestyle-culture/article/3190279/hollywood-used-bend-over-backwards-china-top-gun.

[41] Patrick Brzeski, "Mission Aborted: Why China's `Top Gun' Never Took Off, *Hollywood Reporter*, December 22, 2022, https://www.hollywoodreporter.com/movies/movie-features/chinas-top-gun-born-to-fly-1235282997/.

[42] Laura Silver, Christine Huang, and Laura Clancy, *Negative Views of China Tied to Critical Views of Its Policies on Human Rights*, Pew Research Center, June 29, 2022, https://www.pewresearch.org/global/2022/06/29/negative-views-of-china-tied-to-critical-views-of-its-policies-on-human-rights/.

[43] Richard Wike, Janell Fetterolf, Moira Fagan, and Sneha Gubbala, *International Attitudes Toward the U.S., NATO and Russia in a Time of Crisis*, Pew Research Center, June 22, 2022, https://www.pewresearch.org/global/2022/06/22/international-attitudes-toward-the-u-s-nato-and-russia-in-a-time-of-crisis/.

[44] Alex Ward, "China is buying Muslim leaders' silence on the Uyghurs", *Vox,* June 23, 2021, https://www.vox.com/2021/6/23/22545232/axios-pakistan-khan-china-uyghurs-belt-road.

[45] Amber Wang, "Western-style democracy behind wars, chaos and human misery, Chinese president tells top officials," *South China Morning Post*, June 16, 2022, https://sc.mp/96s0.

[46] State Council Information Office of the People's Republic of China, China: Democracy That Works, December 4, 2021, http://www.news.cn/english/2021-12/04/c_1310351231.htm.

[47] Yana Gorokhovskaia, Adrian Shahbaz, and Amy Slipowitz, *Marking 50 Years in the Struggle for Democracy*, Freedom House, 2023, https://freedomhouse.org/report/freedom-world/2023/marking-50-years.

[48] Bernardo Mariani, *China's Approaches to Conflict Management*, The London School of Economics and Political Science, July 5, 2022, https://blogs.lse.ac.uk/cff/2022/07/05/chinas-approaches-to-conflict-management/.

[49] Damian Raess, Wanlin Ren, and Patrick Wagner, "Hidden Strings Attached? Chinese (Commercially Oriented) Foreign Aid and International Political Alignment," *Foreign Policy Analysis, Vol.* 18, No. 3, 2022, https://doi.org/10.1093/fpa/orac010.

[50] Yun Sun, "What to Expect From a Bolder Xi Jinping," *Foreign Affairs*, July 28, 2022, https://www.foreignaffairs.com/china/what-expect-bolder-xi-jinping.

[51] Karin Fischer and Sasha Aslanian, *Fading Beacon*, APM Reports, August 3, 2021, https://www.apmreports.org/episode/2021/08/03/fading-beacon-why-america-is-losing-international-students.

[52] The Economist, "Why China is lavishing money on foreign students," January 26, 2019, https://www.economist.com/china/2019/01/26/why-china-is-lavishing-money-on-foreign-students.

[53] Joseph Nye, "Soft power and higher education," *Forum for the Future of Higher Education*, 2005, https://library.educause.edu/-/media/files/library/2005/1/ffp0502s-pdf.

[54] Ben Blanchard and Yimou Lee, "Taiwan's 'Mr Democracy' Lee Teng-hui championed island, defied China," *Reuters*, July 30, 2020, https://www.reuters.com/article/uk-taiwan-lee-obituary/taiwans-mr-democracy-lee-teng-hui-championed-island-defied-china-idUKKCN24V29C; Nye, "Soft power and higher education," 2005.

[55] Ryan Fedasiuk, Alan Omar Loera Martinez, and Anna Puglisi, *A Competitive Era for China's Universities*, Center for Security and Emerging Technology, March 2022, https://cset.georgetown.edu/wp-content/uploads/CSET-A-Competitive-Era-for-Chinas-Universities.pdf.

[56] Ryan Fedasiuk, Alan Omar Loera Martinez, and Anna Puglisi, *A Competitive Era for China's Universities*, Center for Security and Emerging Technology, March 2022, https://cset.georgetown.edu/wp-content/uploads/CSET-A-Competitive-Era-for-Chinas-Universities.pdf.

[57] Kate Bartlett, "Why African Nations Are Mostly Silent on China's Rights Record," *VOA*, September 24, 2022, https://www.voanews.com/a/why-african-nations-are-mostly-silent-on-china-s-rights-record-/6760590.html.

[58] Hisham Aidi, *China's Economic Statecraft in Africa*, The Policy Center for the New South, August 6, 2018, https://www.policycenter.ma/publications/china%E2%80%99s-economic-statecraft-africa.

[59] Robert Blackwill and Jennifer Harris, "The Lost Art of Economic Statecraft," *Foreign Affairs*, Vol. 95, No. 2, March/April 2016, https://www.foreignaffairs.com/united-states/lost-art-economic-statecraft.

[60] Deborah Brautigam and Meg Rithmire, "The Chinese 'Debt Trap' Is a Myth," *The Atlantic*, February 6, 2021, https://www.theatlantic.com/international/archive/2021/02/china-debt-trap-diplomacy/617953/; Umesh Moramudali and Thilina Panduwawala, "Evolution of Chinese Lending to Sri Lanka Since the mid-2000s – Separating Myth from Reality," *SAIS-CARI Briefing Paper No. 8*, November 2022, https://static1.squarespace.com/static/5652847de4b033f56d2b-dc29/t/638689771d0e3c4beb14bf2f/1669761400150/Briefing+Paper+-+Sri+Lanka+Debt+-+V5.pdf; Oyintarelado Moses, Cecilia Springer, Kevin P. Gallagher, "Demystifying Chinese Overseas Lending and Development Finance: Why China Became the World's Largest Official Bilateral Lender," *Boston University Global Development Policy Center – Global China Initiative Policy Brief 018,* April 2023, https://www.bu.edu/gdp/files/2023/04/GCI_PB_018_Chinas_OLDF_FIN.pdf; Bloomberg Originals, "The Myth of the Chinese Debt Trap in Africa," *YouTube*, March 17, 2022, https://www.youtube.com/watch?v=_-QDEWwSkP0&t=1s; Deborah Brautigam, "Is China the World's Loan Shark?" *The New York Times*, April 26, 2019, https://www.nytimes.com/2019/04/26/opinion/china-belt-road-initiative.html; The Citizen, "Russia and China are not trying to lead us into a 'debt trap' – Ramaphosa," October 28, 2019, https://citizen.co.za/news/south-africa/government/2196818/russia-and-china-are-not-trying-to-lead-us-into-a-debt-trap-ramaphosa/; Halima Athumani, "Uganda Not Worried China Will Seize Assets Over Rising Debt," Voice of America News, January 11, 2019, https://www.voanews.com/a/uganda-not-worried-china-will-seize-assets-over-rising-debt/4739048.html; Salem Solomon, "Zambia Continues to Borrow as China Debt Concerns Rise," Voice of America News, September 11, 2018, https://www.voanews.com/a/zambia-continues-to-borrow-as-china-debt-concerns-rise/4566634.html; Geoffrey York, "Djibouti's debt-defying stunt: Taking China's money without accepting China's control," *The Globe and Mail*, July 16, 2019, https://www.theglobeandmail.com/world/article-djiboutis-debt-defying-stunt-taking-chinas-money-without-accepting/; and Tetsushi Kajimoto and Tim Kelly, "African lender says China not trying to lead region into 'debt trap'," *Reuters*, August 30, 2019, https://www.reuters.com/article/us-japan-ticad-china/african-lender-says-china-not-trying-to-lead-region-into-debt-trap-idUSKCN1VK0AR.

[61] "China's Influence on African Media," *Africa Center for Strategic Studies*, May 12, 2023, https://africacenter.org/spotlight/chinas-influence-on-african-media/.

[62] Joshua Eisenman, "China's Media Propaganda in Africa: A Strategic Assessment," *United States Institute of Peace Special Report No. 516*, March 2023, https://www.usip.org/sites/default/files/2023-03/sr_516-china_media_propaganda_africa.pdf.

[63] Joshua Eisenman, "China's Media Propaganda in Africa: A Strategic Assessment," *United States Institute of Peace Special Report No. 516*, March 2023, https://www.usip.org/sites/default/files/2023-03/sr_516-china_media_propaganda_africa.pdf.

[64] Dani Madrid-Morales and Herman Wasserman, "How effective are Chinese media in shaping audiences' attitudes towards China? A survey analysis in Kenya, Nigeria, and South Africa," *Online Media and Global Communication*, Vol. 1, No. 4, 2022, 671-696, https://www.degruyter.com/document/doi/10.1515/omgc-2022-0047/pdf.

[65] Thomas P. Sheehy and Joseph Asunka, "Countering China on the Continent: A Look at African Views," *Afrobarometer,* June 23, 2021, https://www.afrobarometer.org/publication/countering-china-on-the-continent-a-look-at-african-views/.

[66] Caleb Slayton, "Africa: The First U.S. Casualty of the New Information Warfare Against China," *War on the Rocks*, February 3, 2020, https://warontherocks.com/2020/02/africa-the-first-u-s-casualty-of-the-new-information-warfare-against-china/.

[67] W. Gyude Moore, "African countries should stay loyal to China's troubled Huawei—regardless of Trump," *Quartz Africa*, May 27, 2019. As of July 6, 2023: https://qz.com/africa/1629078/africa-will-stay-loyal-to-chinas-huawei-regardless-of-trump.

[68] Jevans Nyabiage, "China's Huawei seeks to lead 5G boom in Africa, as US, Europe shut doors," *South China Morning Post*, November 7, 2022, https://www.scmp.com/news/china/diplomacy/article/3198622/chinas-huawei-seeks-lead-5g-boom-africa-us-europe-shut-doors.

[69] Caleb Slayton, "Africa: The First U.S. Casualty of the New Information Warfare Against China," *War on the Rocks*, February 3, 2020, https://warontherocks.com/2020/02/africa-the-first-u-s-casualty-of-the-new-information-warfare-against-china/.

[70] Caleb Slayton, "Africa: The First U.S. Casualty of the New Information Warfare Against China," *War on the Rocks*, February 3, 2020, https://warontherocks.com/2020/02/africa-the-first-u-s-casualty-of-the-new-information-warfare-against-china/.

[71] Nadège Rolland, *A new great game? Situating Africa in China's Strategic Thinking,* The National Bureau of Asian Research, 2021, https://www.nbr.org/publication/a-new-great-game-situating-africa-in-chinas-strategic-thinking/.

[72] Robbie Gramer and Amy Mackinnon, "U.S. Embassies in Africa Are Chronically Short-Staffed," *Foreign Policy*, July 22, 2022, https://foreignpolicy.com/2022/07/22/africa-embassies-short-staffed-us-sahel-china-russia/.

[73] Peter Fabricius, "China's 'palate democracy' may not be to Africa's taste," *Institute for Security Studies*, December 5, 2019, As of July 6, 2023: https://issafrica.org/iss-today/chinas-palate-democracy-may-not-be-to-africas-taste.

[74] William Gumede, "How China is changing democracy in Africa," *News24*, August 23, 2018, https://www.news24.com/news24/how-china-is-changing-democracy-in-africa-20180823.

[75] William Gumede, "How China is changing democracy in Africa," *News24*, August 23, 2018, https://www.news24.com/news24/how-china-is-changing-democracy-in-africa-20180823.

[76] Karin Fischer, and Sasha Aslanian, "Fading Beacon—The U.S. may never regain its dominance as a destination for international students. Here's why that matters," *APM Reports*, August 3, 2021, https://www.apmreports.org/episode/2021/08/03/fading-beacon-why-america-is-losing-international-students.

[77] Development Reimagined, "Where Will Africa's Students Study Abroad in Post-COVID19 Times?" webpage, September 8, 2020, https://developmentreimagined.com/2020/09/08/where-africans-study-abroad-post-covid19/#.

[78] Development Reimagined, "Where Will Africa's Students Study Abroad In Post-COVID19 Times?" webpage, September 8, 2020, https://developmentreimagined.com/2020/09/08/where-africans-study-abroad-post-covid19/#.

[79] "61 Confucius Institutes, 48 Confucius Classrooms established in Africa: white paper," *Xinhua News*, November 26, 2021, http://www.news.cn/english/2021-11/26/c_1310334064.htm. There were 59 Confucius Institutes in Africa in 2018. South Africa had six, Kenya had four, and Morocco had three, while Egypt, Ethiopia, Ghana, Madagascar, Nigeria, and Tanzania all had two each.

[80] Xinhua, "Interview: Africans show growing interest in Chinese language studies," May 20, 2018, http://www.xinhuanet.com/english/2018-05/20/c_137193310.htm.

[81] Hal Brands and Michael Beckley, "China Is a Declining Power—and That's the Problem," *Foreign Policy*, September 24, 2021, https://foreignpolicy.com/2021/09/24/china-great-power-united-states/.

[82] Robert D. Hormats, "The Roots of American Power," *Foreign Affairs*, June 1, 1991, https://www.foreignaffairs.com/articles/united-states/1991-06-01/roots-american-power.

[83] Barry Pavel and Daniel Egel, "A civilian U.S. 'Joint Chiefs' for Economic Competition with China?" *The Hill*, April 23, 2023, https://thehill.com/opinion/finance/3963170-a-civilian-us-joint-chiefs-for-economic-competition-with-china/.

Demoralizing Defeat

An Assessment of the Strategic Breakthrough, from Alexander the Great to Operation Iraqi Freedom

By Michael P. Ferguson

Russia's February 2022 invasion of Ukraine loosened a flood of theories about the evolving character of modern wars.[1] The first year of the conflict saw numerous breakthroughs but no clear victor, beginning with Russia's penetration to the outskirts of Kyiv, followed by Ukrainian counteroffensives at Kharkiv and Kherson in the fall.[2] These developments sparked debate among Western defense analysts regarding the dyad of attrition versus maneuver warfare, and further demonstrated that most breakthroughs culminate at the operational level, failing to exploit tactical success for strategic gain. While there are many historical analogues, perhaps three of the most remarkable breakthroughs were those of Alexander the Great at Gaugamela, Germany's lightning war or *blitzkrieg* into France, and the 2003

Alexander versus Darius at the Battle of Gaugamela (Painting by Pietro da Cortona, c.1648, Wikimedia Commons).

Capt. Michael P. Ferguson, USA, is a Ph.D. Student, Department of History, University of North Carolina at Chapel Hill.

Coalition invasion of Iraq. Each of these cases involved one or more penetrating maneuvers that generated strategic effects far beyond the immediate field of battle, revealing instructive principles for further research and calling into question the validity of theories that view war through the binary prism of attrition and maneuver.

The term "strategical penetration" appeared in the 1966 publication of David Chandler's history of Napoleon Bonaparte's campaigns.[3] Though historians have used different terms to describe a penetration and its subsequent methods of exploitation, they encompass what is fundamentally the same concept: a maneuver that breaks through an enemy's lines and produces disintegrating effects on his physical structure, his decision-making systems, and his will to resist. Clausewitz characterized a breakthrough as a penetration, while Capt. B. H. Liddell Hart in 1954 described it as a "strategic dislocation."[4] Modern U.S. Army doctrine adopted penetration as one of its six forms of tactical maneuver in early versions of Field Manual 3-0, *Operations*, but strategic penetration, despite its rich history, is rarely discussed in the literature and undefined in the doctrine.[5] As the Pentagon aims to transform its theory of Multi-Domain Operations (MDO) into a capability and to reform defeat mechanisms in its joint doctrine, studying trends in the breakthrough can help focus efforts.[6]

Although the practice of strategic breakthrough dates to the period of chariot warfare during the fifth century B.C., the character of war has certainly evolved dramatically since then.[7] Yet the war in Ukraine makes clear that breakthroughs in modern warfare remain as challenging to exploit strategically as they are prevalent. This complexity extends from the reality that the demoralization of an opponent, vice his simple material destruction through attrition and maneuver, remains the link between tactical victory and strategic success. This article begins with an overview of terminology before examining the three cases. It continues by identifying potential areas for further research and concludes with implications for the attrition-maneuver debate concerning Russia's war on Ukraine.

TERMINOLOGY AND SCOPE OF STUDY

A strategic breakthrough is defined in this study as an operational maneuver that penetrates defenses and sets in motion an outcome that directly supports the national aim. Its scope of effects must extend far beyond the battlefield, preferably into the minds of the public and their political officials. Reinforcing the relevance of this maneuver is its desired end, which Jomini described as "the destruction or disorganization of the enemy's forces."[8] We will return to these two elements later, as the latter complements Hart's focus on dislocation vice simple material destruction that has come to characterize some modern maneuvers.

Underpinning the strategic breakthrough are the concepts known as defeat mechanisms in U.S. Joint doctrine, two of which this study prioritizes as essential to a penetration: dislocation and disintegration. Although the Major Combat Operations (MCO) Joint Operating Concept (JOC) identifies three such mechanisms, it emphasizes "disintegration as the principal mechanism used to defeat an adversary's military system" through integrated destruction and dislocation.[9] The army defines disintegration as "the means to disrupt the enemy's command and control, degrading the synchronization and cohesion of its operations."[10] These physical and psychological processes can both support and be supported by a successful breakthrough. Much of the academic research on defeat mechanisms, however, focuses overwhelmingly on the material destruction of systems at war, but a broader historical review of the breakthrough suggests that attrition alone does not produce strategic effects for major powers, and it is in fact the will to

fight—the moral and psychological factors—that are most consequential.[11] America's wars in Iraq and Afghanistan and Ukraine's extraordinary resistance to Russia's repeated invasions are a further testament to this observation.

The premise of a strategic breakthrough's utility is based on the understanding that uprooting an opponent's assumptions regarding how a battle might unfold can be decisive because it induces cognitive dissonance. This shock can foment doubt that leads to cascading miscalculations and muddied war policy, or what J.F.C. Fuller called "strategic paralysis."[12] In Clausewitz's analysis of the offensive maneuver, he describes the process as one of "using mistakes into which the enemy can be lured" to generate effects that disrupt an opponent's equilibrium.[13] Hart went further by arguing that dislocation is in fact the aim of strategy itself, and its "sequel" may be the destruction of enemy forces or a more advantageous position in battle.[14]

Increased sophistication of competitor anti-access/area denial (A2/AD) capabilities and the introduction of MDO as an official operational concept have placed greater emphasis on penetration in U.S. doctrine. Published in October 2022, the U.S. Army's updated Field Manual 3-0, *Operations*, describes how the service will fight in MDO. The Army defines MDO as "the combined arms employment of joint and Army capabilities to create and exploit relative advantages that achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commanders."[15] In response to guidance within the 2018 and 2022 National Defense Strategies, the U.S. Army intends to stand up an MDO-capable combined arms formation known as the "Penetration Division," further demonstrating the enduring relevance of maneuver.[16] Indeed, the Pentagon's 2012 Joint Operational Access Concept (JOAC), which still informs joint force development, provides a requirement for such capacity:

> *The penetration is designed to disrupt the integrity of the enemy defensive system, the preferred defeat mechanism, by striking at critical hostile elements, such as logistics and command and control nodes, long-range firing units, and strategic and operational reserves.*[17]

The JOAC continues by implying that a strategy of attrition could be politically unacceptable to the United States, which in turn obligates the joint force to build capabilities that support penetrating maneuvers and systems paralysis:

> *The historical alternative to [a penetration] is to attack the perimeter of the enemy's defenses…. Such an approach operates primarily by attrition and does not threaten the integrity of the enemy's defensive system…. This may actually play into the enemy's anti-access/area-denial strategy, which likely will attempt to use space and time to inflict cumulatively unacceptable casualties on an advancing joint force.*[18]

More recent studies from experts such as Heather Venable and Michael Kofman, however, argue that paralysis in modern war is a fallacy, but even if true, this would make analysis of strategic breakthroughs critical to understanding why something so prevalent in the past, and present in current joint doctrine, is supposedly nonexistent in the future.[19]

Penetrating maneuvers must be examined through a historically broad lens because each expression did not occur in a vacuum. They were revisions of previous approaches studied deeply by military leaders and fused with the ways and means available in their time. Although there are many examples of breakthroughs at sea, in the interest of concision this study focuses on the land domain alone.[20] Regarding terminology, though the terms *breakthrough* and *penetration* are distinct activities in U.S. doctrine, for simplicity's sake, they are used interchangeably here.[21] Finally, this is not a review of grand strategy—or even strategy for that matter—but rather one of maneuver with strategic implications. As such, the following offers the reader

sufficient political context for each example, but only so far as necessary to make clear the nature of strategic breakthrough.

ALEXANDER III OF MACEDON (331 B.C.)

John Keegan hailed Alexander "the greatest of conquerors."[22] Part of this martial greatness came from his ability to smash through enemy lines and send them into chaos. Up to the point of Alexander III's reign as king of Macedonia, chariots were most often used to break through the frontages of ancient armies and throw them into disarray.[23] Yet breakthroughs occurred elsewhere as well. Xenophon wrote that the Spartan's maritime formation at the Battle of Arginusae in 406 was designed as a single line "to be able to execute the maneuvers of breaking through and wheeling back on the enemy," thus describing a penetration followed by an exploitation as codified in military doctrines even today.[24] But none so deftly applied the penetration as Alexander, and he did so without chariots.

Plutarch tells us Alexander won battles when only sixteen years old while appointed regent of Macedonia in King Philip II's absence, but Alexander solidified his affinity for the breakthrough two years later against an Athenian alliance at the Battle of Chaeronea in 338.[25] Philip's death in 336 allowed Alexander to assume the throne and launch his campaign against the Persian King Darius III, a decisive point of which was the breakthrough at the Battle of Gaugamela (also called Arbela, a city about sixty-five miles away).[26] The intensity of the battle and the massive dust clouds produced by its cavalry led to conflicting accounts in the ancient sources regarding numbers and specifics.[27] A balanced analysis suggests that in the fall of 331 a Macedonian force of approximately 50,000 routed a Persian army of at least 150,000 with a penetrating charge and exploitation.[28] Prior to the encounter, these numbers did not startle Alexander.

In Diodorus's version of events, the king slept soundly the night before because "Darius had relieved all his stress by assembling his forces in one place," thereby making certain the Persian Empire's demise.[29] Curtius wrote that Alexander instructed his soldiers not to fear the enemy because there "were more men *standing* on the Persian side, but more were going to be *fighting* on the Macedonian."[30] Just before moving to contact, as he had done two years prior at Issus, Alexander charged the hearts of his men by riding up and down their ranks, shouting out many by name and reminding them of their acts of valor to boost morale.[31]

The Persian commander Bessus, who would later depose Darius (for which Alexander had Bessus' nose and ears removed), occupied the Persian left with a mix of foreign cavalry including Bactrians.[32] Darius positioned himself center-left. On his flanks were his elite Immortals and the Greek mercenaries for whom Alexander reserved a particular disdain. The Persian lines also held 200 scythed chariots and fifteen Indian war elephants. On the Macedonian side, Alexander gave command of his right to Cleitus (not Cleitus the Black) under whom he entrusted Hephaestion to lead the elite hypaspists (like special operations forces).[33] Alexander took up the right with his infantry phalanx opposite Darius, looking to avoid a battle of attrition, and cut the head off the snake by killing or capturing the Persian king himself.[34]

The battle involved some of the fiercest fighting recorded in Alexander's campaigns. Scythed chariots dismembered bodies and ripped open men's torsos. Persian cavalry nearly destroyed the Macedonian baggage train and later encircled but could not kill Parmenion, perhaps Alexander's most capable general.[35] The battle's turning point was characteristic of Alexander's god-like mystique, as his army found renewed vigor when they saw an eagle hovering above the king's head amid the chaos.[36]

Charged by this symbol, the Macedonians managed to spread the Persian left thin enough for Alexander to mount another horse—as he had exhausted several—and take his Companions and some infantry on a lightning charge at Darius, splitting his lines.[37] In this instance the violence of the breakthrough itself was decisive, particularly after Darius's charioteer was killed by a javelin that some thought wrongly had pierced the Persian king himself. Darius was the first to flee, and with him went the integrity of his left flank as the Macedonians broke through and wheeled back onto the Persian center and right.[38]

The fighting continued, but Alexander would not claim his prize here. Again, as at Issus in 333, the Persian king evaded him. Yet having fled Alexander in both battles, Darius's claim as god king lost its luster, and the outcome at Gaugamela heralded the demise of the Persian Empire. Ian Worthington surmised that news of this disgrace "spread like wildfire through the Persian line and broke the soldiers' spirits."[39] David Lonsdale also wrote of the impact this "crushing physical assault" had "on the morale and cohesion of the enemy army."[40] By summer 330 Darius was dead, and Alexander laid claim to all of Persia. Yet this was not enough. Alexander's string of unbroken victories sparked within him an insatiable lust for conquest that bloated his strategic aims the further east he marched, eventually driving his army to near mutiny on two occasions.[41]

From Alexander's experience we may draw two conclusions. The first is that a strategic penetration with cavalry came to personify the Alexandrian way of warfare.[42] The second is that the effect of demoralization on the opposing army and not simply its material destruction was paramount to Alexander's military philosophy. At Gaugamela, Alexander sought to demoralize the Persian army by disintegrating its central control system—the king they called a god—and it worked brilliantly. The centuries that followed bore witness to other leaders who shunned attrition warfare in favor of decisive battle, such as Napoleon Bonaparte. But despite Napoleon's record of successful breakthroughs, his *Grand Armée* reached Moscow in a state of disrepair that emboldened instead of demoralizing the Russian army in October 1812.[43] Like Alexander, Napoleon's hubris stretched his forces too thin. As the breakthrough evolved over the centuries, militaries continued to draw inspiration from Alexander, culminating in one of the industrial age's most decisive strategic breakthroughs, that at Sedan.

THE *WEHRMACHT'S* BLITZKRIEG (1940)

As much myth as fact surrounds the German Army's 1940 blitz into France. Liddell Hart, who kept detailed logs of public statements before, during, and after *blitzkrieg*, believed that more

Gen. Heinz Guderian studies a map in France, June 1940 (Polish National Digital Archives, Wikimedia Commons)

"nonsense has been written about it than about any other event of the war."[44] As recently as 2005, German military scholar Dr. Karl-Heinz Frieser was still aiming to dispel "blitzkrieg legends."[45] Yet there is no debate that the armored push through a densely-forested yet poorly-defended point near the Maginot Line led to the fall of Paris in thirty-six days—a key political objective for Germany.[46]

Numerous conditions made this possible, including flaws in French planning prior to the invasion and a great deal of apprehension from the French High Command after. In Williamson Murray's estimation, "It is hard to see in retrospect how the French could have made greater errors in preparing for battle."[47] Among them was Paris' top-down approach to battlefield control that strangled initiative and tactical momentum—a relic of centralized Napoleonic command systems that French military thinking had yet to retire. Also present was a certain degree of luck, but fundamentally the German maneuver was a textbook example of a breakthrough with far-reaching strategic implications.[48]

Much as Alexander benefitted from his father's reforms, the German Army had already charted the course to *blitzkrieg* conceptually when Adolf Hitler rose to power in 1933.[49] The new chancellor simply endorsed it and put it to use.[50] Forefathers of *blitzkrieg*, such as Gen. Heinz Guderian, Gen. Hans von Seeckt, and Col. Ernst Volckheim, drew from the experiences of military thinkers throughout history to formulate their theories.[51] By the time Hitler invaded Poland in 1939, the characteristics of *blitzkrieg* were evident, as explained in September by Lt. Gerald Niebergall of Germany's 24th Artillery Regiment: "They are calling it 'blitzkrieg.' The panzers break through and get behind enemy lines, where they begin to disrupt the enemy's communications and supply lines. The sight of enemy tanks behind the lines also panics the enemy. It is apparently working perfectly in Poland."[52]

There existed a remarkable degree of secrecy around planning the invasion of France. When on 9 May 1940 orders came to invade, most commanders were oblivious. The plan involved the revolutionary use of armor in the maneuver that finally, as Liddell Hart had suggested, untethered tanks from the umbilical cord of the infantry.[53] This piercing thrust was not directed at France's impressive fortification known as the Maginot Line stretching north to south from Luxembourg to the Swiss border, but rather at the strategic gap in the densely vegetated Ardennes Forest that the French High Command saw as an impenetrable natural obstacle.[54] Panzer Group Kleist assigned Gen. Guderian's 19th Panzer Corps to lead this thrust through the Ardennes in what became a masterclass in combined arms warfare.[55] Though tanks often receive much of the credit, the success of armor was only made possible through the skillful application of engineers, airpower, and glider infantry.

By early morning of 10 May, Guderian's 1st Panzer Division, commanded by Gen. Friedrich Kirchner, crossed into Luxembourg as German bombers struck Allied airfields mercilessly, severing Dutch communications lines and grounding aircraft.[56] These strikes, coupled with the French High Command's reluctance to authorize sorties near Belgian villages, enabled German armor to enter Holland nearly uncontested. Still, a decisive point of the invasion was the impressive airborne seizure of Eben Emael, the northernmost post in the Maginot Line.

This Belgian fort atop the Albert Canal near Liége was home to a full battalion of troops (about 1,300 men), eighteen pieces of artillery, and numerous turrets and machine gun positions.[57] Though considered impenetrable at the time, Alistair Horne cited insufficient antiaircraft systems as the primary flaw in its design, while more recent analysis from Canadian Col. Bernd Horn suggested that the fort's lack of infantry fighting positions and rooftop

Entrance of Fort Eben-Emael, the northernmost post in the Maginot Line (Photo by Jean Huston, 4 August 2019, Wikimedia Commons).

obstacles were its downfall. It is likely that Horne referred to the constraints on Belgian antiaircraft weapons, which relied on sound and not radar, and thus allowed the quiet gliders to slip through unseen. At any rate, these shortcomings exposed the fort to a critical vulnerability that Captain Walter Koch and his Storm Group would soon exploit.

Koch's unit of roughly 260 men, comprising mostly sappers and divided into four detachments, had trained on models of Eben Emael since 1939.[58] First Lieutenant Rudolph Witzig led the 85 men of Storm Detachment Granite who would take the fort. Under cover of darkness in the early hours of 10 May, they loaded eleven gliders in Cologne before Ju-52s towed them 8,000 feet above Aachen and released them to begin their silent descent.[59] Despite moderate complications, by the next day Witzig's outfit had destroyed the weapons positions with shaped explosive charges and the Belgians there had surrendered.[60] Horne emphasized the "psychological impact of the sudden collapse of Eban Emael," which triggered rumors of a secret German weapon, drew Paris' eyes north toward the Line and away from Ardennes, and caused demoralization to spread like "germs of a deadly plague."[61] The seizure of Eben Emael proves that deception and psychological warfare were core elements of the breakthrough to Sedan.

Loss of the fort gave way to an orchestra of combat engineers clearing obstacles and blowing bridges across the 19th Corps' front, but even these measures could not prevent the occasional stall of the panzers' advance. While bunched up in a snaking convoy that stretched nearly 100 miles, German officers looked up anxiously at the sky awaiting French bombers to appear—but they never came.[62] Guderian's lead division fought a decisive battle on 11 May near Suxy while the French High Command still believed the German main effort lay between Maastricht and Liége, about 50 miles north of the Ardennes Forest.

As Luftwaffe squadrons continued pummeling targets to enable 1st Panzer's advance, it was not until midafternoon that French pilots received authorization to release ordnance over towns, but the *blitzkrieg* had already moved into the densely vegetated Ardennes, and it was too late. Delays like this prove that Germany's otherwise brilliant plan may not have been successful were it not for numerous mishaps on the French and Belgian side.[63] Guderian did not experience an enemy air attack until the morning of 12 May, and even then, it was rather ineffective.[64] On that day, 1st Panzer broke through the Ardennes and before dusk occupied Sedan relatively unopposed, thus securing a foothold in France. Little more than a month later, lead elements of Germany's 87th Infantry Division entered the open city of Paris, and France's Ninth Army was no more.

The breakthrough at Sedan was so shocking to the French and European consciousness that it all but secured Germany's victory. Like Alexander before him, though, Hitler's impressive victories in Poland and France imbued him with delusions of grandeur, which led to a slew of disastrous overreaches the following year. One of these began on 21 June 1941 when three million German troops crossed the Soviet border and by 30 September received orders to storm Moscow.[65] Still, Gen. William Donovan, founder of the Office of Strategic Services, divulged that many resistance fighters in Nazi-occupied France only began jumping on the "bandwagon" after D-Day in June 1944, even though British intelligence had agents there as early as 1940 supporting the underground movement.[66] It took the largest multinational beachhead and airborne assault in history to reinvigorate European morale after *blitzkrieg*.

Guderian admitted that this maneuver was in part the brainchild of British officers and armor advocates J.F.C. Fuller and B. H. Liddell Hart, and by extension a continuation of the type of Alexandrian warfare both admired.[67] Indeed, historians have long-since compared Alexander to Hitler, if only for their capacity for slaughter and favor of the offense. Yet perhaps their greatest military similarity is their contribution to the study of the penetrating maneuver.[68] The world saw many breakthroughs after 1940, but the 2003 allied invasion of Iraq bore witness to a sophisticated new type of penetration that for all its novelty possessed the same characteristics, and remained vulnerable to the same flaws, as those centuries prior.

THE COALITION BLITZ TO BAGHDAD (2003)

A unique aspect of the modern breakthrough is the robust application of airpower and special operations forces (SOF) to shape and soften the battlefield. This form of strategic penetration is less about the traditional outcome of destruction and more the secondary effects highlighted by Jomini and Liddell Hart of disintegration and dislocation. However, they still possess the same fundamental purpose that drove Alexander to charge Darius at Gaugamela: the demoralization of an enemy rather than the simple attrition of his forces.

In March 2003, Iraqi Army numbers were vague, resting somewhere between 150,000 to 200,000 in strength, while the loyalist Republican Guard, pulled mostly from the Al Anbar province in the Sunni Triangle, consisted of roughly 60,000 men.[69] Regarding conventional forces, Iraq's 11th Division held the south near Al Nasiriyah, while the 6th, 8th, 14th, and 10th Divisions took position along the Tigris River arrayed south to north through Al Amarah. Saddam tasked his Republican Guard divisions to encircle Baghdad and fight to the death, assuming any Coalition forces who made it that far would crumble against a wall of his fanatic supporters.[70] Not included in these numbers were the irregular *fedayeen* spread about the country in unknown strength, composed of foreign fighters as much as Iraqis. Having suffered a crippling defeat

twelve years prior in the First Gulf War and fighting a near decade-long conflict with Iran just before that, an Iraqi force already fitted with poorly maintained Soviet equipment faced an American military at the height of its technological dominance.

American planners therefore selected a much smaller force than the one used to push Saddam out of Kuwait in 1991, assuming modern weapons would compensate for a lack of mass. Williamson Murray and Robert Scales explained this revolution in one of the earliest military histories of the invasion:

Instead of focusing on overwhelming numbers, planners focused on electrons—sensors and information systems that displayed with greater fidelity than ever before what was happening on the battlefield. This allowed the Coalition to apply fewer numbers in precise ways aimed at the psychological dislocation of the enemy.[71]

While awaiting presidential authority to invade, military leaders took the initiative to position forces in Kuwait under the guise of training exercises beginning in late 2002. Meanwhile, President George W. Bush built a coalition of 37 partner nations to fight alongside U.S. forces.[72] By 19 March, special operations teams from the United States, Poland, and Britain had carried out several high-risk, covert shaping operations in Iraq.

Under the direction of U.S. Special Forces Col. John F. Mulholland, teams destroyed long-range ballistic missiles and their launchers to deny Saddam the option of attacking America's allies in the region. Navy SEAL operators under Capt. Robert S. Harward, along with European commandos, secured petroleum reserves on land and offshore while the 160th Special Operations Aviation Regiment eliminated early warning systems and observation posts along Iraq's border with Kuwait. As this took place, U.S. Special Forces Col. Charles Cleveland directed elements to link up with Peshmerga forces in the north while a widespread psychological warfare campaign took place across the country.[73]

These well-coordinated operations dislocated Saddam's security apparatus from critical resources it relied upon for situational awareness and intelligence. As a result, before the invasion began the Iraqis were disintegrated and incapable of assessing Coalition intentions, as evidenced by Saddam dedicating a significant portion of his combat power to guard his flanks in anticipation of incursions via Iran and Jordan that never came.[74] In essence, the Coalition achieved strategic paralysis against Saddam's regime through a systems disintegration approach that enabled a strategic breakthrough.

The invasion began on 20 March 2003 with an early-morning F-117A Nighthawk strike on the suspected location of Saddam Hussein and his two sons, Uday and Qusay.[75] Like Alexander's run at Darius, the strike was unsuccessful, but, as at Gaugamela, it had other effects in the psychological domain. The bombing made apparent to Saddam that the United States intended to remove him and his sons from power and was prepared to strike deep within Iraq's borders to do so. Thus began the air campaign that coincided the following day with a ground invasion through Kuwait.

The main force consisted of the U.S. Third Infantry Division, U.S. First Marine Division, U.K. First Armoured Division, elements of the U.S. 82nd and 101st Airborne Divisions, and various smaller units such as the British Paras and several attack aviation units.[76] Though all this power was aligned under U.S. Central Command (CENTCOM) based in Tampa, Florida, the Coalition Forces Land Component Command (CFLCC) and Air Component Command (CFACC) planned and executed the operational maneuver. All told, the Coalition entered Iraq with a force of approximately 60,000—less than one tenth of the combat power used to expel Saddam from Kuwait in 1990.[77]

Drawing on the historical success of *blitzkrieg*, the armored divisions planned to advance north to Baghdad straddling the Euphrates and clear a path

An F-117 from the 8th Expeditionary Fighter Squadron (EFS) out of Holloman Air Force Base (AFB), N.M., flies over the Persian Gulf on April 14, 2003 in support of Operation Iraqi Freedom in March 2003 (Photo by Derrick C. Goode USN, Wikimedia Commons).

for the infantry who would mop up any dwindling resistance in the cities to the rear of the tanks. The U.S. Army's official history of the war used declassified documents to reveal that America's apprehension during the Gulf War convinced Saddam that the Coalition would not invade, and if it did, it would seize and hold cities sequentially.[78] In this light, it appears Saddam attempted a strategy like that of Russia against Napoleon on his way to Moscow in 1812, looking to exhaust the Coalition's supply lines before it reached Baghdad.

Securing the cities was indeed critical due to the 300-mile logistics routes upon which the lead elements relied for resupply of fuel, food, and ammunition. But Coalition forces sacrificed security for speed as Alexander and Guderian had done before them, and it paid off. By 5 April, the Third Infantry Division began conducting "thunder runs" into the heart of Baghdad, splintering the ill-equipped Republican Guard charged with defending the city.[79] Saddam's regime fell in twenty days, roughly sixteen days faster than the *Wehrmacht* took Paris.

As an evolution from *blitzkrieg*, the invasion of Iraq was a groundbreaking demonstration of joint, combined arms warfare. No single instrument was decisive. Rather, the careful synchronization of many forms of power was key to success. From the widespread use of special operations teams for shaping the theater to the rapid employment of airpower in the deep fight, the fall of Baghdad was made possible by means that pried apart Iraqi defenses and enabled not one, but two breakthroughs within three weeks: the first at the southern border with Kuwait and the second at the perimeter defense surrounding Baghdad.

Like the French High Command and Darius before it, Saddam did not believe his enemy would commit to a full-scale invasion, especially one that pressed all the way to the capital, because American officials had been reluctant to do so previously.[80]

In turn, Saddam did not prepare for one. If the Coalition's goal was to destroy the Iraqi Army's ability to coordinate and fight as a cohesive element, it achieved that consummately. But what followed were objectives disconnected from the original act of penetrating Baghdad, which simply fractured the existing army and created new but less hierarchical threat groups.[81] The Iraqi Army was *dislocated* and *disintegrated*, but not necessarily *demoralized* or destroyed, as many of its members evaporated into the cities and joined the insurgency already underway with the *fedayeen*.[82]

U.S. forces failed to adequately anticipate or appreciate the complexity of the operation's fourth phase, when Saddam had been removed and Coalition forces were charged with conducting stability operations by erecting peacetime governing institutions even as combat operations persisted.[83] Large swaths of irregular *fedayeen* were not demoralized but rather energized by the presence of a foreign occupying force—as were thousands of fighters around the world who flocked to fight the Western invaders.[84] Like Alexander's tunnel vision in Central Asia, Western policy became fixated on simply getting to Baghdad and removing Saddam, and thus encountered great difficulty after doing so.

From the coalition breakthrough we may draw three lessons that contribute to a richer understanding of the history of strategic breakthrough. The first is that a dislocated and disintegrated force, if not also demoralized, will find creative ways to resist even a much larger opponent. Second, the sophistication of an opponent's defense is concomitant to the scope of conditions required to penetrate said defenses. Setting conditions for a breakthrough was a separate campaign of equal import even against Saddam's second-rate army. This process would likely be far more complex when facing modern

M1A1 Abrams Main Battle Tanks under the Victory Arch in Baghdad, 2003 (Photo by Technical Sergeant John L. Houghton, Jr., U.S. Air Force, Wikimedia Commons).

A2/AD systems.[85] Yet conversely, developments in long-range precision fires, precision strike, offensive Cyber, and clandestine activities could make paralysis more likely because they provide additional options for targeting critical nodes that an enemy relies upon to mobilize and sustain its forces.[86] Finally, past is not always prologue. Saddam's experience with the U.S. military in 1991 polluted his thinking in 2003, and ingratiating aides only contributed to his rosy assumptions about a supposed lack of political will in Washington.

FURTHER STUDY OF THE STRATEGIC BREAKTHROUGH

From this study one may conclude that despite great leaps in military technology and the character of warfare, war's common nature exposes fundamental truths in the strategic breakthrough that remain constant. Among them are:

- Successful breakthroughs depend on massing effects, not necessarily forces, at the decisive place and time to *dislocate* control nodes, *disintegrate* an opponent's organization, and *demoralize* his forces.[87]
- Breakthroughs end in failure most often not because of inferior technology or tactics, but because the process of demoralization remains *technologically agnostic*.
- Many breakthroughs are preceded by *political and military deception campaigns*, which means the most effective are also the least expected.
- The most successful breakthroughs tend to incite within their arbiters a *hubris* that leads to *catastrophic overreach*.

Even in the digital age, these maxims lend further credibility to the conclusions of Thucydides, Napoleon, Clausewitz, Col. Ardant du Picq, and Michael Howard regarding the moral nature of war.[88] The realities of trench warfare in Ukraine are a further testament to this truth.[89] One potential framework for additional study involves using these findings to examine penetrations within the context of center of gravity (COG) analysis or theories of victory (TOV) and theories of success (TOS).[90] In 2008, J. Boone Bartholomees, Jr. questioned America's ability to connect a TOV on the battlefield to its political origins.[91] Since then, scholars and practitioners have expressed the need for a TOS that incorporates such considerations.

It is necessary then to recognize some of the ways modern states might adapt the strategic breakthrough for the Information Age. Just as Alexander aimed to disintegrate the Persian army's ability to coordinate and fight at Gaugamela by removing its king instead of simply killing its soldiers, a theory of modern breakthrough involves similar designs. Military theorists in the Chinese Communist Party characterize this as *systems warfare*, a process of attacking an opponent's critical systems that allow it to fight rather than the opponent itself.[92] The defeat mechanism of disintegration compliments a systems warfare approach.

This idea is a byproduct of the Information Age's introduction of constraints principles to military operations, in which the more tightly integrated battlefield networks become, the less disruption its individual parts can sustain without causing the entire system to collapse. Cyber and counter-space attacks are not yet powerful enough to be decisive in war, but they could set conditions through a digital penetration that disrupts military mobilization, early warning, and response systems, thus exposing a nation to paralysis and exploitation.[93] As of August 2023, U.S. officials were searching for suspected Chinese malware that had infiltrated critical infrastructure networks and could potentially disrupt military mobilization and logistics.[94]

Moscow's cyber-attacks and targeting of Ukraine's civilian infrastructure in late 2022 challenged Kyiv's resolve, but the depletion of a

significant portion of Russian combat power before winter prevented the attacks from demoralizing Ukrainian resistance.[95] The strikes were, however, emblematic of systems warfare. Modern armies are largely connected by networks that commanders rely upon to make decisions and measure effects; therefore, maneuver is not the only means by which an enemy can be physically and psychologically dislocated. Sophisticated counter network attacks will become more valuable, especially as armies further disperse their forces and supply depots to confound increasingly advanced detection, targeting, and fires capabilities.[96]

Reliance on digital networks in modern war has also given life to conversations surrounding the role of systems warfare in support of multi-domain operations, including how the concept might contribute to reforming defeat mechanisms.[97] Frank Hoffman, Marinus Era Novum, and Heather Venable are noteworthy contributors to this conversation, and the attrition-versus-maneuver dialectic permeates the debate. In 2012, Canadian Forces officer Cole F. Petersen characterized the binary attrition-or-maneuver structure aptly as a false dichotomy.[98] Neither approach is objectively superior to the other because it is the combined effects of attrition and maneuver on the cognitive domain of an enemy, and subsequent degradation of his will to resist, that induces victory. The conclusions of scholars such as Stephen Biddle and Frank Hoffman appear in line with this assessment.[99] Petersen further observed that because attrition and maneuver are also tactical concepts often injected into strategic discussions, Western doctrine should instead use *annihilation* and *exhaustion* in strategy formulation.[100]

Still, though, the aim of both is to render an opponent unwilling (exhaustion) or unable (annihilation) to resist. Eado Hecht's paradigm that portrayed defeat mechanisms as ways of targeting either the *will* or *capability* of an opponent reinforces this perspective.[101] In either case, the question remains: what will most effectively demoralize an enemy under conditions deemed acceptable to the national interest? The answer to that question might be attrition through a robust defense that gains decision space in one instance and maneuver with a bold offense in another. Discerning which may have the greatest demoralizing impact on an adversary can help link operations to strategic effects.

DESPITE ATTRITION IN UKRAINE, THE UNITED STATES NEEDS TO MANEUVER

This study has shown that attrition can set conditions for strategic breakthrough, whether through systems or personnel destruction, whereas the demoralizing effect of a successful penetration can create opportunities for further attrition. Alexander pursued the former while the *Wehrmacht* in France and the Coalition in Iraq applied the latter. Even while extolling the superiority of attrition, William F. Owens conceded that maneuver can "gain a positional advantage relative to an opponent" which "may be used to deliver overwhelming violent attrition."[102] Franz-Stefan Gady and Michael Kofman acknowledged the enduring presence of this reciprocity more recently while lauding Ukraine's strategy of attrition against Russia:

[Ukraine's] offensive effort proved successful in autumn 2022 because the conditions had been set by Russian forces' structural personnel deficit and extensive attrition. The attrition had multiple causes, including combat losses, soldiers who refused to fight and depleted morale due to exhaustion. Attrition has been both sides' primary approach at the tactical level of war; manoeuvre warfare yielded operational results because extensive attrition made it possible.[103]

Debate continues over Ukraine's strategic approach, but Russia's attempt to seize Kyiv within the first week of the invasion is a far cry from a strategy of attrition.[104] Poorly imagined maneuver is not

evidence of maneuver's futility, and Ukraine's effective use of attrition does not signal an evolution in warfare. In his examination of George Washington's Revolutionary War strategy, Russell F. Weigley characterized attrition as a "strategy founded upon weakness" in relation to one's opponent—an assertion supported by Washington's own writings.[105] Smaller armies or those with restrictions imposed upon their operations often use attrition to gain time, degrade enemy morale, and preserve forces. In essence, it is a strategy of deliberate protraction.

While discussing delays to Ukraine's 2023 counteroffensive in May, President Volodymyr Zelensky said equipment shortages would make the casualties associated with such a maneuver "unacceptable."[106] The value of attrition and maneuver is as circumstantial in Ukraine as it has been elsewhere—commanders and doctrine writers can ill afford to select one or the other as uniquely emblematic of the future.[107] That said, the strategies of Washington and Zelensky suggest that attrition is most effective in defensive wars where resistance and survival are key strategic objectives. This method is less germane for expeditionary militaries, such as those of the United States, Britain, and Australia, that rely upon a strong offensive capability to gain strategic access and project military power globally as opposed to defending locally.

For the United States to achieve this access against an adversary with like means, the evidence suggests that a systems disintegration approach targeting space assets and commercial network infrastructure could be the most effective way to produce a strategic breakthrough. Martin Van Creveld foresaw these dependencies in 1985. His concerns would likely be amplified by the contested logistics challenges associated with, for instance, a hypothetical conflict in the Indo-Pacific region:

Without a firm directing hand providing for the uninterrupted flow of supplies, replacements, and reinforcements a machine-age army will cease to function within a matter of days in the same way as an automobile factory deprived of its supply parts. Insofar as such an army consists of more specialized parts and to that extent is more dependent on mutual cooperation, its disintegration may possibly be more rapid and more complete than that of a preindustrial force.[108]

Recent testimony from senior U.S. Space Force officials supports this assessment.[109] In other words, an expeditionary power such as the United States can hardly rely on a strategy of attrition if it cannot disintegrate an enemy's operational integrity and penetrate its A2/AD defenses to gain the positional advantage that makes attrition possible. For the United States to gain such an advantageous position, it must maneuver into one.

There remains much to learn from the war in Ukraine, but those lessons are not a universal template for the future of warfare, nor do they necessarily foretell the conditions of America's next conflict in a way that should compel the joint force to abandon its doctrinal and conceptual foundations in maneuver. Researchers must be careful to avoid flirting with presentism by drawing overly broad inferences from the latest war. Each conflict, when viewed in isolation and particularly as it is unfolding, has no more of a monopoly on the future than its predecessors.[110]

CONCLUSION

Strategic breakthroughs have for thousands of years been the method of choice for achieving dislocation, disintegration, and demoralization of an opposing force. They must be shocking enough to destabilize an opponent's response systems and impose—if only temporarily—decision paralysis. The targeting of psychological nodes through a systems disintegration approach that disrupts the assumptions behind an enemy's plans makes this possible. Without this element, material destruction alone, whether through attrition or maneuver, is more likely to protract war than bring it to an end. This study also

reveals a paradox: the more effective the breakthrough, the more hubris it instills in its arbiters, thus increasing the propensity for overreach.

Alexander's seamless chain of victories fed into his dream of conquering the known world.[111] In 1941, less than a year after taking Paris, Hitler thought it wise to betray Joseph Stalin and invade Russia using similar tactics under the assumption he could destroy the Soviet Union in ten weeks.[112] The United States, reveling in the speed with which it deposed Saddam Hussein, spent the next two decades struggling to build constitutional democracies with cohesive national armies in tribal regions of the Middle East. In each instance, both maneuver and attrition played a role, but their strategic effects in isolation were indecisive, whereas their interplay proved critical.

Many successful breakthroughs ultimately end in failure due less to poor tactics or even shortfalls in theories of victory and more to flawed theories of success related to the presumed effects of material destruction on the moral forces of the opposition. For Hitler in Russia and the Coalition in Iraq, these lessons came at a high price after grinding campaigns of attrition followed their breakthroughs. Maneuver, then, most often fails in the exploitation phase where demoralization must link tactical activities to strategic outcomes by influencing the moral dimension of war.[113] Identifying the causal forces of societal demoralization in further research could help shape a clearer understanding of the roots of victory and failure in past conflicts, while also informing the visualization of those yet to come. PRISM

Notes

[1] Paul Robinson, "The Russia-Ukraine Conflict and the (Un)Changing Character of War," *Journal of Military and Strategic Studies* 22, 2 (Dec. 2022): 65-88.

[2] Steven Pifer, "The Russia-Ukraine war and its ramifications for Russia," *Brookings Institution*, 8 December 2022, available at https://www.brookings.edu/articles/the-russia-ukraine-war-and-its-ramifications-for-russia/; Editorial Board, "Ukraine's Kherson Breakthrough," *Wall Street Journal*, 11 November 2022, available at https://www.wsj.com/articles/ukraines-kherson-breakthrough-counteroffensive-russia-vladimir-putin-11668199263.

[3] David G. Chandler, *The Campaigns of Napoleon: The Mind and Method of History's Greatest Soldier* (New York: Simon & Schuster, 1966), 162-163, 175.

[4] Carl von Clausewitz, *On War*, trans. Michael Howard (Princeton, NJ: Princeton University Press, 1976), 3.12; B. H. Liddell Hart, *Strategy* (London: Faber & Faber, Ltd., 1954), 326-329, 336.

[5] U.S. Army doctrine lists *dislocation* and *disintegration* as two of its four "defeat mechanisms," but omits demoralization's role in either. Field Manual [FM] 3-0, *Operations* (Washington, D.C.: U.S. Government Publishing Office [GPO], October 2022); FM 3-90, *Tactics* (Washington, D.C.: U.S. GPO, May 2023).

[6] Frank Hoffman, "Defeat Mechanisms in Modern Warfare," *Parameters* 51, no. 4 (2021): 49-66, https://doi.org/10.55540/0031-1723.3091.

[7] For instance, Thucydides' *Peloponnesian Wars*, Herodotus' *The Histories*, and Xenophon's *A History of My Times*.

[8] Antoine Henri de Jomini, "Supplement to the Summary of the Art of War" in *The Art of War*, trans. G. H. Mendell and W. P. Craighill (New York: 1862).

[9] Donald H. Rumsfeld and Peter Pace, *Major Combat Operations Joint Operating Concept v.2.0* (Washington, D.C.: U.S. GPO, December 2006), v, 12.

[10] FM 3-0, *Operations*, 3-20.

[11] Heather Venable, "Paralysis in Peer Conflict? The Material versus the Mental in 100 Years of Military Thinking," *War on the Rocks*, 1 December 2020, available at https://warontherocks.com/2020/12/paralysis-in-peer-conflict-the-material-versus-the-mental-in-100-years-of-military-thinking/.

[12] Fuller used this term to describe Germany's 1940 *blitzkrieg* into France. J.F.C. Fuller, *The Conduct of War, 1789-1961: A Study of the Impact of the French, Industrial, and Russian Revolutions on War and its Conduct* (New Brunswick, NJ: Rutgers University Press, 1961), 255-256.

[13] Clausewitz, *On War*, 7.13.

[14] Liddell Hart, *Strategy*, 325.

[15] FM 3-0, *Operations*, p. 1-2.

[16] Nathan A. Jennings, "Considering the Penetration Division: Implications for Multi-Domain Operations," Association of the United States Army: Land Warfare Paper No. 145, 26 April 2023, available at https://www.ausa.org/publications/considering-penetration-division-implications-multi-domain-operations.

[17] Martin E. Dempsey, *Joint Operational Access Concept (JOAC) v.1.0* (Washington, D.C.: U.S. GPO, 17 January 2012), 24, available at https://dod.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf.

[18] Ibid.

[19] Venable, "Paralysis in Peer Conflict?"; Michael Kofman, "A Bad Romance: US Operational Concepts Need to Ditch their Love Affair with Cognitive Paralysis and Make Peace with Attrition," *Modern War Institute at West Point*, 31 March 2021, available at https://mwi.westpoint.edu/a-bad-romance-us-operational-concepts-need-to-ditch-their-love-affair-with-cognitive-paralysis-and-make-peace-with-attrition/.

[20] Artemisia, a brazen female commander who sailed for Xerxes and escaped Salamis, was the only dissenting voice against battling Athens at sea. Herodotus, *Histories*, 8.83-8.96, 8.68.

[21] A breakthrough is "a rupturing of the enemy's forward defense that occurs as a result of an attack." The maneuver permits the passage of an exploitation force. Without exploitation a penetration is useless, as evidenced by the Persian breakthrough to Alexander's baggage train at Gaugamela. FM 3-90, *Tactics*, 5-17.

[22] John Keegan, *A History of Warfare* (London: Vintage Books, 1993), 74.

[23] Arrian, *Anabasis*, 1.1.8-13.

[24] Xenophon, *A History of My Times*, 1.6.29-32; Also see, FM 3-90, *Tactics*; FM 3-0, *Operations*, 6-106 – 6-124.

[25] Diodorus, 16.85-87; Plutarch, *Alexander,* 9.2-3; Ian Worthington, *Philip II of Macedonia* (New Haven, CT: Yale University Press, 2008), 147-151.

[26] Arrian, *Anabasis*, 3.15.5.

[27] At times the dust became so thick that the Macedonian army stumbled around "like people in the dark," slashing and stabbing at sounds: Curtius, 4.15.33. See also Ian Worthington, *By the Spear: Philip II, Alexander the Great, and the Rise and Fall of the Macedonian Empire* (New York: Oxford University Press, 2014), 191.

[28] Arrian, *Anabasis*, 3.8.6; Diodorus, 17.39.4; Curtius, 4.12.13; Plutarch, *Alexander* 31.1.

[29] Diodorus, 17.56.3-4.

[30] Curtius, 4.14.5; Alexander's gumption was the opposite of the trepidation Arrian describes on the Persian side: Arrian, *Anabasis*, 3.11.1-2.

[31] Arrian, *Anabasis,* 2.10.2; Plutarch, *Alexander,* 33; Justin 11.9.3-6; Worthington, *By the Spear*, 191.

[32] Arrian, *Anabasis*, 3.11.3-7; Diodorus 17.60.4; Curtius 4.14.8; For the mutilation of Bessus, see Arrian, *Anabasis*, 4.7.3.

[33] Arrian, *Anabasis*, 3.11-12.

[34] Curtius 4.13.35; Diodorus 17.57.1-3.

[35] Here we see that Darius's forces penetrated the Macedonian line first but failed to exploit it sufficiently. Diodorus 17.58.5; Curtius 4.15.14-21.

[36] In the *Iliad*, Homer depicts Aias the Achaian receiving a similar omen in battle against Hektör: Homer, *Iliad*, 13.821-823; Alexander was said to have carried a copy of the *Iliad* containing Aristotle's personal notes. Plutarch, *Alexander*, 8.

[37] Curtius 4.15.31; Arrian, *Anabasis*, 3.14.2.

[38] Arrian 3.14.3; Diodorus 17.60.4.

[39] Worthington, *By the Spear*, 192.

[40] David J. Lonsdale, *Alexander the Great, Killer of Men: History's Greatest Conqueror and the Macedonian Art of War* (New York: Carroll & Graf, 2004), 141.

[41] Philip's 337 proposal to the League of Corinth sanctioned the invasion of Persia only. Use of the term "mutiny" remains disputed because the Macedonian Army never sought to replace Alexander, but the incidents at the Hyphasis River in India (326) and Opis (324) were clearly problematic. Arrian, Anabasis, 4.5.6, 7.8.3; Diodorus 17.109.

[42] Lonsdale expands upon Alexander's combined-arms approach that placed greater emphasis on the decisive use of cavalry. David J. Lonsdale, *Alexander the Great: Lessons in Strategy* (New York: Routledge, 2007), 79-86.

[43] In a 3 January 1813 letter, the aide to Napoleon's brother described the derelict conditions of Napoleon's army in Moscow. Napoleon Bonaparte, *Correspondence in "memoires du roi Joseph," Vol. II* (New York: D. Appleton and Company, 1856), 19.769; Chandler, *Campaigns of Napoleon*, 819.

[44] B. H. Liddell Hart, *Defence of the West* (New York: William Morrow & Co., 1950), 3, 4-6.

[45] Manstein conceptualized the plan in November 1939, which was so unpopular he was given an infantry corps and placed in the third wave of the attack. Guderian thus took up the cause of advocating Manstein's plan to the high command. Gen. Heinz Guderian, *Panzer Leader*, trans. Constantine Fitzgibbon (Cambridge, MA: De Capo Press, 1996), 89-90; Karl Heinz Frieser, *Blitzkrieg Legend: The 1940 Campaign in the West* (Annapolis, MD: Naval Institute Press, 2005), 2; Hart, *Defence of the West*, 8-11.

[46] The Germans called the Ardennes region "the prolonged Maginot Line" and saw it as a weakness. Guderian, *Panzer Leader*, 96-97.

[47] Williamson Murray, "May 1940: Contingency and Fragility of the German RMA" in *The Dynamics of Military Revolution, 1300-2050* (New York: Cambridge University Press, 2001), 164.

[48] The defenders of Eban Emael failed to wage a counterattack because of a miscommunicated order, and the French division at Monthermé – which 6th Panzer Corps reached by 14 August – possessed not a single anti-tank weapon. Hart, *Defence of the West*, 7-8, 11; Anti-tank weapons and mines arrived too late or were not used. Horne, *To Lose a Battle*, 380-381, 415.

[49] Robert M. Citino, *The Path to Blitzkrieg: Doctrine and Training in the German Army, 1920-1939* (Mechanicsburg, PA: Stackpole Books, 1999), 223; Robert M. Citino, *Death of the Wehrmacht: The German Campaigns of 1942* (Lawrence: The University Press of Kansas, 2007), 15.

[50] Hitler did, however, prioritize airpower and heed the urgings of generals such as Guderian who argued that armor should spearhead the operation. Hart, *Defence of the West*, 6; Hitler entertained Guderian's plan during a 14 February 1940 wargame where other generals were skeptical. Guderian, *Panzer Leader*, 91-92.

[51] Citino, *Path to Blitzkrieg*, 201-202; Ian Ona Johnson, "Ernst Volckheim, Heinz Guderian, and the Origins of the German Armored Doctrine," *Journal of Military History* 87, no. 1 (January 2023): 145-168.

[52] German officer Siegfried Knappe recorded this statement from his 1st battalion adjutant as the first casualty reports came in from the Polish front. Siegfried Knappe and Ted Brusaw, *Soldat: Reflections of a German Soldier, 1936-1949 [English version]* (New York: Orion Books, 1992), 137.

[53] Citino, *Path to Blitzkrieg*, 203-204; Horne, *To Lose a Battle*, 79-80, 90.

[54] A puzzling conclusion in Horne's estimation, given the maneuverability of modern motorized formations. Horne, *To Lose a Battle*, 243-244.

[55] Frieser, *Blitzkrieg Legend*, 100-102.

[56] To Guderian's north, Gen. Rommel's 7th Panzer Division sped through Belgium. Horne, *To Lose a Battle*, 258-261; Guderian, *Panzer Leader*, 98-99.

[57] Bernd Horn, *Innovation and Daring: The Capture of Eban Emael, 10 May 1940* (Ottawa, Ontario: Canadian Special Operations Forces Command, 2014), 12; Horne, *To Lose a Battle*, 267.

[58] Horn, *Innovation and Daring*, 17-20; Horne, *To Lose a Battle*, 268.

[59] Horne, *To Lose a Battle*, 267-269.

[60] Liddell Hart, *Defence of the West*, 7-8

[61] Horne, *To Lose a Battle*, 270.

[62] Ibid., 284.

[63] Liddell Hart, *Defence of the West*, 11-13.

[64] The airstrike targeted 1st Panzer's bridge in southern Bouillon but left the structure undamaged. Guderian, *Panzer Leader*, 100; Horne, *To Lose a Battle*, 300.

[65] Operation Barbarossa, the invasion of Soviet Russia, evolved into Operation Typhoon, Hitler's march on Moscow, which ended in disaster. Citino, *Death of the Wehrmacht*, 34-49.

[66] MI6 Chief Maj. Gen. Sir Stewart G. Menzies had agents in France by 1940. Sir Charles Hambro, leader of England's Special Operations Executive, had operatives there since at least 1943. Douglas Waller, *Wild Bill Donovan: The Spymaster Who Created the OSS and Modern American Espionage* (New York: The Free Press, 2011), 165, 237, 247; Will Irwin, *The Jedburghs: The Secret History of the Allied Special Forces, France 1944* (New York: Public Affairs, 2005), 42.

[67] Guderian, *Panzer Leader*, 20; Van Creveld claimed that Fuller and Hart deserve no credit for German armored warfare, but Guderian's writings are at odds with this. Creveld, *Command in War*, 192-193.

[68] Victor Davis Hanson, *Carnage and Culture: Landmark Battles in the Rise of Western Power* (New York: Doubleday, 2001), 89-90.

[69] John Keegan, *The Iraq War* (New York: Vintage Books, 2005), 128-129.

[70] Joel D. Rayburn and Frank Sobchack (eds.), *The U.S. Army in the Iraq War – Volume 1: Invasion – Insurgency – Civil War, 2003-2006* (Carlisle, PA: U.S. Army War College Press, 2019), 73-75.

[71] Williamson Murray and Maj. Gen. Robert H. Scales, Jr., *The Iraq War: A Military History* (Cambridge, MA: The Belknap Press of Harvard University Press, 2005), 93.

[72] Stephen A. Carney, *Allied Participation in Operation Iraq Freedom* (Washington, D.C.: U.S. Army Center of Military History, 2011), 1.

[73] Mulholland commanded 5th Special Forces Group, Cleveland 10th Special Forces Group, and Harward Naval Special Warfare Group Central Iraq. Rayburn and Sobchack, *Army in the Iraq War*, 81-82; Murray and Scales, *The Iraq War*, 185-190.

[74] Rayburn and Sobchack, *Army in the Iraq War*, 73, 83.

[75] Murray and Scales, *The Iraq War*, 154-156; See also Lt. Gen. T. Michael Moseley, "Operation IRAQI FREEDOM – By the Numbers," Assessment and Analysis Division, U.S. Air Force, 30 April 2003, available at https://media.defense.gov/2013/Jun/13/2001329960/-1/-1/0/uscentaf_oif_report_30apr2003.pdf.

[76] CENTCOM and CFLCC planners originally scheduled five divisions for the invasion, but Turkey's refusal to allow an attack from the north reduced the invasion force to roughly three divisions. Rayburn and Sobchack, *Army in the Iraq War*, 59, 63-64.

[77] The boots on the ground number comes from Gen. Mattis' memoirs: James Mattis, *Call Sign Chaos: Learning to Lead* (New York: Random House, 2019), 85; Fiscal year 2003 saw a monthly average of 78,100 U.S. troops in Iraq, though the operational report listed 141,100 directly supporting. Amy Belasco, "Troop Levels in the Afghan and Iraq Wars, FY2001-FY2012: Cost and Other Potential Issues," *Congressional Research Service*, 2 July 2009, available at https://sgp.fas.org/crs/natsec/R40682.pdf. There were more than 500,000 American troops in Saudi Arabia by the end of 1990. Shannon Collins, "Desert Storm: A Look Back," *U.S. Department of Defense*, 11 January 2019, available at https://www.defense.gov/News/Feature-Stories/story/Article/1728715/desert-storm-a-look-back/.

[78] Rayburn and Sobchack, *Army in the Iraq War*, 70-73.

[79] Keegan, *The Iraq War*, 193-195; Murray and Scales, *The Iraq War*, 230.

[80] Murray and Scales, *The Iraq War*, 95-96; Rayburn and Sobchack, *Army in the Iraq War*, 69-70.

[81] Michael J. Mazarr, *Leap of Faith: Hubris, Negligence, and America's Greatest Foreign Policy Tragedy* (New York: Public Affairs, 2019), 185-186, 205, 341, 372-374; Thomas E. Ricks, *Fiasco: The American Military Adventure in Iraq, 2003-2005* (New York: Penguin Press, 2006), 209-212, 393-394; Bing West, *No True Glory: A Frontline Account of the Battle for Fallujah* (New York: Bantam Dell, 2005), 20-24.

[82] Ahmed S. Hashim, "The Insurgency in Iraq," *Small Wars & Insurgencies* 14, 3 (2003): 1-22; Rayburn and Sobchack, *Army in the Iraq War*, 154, 156-157; Mattis, *Call Sign Chaos*, 113, 133-134.

[83] Thomas E. Ricks, *The Generals: American Military Command from World War II to Today* (New York: Penguin Press, 2012), 397-431; Lawrence Freedman, *Command: The Politics of Military Operations from Korea to Ukraine* (New York: Oxford University Press, 2022), 430.

[84] Angela Rabasa and Cheryl Benard, *Eurojihad: Patterns of Islamist Radicalization and Terrorism in Europe* (New York: Cambridge University Press, 2015).

[85] Hassan M. Kamara, "Countering A2/AD in the Indo-Pacific: A Potential Change for the Army and the Joint Force," *Joint Force Quarterly* 97, no. 2 (2020): 97-102.

[86] This theory came to the surface in July: David E. Sanger and Julian E. Barnes, "U.S. Hunts Chinese Malware That Could Disrupt American Military Operations," *New York Times*, 29 July 2023, available at https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

[87] The recent update to U.S. Army tactical doctrine mentions *mass* more than 100 times but refers more often to "massing overwhelming combat power" and "forces" than it does effects. FM 3-90, *Tactics*, 1-6 – 1-8, 8-11.

[88] Thucydides famously wrote that "fear, desire for respect, and gain" drove all wars. Thucydides, *The Peloponnesian War,* Walter Blanco (ed.), trans. Walter Blanco and Jennifer Tolbert Roberts (New York: W. W. Norton & Company, Inc., 1998), 1.76; Gen. H. Camon, *La guerre Napoléonienne – Les systems d'operaitons* (Paris: 1907), 5; Chandler, *Campaigns of Napoleon*, 155-156; Clausewitz, *On War*, 3.3; Picq believed moral factors govern war's conduct and outcome. Charles Jean Jacques Joseph Ardant du Picq, *Battle Studies*, trans. Roger J. Spiller (ed.) (Lawrence: University Press of Kansas, 2017), 51-60.

[89] Michael P. Ferguson, "Why Modern Wars Cannot Escape the Trenches," *The Hill*, 8 December 2022, available at https://thehill.com/opinion/national-security/3765218-why-modern-wars-cannot-escape-the-trenches/.

[90] A TOV is associated with military strategy while a TOS considers how military victory feeds into political objectives. Frank Hoffman, "The Missing Element in Crafting National Strategy: A Theory of Success," *Joint Force Quarterly* 97, no. 2 (2nd Quarter 2020): 55-64.

[91] This phrase, seemingly coined by Eliot Cohen, gained popularity as the United States struggled in Iraq. J. B. Bartholomees, "Theory of Victory," *Parameters* 38, no. 2 (2008), https://doi.org/10.55540/0031-1723.2419.

[92] Alexander waged a form of systems destruction warfare against Darius. Jeffrey Engstrom, *Systems Confrontation and Systems Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), 9-18; For a proposed U.S. counter, see Robert O. Work, "A Joint Warfighting Concept for Systems Warfare," *Center for a New American Security*, 17 December 2020, available at https://www.cnas.org/publications/commentary/a-joint-warfighting-concept-for-systems-warfare.

[93] Grace B. Mueller, Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias, *Cyber Operations during the Russo-Ukrainian War* (Washington, D.C.: Center for Strategic and International Studies, July 2023), 1-3; see also Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 43-53, 172.

[94] Sanger and Barnes, "U.S. Hunts Chinese Malware."

[95] Pia Hüsch and Joseph Jarnecki, "All Quiet on the Cyber Front? Explaining Russia's Limited Cyber Effects," *RUSI*, 1 June 2023, available at https://rusi.org/explore-our-research/publications/commentary/all-quiet-cyber-front-explaining-russias-limited-cyber-effects; "Ukraine: Russian Attacks on Energy Grid Threaten Civilians," *Human Rights Watch*, 6 December 2022, available at https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians.

[96] Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V. Danylyuk, and Nick Reynolds, "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February – July 2022," *RUSI*, 30 November 2022, 2-3, available at https://static.rusi.org/359-SR-Ukraine-Preliminary-Lessons-Feb-July-2022-web-final.pdf.

[97] Frank Hoffman, "Updating Defeat Mechanisms: Concepts of Victory for Contemporary Warfare," *Marine Corps Gazette* (February 2022), 72-77, available at https://mca-marines.org/wp-content/uploads/Updating-Defeat-Mechanisms.pdf.

[98] Cole F. Petersen, "Clearing the Air – Taking Manoeuvre and Attrition Out of Strategy," *Infinity Journal* 2, no. 3 (2012): 15-19, available at https://www.militarystrategymagazine.com/article/clearing-the-air-taking-manoeuvre-and-attrition-out-of-strategy/.

[99] Stephen Biddle, "Ukraine and the Future of Offensive Maneuver," *War on the Rocks*, 22 November 2022, available at https://warontherocks.com/2022/11/ukraine-and-the-future-of-offensive-maneuver/; Hoffman, "Updating Defeat Mechanisms," 76.

[100] Petersen, "Clearing the Air."

[101] Eado Hecht, "Defeat Mechanisms: The Rationale Behind the Strategy," Infinity Journal 4, no. 2 (Fall 2014): 24-30, available at https://www.militarystrategymagazine.com/article/defeat-mechanisms-the-rationale-behind-the-strategy/.

[102] William F. Owen, "The Manoeuvre Warfare Fraud," *RUSI Journal* 153, no. 4 (2008).

[103] Franz Stefen-Gady and Michael Kofman, "Ukraine's Strategy of Attrition," *Survival* 65, no. 2 (2023), 7-8, https://doi.org/10.10180.

[104] John Spencer, "The 2022 Battle of Kyiv: A Lecture," *Modern War Institute at West Point*, 14 April 2023, available at https://mwi.westpoint.edu/the-2022-battle-of-kyiv-a-lecture/.

[105] Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington: Indiana University Press, 1973), 5.

[106] Hugo Bachega, "Zelensky says Ukraine needs more time for counter-offensive," *BBC News*, 11 May 2023, available at https://www.bbc.com/news/world-europe-65550427.

[107] Michael Kofman, for example, believes embracing a doctrine of attrition is inevitable and necessary. Kofman, "A Bad Romance."

[108] Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 185-186.

[109] U.S. Space Force Chief of Space Operations Gen. B. Chance Saltzman testified on 14 March 2023 that he expects to see blinding and disruption of U.S. satellite sensors in the next conflict. C. Todd Lopez, "Space Force Focuses on Partnership, Spirit, Combat Readiness," *U.S. Department of Defense*, 15 March 2023, available at https://www.defense.gov/News/News-Stories/Article/Article/3330161/space-force-focuses-on-partnerships-spirit-combat-readiness/.

[110] Humankind's track record is lackluster in this regard, as nations tend to exaggerate the influence of emerging military capabilities or concepts on war's conduct. Lawrence Freedman, *The Future of War: A History* (New York: Public Affairs, 2017), 278-280.

[111] This goal became clear after the demise of Bessus and obeisance controversy. Arrian, *Anabasis*, 4.9-10.

[112] Germany's chief of the army general staff told Guderian they would conquer Russia in 8-10 weeks, to which Guderian objected. Guderian, *Panzer Leader*, 142; Richard Overy, *Blood and Ruins: The Last Imperial War, 1931-1945* (London: Penguin Press, 2021), 147-149, 166.

[113] Citino, *German Way of War*, 311-312.

Preparing for a Post-Armed Conflict Strategic Environment

By Michael P. Fischerkeller

In the months following Russia's invasion of Ukraine, scholars and policymakers began examining potential outcomes, including Russian victory, loss, or stalemate. No matter the outcome of the armed conflict, the North Atlantic Treaty Organization (NATO) and its member states will likely face significant strategic risk in the immediate post-armed conflict environment. The constancy of Russia's unrelenting ambition, the increase in Russia's operational tempo and intensity of cyber operations targeting NATO and its member states, and the ongoing attrition of Russia's conventional force capabilities portend dangerous cyber futures for the Western allies.

Devastation in Bucha, Ukraine (Public Domain, Rawpixel.com).

Dr. Michael P. Fischerkeller is a Researcher at the Institute for Defense Analyses.

From the lens of cyber persistence theory, one can forecast two alternative cyber futures.[1] First, *because of* the resultant vacuum of conventional force capabilities, Russia will sustain or increase the current tempo and intensity of cyber campaigning targeting NATO and its member countries while taking care to not breach the tacit ceiling of cyber agreed competition—that is, Russia will not engage in cyber operations that cause armed-attack equivalent effects. Alternatively, *in spite of* the resultant vacuum of conventional force capabilities but because of its nuclear deterrent, Russia will be emboldened to breach the tacit ceiling of cyber agreed competition and target NATO and its member states with cyber campaigns/operations of armed-attack equivalence. Both futures rest on the same assumption—at the end of kinetic hostilities, Russia will not fold up its tent and go home but rather will continue its strategic competition with NATO through aggressive cyber campaigning.

Both futures should cause NATO and the West to pause and reassess current objectives, preparations for the post-armed conflict environment, strategic shifts or tilts to China by some member states, and NATO's strategic concept.[2] A post-armed conflict Russia that is more aggressive in and through cyberspace has the potential to weaken the democratic world and the transatlantic alliance and, in so doing, create an "invaluable distraction dividend" and "strategic running room" for China to exploit.[3] NATO and its member states should not make strategic decisions based on the presumption that when major combat operations abate in the Russia-Ukraine armed conflict, so too will an active strategic threat from Russia.

In this article, I review alternative outcomes of the armed conflict, consider Russia's military capability profile in a post-armed conflict environment, and posit alternative cyber security futures based on Russian motivation(s) and capabilities. I then address three policy questions: Is the current objective of weakening only Russia's conventional force generation functions prudent? How can NATO optimize its member states' aggregate cyber capabilities and capacities to prepare for these cyber futures? And, might recent shifts and tilts to China distract from such preparations?

POTENTIAL RUSSO-UKRAINIAN ARMED-CONFLICT OUTCOMES

Most observers predict one of three armed-conflict outcomes: Russian victory, Russian loss, or stalemate.[4] In every case, Russia's motivation(s) will fuel aggressive actions against NATO and its member states.

Russian Victory

There is consensus that a Russian victory would invite increased adventurism by Russia. Michael Miklaucic argues that a Russian victory would be "very bad," as it would "signal that armed force is the arbiter of sovereignty" and that "armed aggression is not only permissible behavior but effective statecraft."[5] Eliot Cohen similarly argues that Putin would be empowered to expand Russia's influence with "unlimited violence."[6] Noting that Putin has yet to halt his efforts to dominate the security structure in Europe, Anthony Cordesman argues that a Russian victory would leave Russia so divided from Europe that Russia would face a major ongoing confrontation with the West.[7] And Dov Zakheim argues that if Russia triumphs to any degree, including merely retaining control of Crimea, it could evoke in Moscow and across the country a sense of popular triumphalism to undermine or invade other states in the near-abroad.[8]

Russian Loss

Views also converge in discussions of a Russian loss. Liana Fix and Michael Kimmage propose that the most plausible Ukrainian victory would be "winning small," where Russia is expelled from the western side of the Dnieper River, and

Ukraine establishes perimeters of defense around the Russian-controlled areas in Ukraine's east and south and secures its access to the Black Sea.[9] Justin Bronk argues that Moscow would "feel very vulnerable" were this to be the outcome (because Russia's conventional force capabilities will be significantly degraded both in terms of their actual and perceived potential),[10] but Fix and Kimmage posit that a Ukrainian victory will "only spur more Russian intransigence in its wake" and that Russia will use a narrative of humiliation to stir domestic support for a renewed effort to control Ukraine.[11] Additionally, they argue that Putin would continue to engage in "active measures" to probe for western vulnerabilities.[12] Zakheim argues that should Russia suffer defeat, Moscow would be "consumed by revanchist irredentism" and thus a danger to its contiguous neighbors and to all of Europe for years to come.[13] Finally, Cohen argues that a defeated Russia will still be "malevolent, angry, and vengeful" and that it will "engage in subversion, political warfare, and malicious behavior of all kinds."[14]

Russian and Ukrainian Stalemate

Rudolf Adam argues that a third potential outcome—a stalemate or "frozen conflict"—is the likely result of the armed conflict, comprising an "uneasy truce along a disputed and heavily armed line of demarcation."[15] Both Eugene Rumer and Cordesman suggest that this outcome would be similar to the permanent standoff on the Korean Peninsula, where both sides would agree to stop fighting but remain deployed.[16] But Cordesman argues that, although this kind of unstable settlement has worked with the two Koreas, it has done so only at the cost of constantly being on the edge of another war. Thus, this outcome would do little or nothing to stabilize the overall security of Western Europe and particularly the European states along the Russian border. He claims it would create the equivalent of a "rules-based disorder" where individual European states would secure their position relative to Russia along different lines, with some bolstering a deterrent posture and others seeking to ease tensions. Joshua Huminski argues that, should the outcome be stalemate, Russia will nonetheless continue to be "determined to bring it (Ukraine) back into its orbit."[17]

No matter the outcome of the fighting in Ukraine, the constancy of Russia's ambition to expand its power will continue to pose a strategic threat to NATO and its member states.[18]

RUSSIA'S POST-ARMED-CONFLICT CAPABILITY PROFILE

Absent a severe escalation of the armed conflict, Russia's nuclear arsenal and the strategic deterrent it provides will remain intact in the immediate post-armed-conflict environment. Additionally, although open-source reporting offers some evidence of NATO member states disrupting and degrading deployed Russian or Russian-affiliated cyber capability sets and/or command and control infrastructure,[19] no reporting points to the West directly targeting the cyber force generation functions of Russia's military, intelligence services, contractors, and proxies. Therefore, Russia's cyber capabilities will also be largely intact after kinetic conflict ends.

If the outcome is a stalemate, Cordesman argues that Russia would continue to build up its conventional capabilities,[20] although Russia would be motivated to do so no matter the outcome. But, importantly, Zakheim argues that "wartime losses and economic sanctions may set it [Russia] back in the immediate future."[21] It may be the case, moreover, that the "immediate future" is a period of several years. In September 2022, British officials remarked that some of Russia's conventional forces had been "severely weakened."[22] For example, "1 GTA [1st Guards Tank Army] suffered heavy casualties in the initial phase of the invasion and had not been fully reconstituted prior to the Ukrainian

counteroffensive in Kharkiv," said the U.K. Ministry of Defense. As one of the most prestigious of Russia's armies, it is allocated for the defense of Moscow and intended to lead counterattacks in the case of a war with NATO.[23] The Ministry further concluded that "With 1GTA and other WEMD [Western Military District] formations severely degraded, Russia's conventional force designed to counter NATO is severely weakened. It will likely take years for Russia to rebuild this capability."[24] This view has been echoed by Estonian military intelligence, the German Council on Foreign Relations, and the European Council on Foreign Relations.[25]

Comments by U.S. Secretary of Defense Lloyd Austin III in April 2022 bolster this assessment. "We want to see Russia weakened to the degree that it can't do the kinds of things that it has done in invading Ukraine," stated Secretary Austin, further noting that Russia "has already lost a lot of military capability, and a lot of its troops, quite frankly. And we want to see them not have the capability to very quickly reproduce that capability."[26] The reference to reproduction capacity is notable, as it suggests the United States is seeking to degrade Russia's conventional force generation functions (i.e., its defense industrial base). This policy, if successful, would further increase the time necessary for Russia to reconstitute its conventional force capabilities.[27] The policy was clarified and expanded days later in remarks by then-press secretary of the White House Jen Psaki who, when asked whether U.S. policy was now to permanently degrade Russia's military, replied that Austin was talking about preventing Russia from taking Ukraine, "but yes, we are also looking to prevent them from expanding their efforts and President Putin's objectives beyond that, too."[28] This position underpinned a sanctions policy targeting G7-produced technology needed for Russia's technology, aerospace, and defense sectors.[29] Expressing similar goals, both the U.K. and the European Union have levied comparable sanctions against Russia.[30] Ukrainian assessments suggest that these policies are beginning to achieve their intended effects.[31]

In sum, for several years after major combat operations cease, Russia will be a nuclear state with substantial cyber capability but likely without significant conventional capability. This capability profile has no precedent in the 21st century international system. When coupled with Russia's post-armed-conflict motivation(s), we are likely to see unprecedented Russian cyber behaviors in the immediate post-armed-conflict period.

ALTERNATIVE CYBER SECURITY FUTURES

James Dubik argues that, after major combat operations cease, Russia will continue to "fight" by other means using, for example, cyber actions to pursue its strategic goals in Ukraine.[32] Such actions would also likely continue against NATO and its member states. Dubik implores Western leaders to avoid the mistake of believing that the conflict with Ukraine, and the larger conflict with NATO and its members, will be over when the fighting stops.[33] Thus, planning should begin now "for the inevitable, post-major combat operations transition period," a view shared by Fix and Kimmage, who argue that the Western strategy must think through "the day after" major combat operations end.[34] But what strategic challenges will "the day after" present to NATO and its members?

No matter the outcome of the kinetic conflict, Russia will still seek to control the security architecture in Europe, fueled by either euphoria or an increased sense of irredentist revanchism. Coupling these motivations with Russia's nuclear-cyber capability profile suggests a novel post-armed-conflict strategic challenge for NATO and its member states. This is recognized in Latvian Minister of Defense Ināra Mūrniece's comment that, despite Russia's major losses in Ukraine, it is a mistake to think that Russia has been weakened by this armed

Russia uses the threat of nuclear retaliation to intimidate NATO. Pictured is an RS-24 Yars MIRV-equipped, thermonuclear armed intercontinental missile. (Credit Vitaly V. Kuzmin, Copyright CC BY-SA 3.0).

conflict and is incapable of new strategic surprises. Consequently, she argues, countries have to prepare for Russia to continue using its hybrid and nuclear threat arsenal to intimidate NATO member states and weaken support to Ukraine.[35]

Regarding Russia's nuclear capabilities, Rumer argues that although Russia's conventional force military stature has been diminished, its actions during the armed conflict have reinforced its reputation as a "dangerous and unpredictable neighbor brandishing nuclear weapons" to achieve its strategic objectives.[36] History has shown, however, that nuclear weapons are not effective instruments of compellence. Thus, absent notable conventional force capabilities, should Russia win the armed conflict, it is unlikely that its nuclear arsenal would successfully support a triumphalism-fueled effort to expand its gains beyond Ukraine.[37] For the same reason, should Russia lose the armed conflict or if it results in stalemate, it is unlikely that Moscow will find that brandishing its nuclear capabilities will successfully support an irredentist revanchist-fueled effort to reclaim Ukraine or other former Soviet territories. However, no matter the outcome of the armed conflict, Russia will continue to lean on its nuclear weapons as a strategic deterrent against any perceived threat of NATO aggression.

What does this portend for how Russia might employ its cyber capabilities?[38] Cyber persistence theory is a structural theory of cyber security arguing that core structural features of cyberspace—interconnectedness, macro-resilience/micro-vulnerability, and mutability—designate conditions of constant contact and offense/defense fluidity to which all cyber actors are subject. The strategic logic for cyber security that flows from these conditions is initiative persistence in setting favorable conditions in and through cyberspace by exploiting others'

vulnerabilities (technical and cognitive) while ensuring they cannot exploit yours. Russia has for many years adopted this cyber strategic logic in pursuit of its European security architecture goals. In the post-armed-conflict environment, absent compellent strategic utility from nuclear weapons and coercive utility from weakened conventional force, it is reasonable to conclude that Russia will employ its cyber capabilities at a scope, scale, and intensity that aligns with its strategic ambitions.

In fact, starting in mid-2022, Russian state-sponsored and state-affiliated cyber actors increased the operational tempo and intensity of cyber campaigns/operations targeting NATO and its member states.[39] Over the first year of armed conflict, cyber phishing activity against NATO and its member states increased 300 percent over pre-armed-conflict levels, with a primary emphasis reportedly on cyber-enabled espionage.[40] Additionally, cyber activities have included distributed denial of service (DDOS) campaigns,[41] information operations,[42] and destructive operations.[43] Whereas Russia's increase in conventional force operations is leading to the attrition of skilled conventional force operators,[44] the opposite is arguably true in and through cyberspace. An increased cyber operational tempo is improving the skills of Russia's cyber operators.

Given Russia's nuclear-cyber capability profile and its post-armed-conflict motivation(s), the strategic logic of cyber persistence theory suggests two alternative cyber futures.[45]

Cyber Security Future #1: Cyber Campaigning Short of Armed-Attack Equivalent Effects

Regardless of the post-armed-conflict outcome, in an effort to keep NATO and its members on their heels, Russia sustains and even increases the current operational tempo and intensity of its cyber campaigns/operations.[46] Given severely degraded conventional force capabilities, Moscow abstains from or significantly limits the number of campaigns/operations that cause armed-attack equivalent effects and focuses on damaging political parties and leaders it dislikes, undermining the internal stability of "anti-Russian" countries, degrading the integrity of the transatlantic alliance, and disrupting the logistics infrastructure of states that support Ukraine's reconstitution. In essence, Russia sustains its ongoing cyber campaigns/operations against NATO and its member states in the current geopolitical condition of armed conflict into a post-conflict condition of competition with the intent of cumulating tactical gains to levels of strategic significance. As cyber persistence theory explains, exploitative cyber campaigning offers an alternative to threats and use of force for maintaining or altering the international distribution of power.

Cyber Security Future #2: Escalating to Cyber Armed-Attack Equivalent Effects

In this alternative future, *in spite of* its severely degraded conventional force capabilities, Russia targets NATO and its members with cyber campaigns/operations that cause armed-attack equivalent effects. Not content with the time it takes to cumulate effects from campaigns short of armed-attack equivalence, Russia escalates its activities in and through cyberspace.

Cyber persistence theory posits that certain destabilizing conditions may encourage states to breach the tacit ceiling of armed-attack equivalent effects and escalate to activities centered on coercion or physical damage/destruction, injury, or loss of life.[47] For example, to arrest a loss of relative power due to cyber strategic competition, a state may make a deliberate decision to threaten use of force or to strike kinetically. A post-armed-conflict, nuclear-armed Russia with significantly degraded conventional force capabilities arguably presents a

novel destabilizing condition and a conundrum for NATO and its member states.

Whereas nuclear weapons as a compellent will not serve Moscow's adventurism, nuclear weapons as a strategic deterrent may encourage Russia to target some NATO member states with cyber campaigns/operations that cause armed-attack equivalent effects to stress test NATO's willingness to invoke Article 5. The absence of significant Russian conventional force capabilities may make NATO cautious in invoking Article 5, because Russia's weakened conventional force effectively removes a buffer (or a medium) in and through which NATO could manage a coercive escalation dynamic before reaching the threshold of nuclear threats, a threshold that Russia has demonstrated an unsettling level of comfort in crossing. Additionally, in a post-armed-conflict geopolitical condition of competition a kinetic response by NATO triggered by cyber-induced armed-attack equivalent effects would be a first for a state or state-level entity and would set a perilous precedent. Alternatively, inaction by NATO (i.e., failure to invoke Article 5) might open a seam in the alliance that Russia could seek to exploit to reconstruct the pre-armed conflict relations it enjoyed with some NATO member states and further push the envelope regarding the threshold of Article 5.[48] Counterintuitively, the West's objective of significantly degrading Russia's conventional force generation functions (defense industrial base) may place the West in an unenviable position when confronting a nuclear-armed, cyber belligerent, post-armed-conflict Russia.

OPTIMIZING NATO'S AGGREGATE CYBER CAPABILITY AND CAPACITY

To prepare for the post-armed-conflict environment, Cordesman argues that NATO today "needs to make a massive effort to rebuild its forces to deter Russia from any further military adventures."[49] Gideon Rose argues that "the fighting must continue until Moscow accepts that it cannot achieve territorial gains by military force."[50] NATO member states should certainly sustain their support for Ukraine and increase their conventional force capabilities, but this article argues that those efforts should be informed as follows: (a) Russia's conventional forces will likely be significantly degraded in the immediate post-armed-conflict environment, (b) the most likely strategic threat to NATO and its member states will be in and through cyberspace, and (c) current (and additional) NATO conventional force capabilities will likely have no deterrent effect on Russia's efforts to destabilize the alliance and its member states via cyber campaigns/operations.[51]

A more strategically salient effort would be to focus on Russia's threat in and through cyberspace. This effort could have two tracks. First, NATO member states with the cyber capability and capacity to do so ought to support any current Ukrainian efforts,[52] or engage in efforts themselves,[53] to target Russia's cyber force generation functions, including but not limited to tools—sets of code used to create, debug, maintain, or otherwise support programs or applications—and Russian domestic cyber infrastructure. Doing so should reduce the likelihood of the potential post-armed-conflict conundrum presented by a vacuum of Russian conventional force capability. Russia will more quickly and successfully reconstitute cyber force generation functions relative to conventional force generation functions,[54] which should encourage capable allied states to engage in such cyber functions persistently.[55] Second, to prepare for the immediate post-armed-conflict environment, the transatlantic alliance ought to begin shifting to a proactive cyber operational posture that leverages the aggregate cyber capabilities and capacities of its member states to mitigate the strategic consequences of a hostile, post-armed-conflict Russia primarily pursuing its strategic goals in and through cyberspace.[56]

The individual decisions of the most cyber-capable NATO member states to support any current Ukrainian efforts, or engage in efforts themselves, to target Russia's cyber force generation functions need not be made with the full backing of all NATO member states, but a NATO shift to a proactive cyber operational posture must. Thus, it is important to consider what this would entail for NATO, how such a posture might be authorized, and how it may be operationalized.

David Van Weel, Assistant Secretary General for Emerging Security Challenges at NATO, recently commented that NATO must take a more proactive approach to achieve security in the strategic competition playing out in and through cyberspace which "is contested at all times."[57] To do so, he argues that NATO and its member states must "foster an entirely new mindset regarding how to operate, compete, and, if necessary, fight in the cyber domain."[58] Indeed, he argues that "being proactive … means being responsible actors."[59] Van Weel highlights three areas of emphasis: NATO "requires a better integration of activities among numerous stakeholders at each of NATO's three cyber defense levels—political, military, and technical;"[60] NATO member states must act coherently with other states and relevant actors, including industry, academia, the private sector, and other international organizations; and NATO and its member states must focus on "getting the basics right and ensuring that defenders have the capabilities to detect, prevent, and mitigate malicious activity."[61]

While Van Weel's priorities are necessary for improving the cyber security of NATO and its member states and supporting preparations "to respond

Locked Shields is the world's largest and most complex international real-time cyber defence exercise, organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Locked Shields 2022 was held from Apr. 19 to 22, 2022 with over 2000 participants from 33 nations (Photo by NATO CCDCOE).

swiftly," they are not sufficient. What is missing is a proactive operational element that supports continuous campaigning "forward" in space and time to preclude, inhibit, or otherwise constrain adversaries' opportunities to realize strategic gains in and through cyberspace.[62] Absent the adoption of a proactive, anticipatory operational element, NATO member states' aggregate cyber capabilities and their employment (or lack thereof) would, at best, support a "response force" that is misaligned with the cyber strategic environment and therefore suboptimal for providing security in and through cyberspace for NATO and its member states.[63]

Although a proactive operational element could, in exigent circumstances, leverage the cyber effects capabilities that have been volunteered by at least nine NATO members to date,[64] its primary focus ought to be leveraging non-exquisite capabilities and capacities that support operating forward to identify, for example, adversary tactics, techniques and procedures, malware, and other adversary signatures and to set favorable security conditions should a crisis or armed conflict erupt. Operating forward would enable the anticipation of adversary operations, preclusion of adversary options, reduction in the number of attack vectors, and denial of cyber terrain. In this context, forward in space may be understood in two ways: as networks, systems, and devices beyond the technical boundaries of NATO's communication and information systems but within the national boundaries of NATO member states, or as networks, systems, and devices beyond those boundaries.[65]

In the first instance, a NATO proactive operational element would support "hunting forward" on a member state's networks, systems, and devices with the permission of that NATO member state. This could take different forms—for example, one alliance member could "hunt" alongside a host nation's cyber defenders, as the United States has done with Albania,[66] Croatia,[67] Estonia,[68] Lithuania,[69] Montenegro,[70] and North Macedonia,[71] and as the United States and Canada have done with Latvia.[72] However, not all member states may be comfortable with this model, so alternatives ought to be considered.[73] For example, after being made aware by the United States that China had compromised its classified defense networks, Japan was wary of the U.S. offer to provide a "hunt forward" team to assist in identifying the breadth and depth of the compromise.[74] A former senior U.S. defense official commented that "They were uncomfortable having another country's military on their networks."[75] Consequently, the United States and Japan arrived at a compromise approach: The Japanese would use domestic commercial firms to assess the severity of the compromise, and a joint U.S. National Security Agency/USCYBERCOM team would review the results and provide guidance on how to mitigate the vulnerabilities.[76]

In the second instance, a cyber team or teams contributed by one or more NATO member states would operate beyond the boundaries of NATO member states.

Fully specifying how NATO could authorize a proactive operational element is beyond the scope of this article, but offering several broad notional frameworks is not. Some have offered a framework where NATO's Intelligence and Security Division would gather intelligence on cyber threats, the Cyberspace Operations Center (CYOC) would outline ways to mitigate those threats, the CYOC would share its analyses with threatened states, and those states would request assistance from allies who have volunteered to support threatened target classes (or countries) by employing their own cyber capabilities against the identified threats.[77] However, this framework excludes important elements likely necessary to support a proactive operational element engaged in continuous campaigning—command and control by Supreme Allied Commander Europe (SACEUR) and a mandate to operate from the North Atlantic Council (NAC).

An alternative is to establish a cyber-focused Memorandum of Understanding (MOU) organization that specifies a framework for allies and partners to coherently, efficiently, and continuously campaign together in and through cyberspace under the command and control of SACEUR and by NAC mandate in competition, militarized crisis, and armed conflict.[78] As such a framework would place some cyber capabilities under the command of SACEUR, it would exceed the requirements of the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism. However, as it enables campaigning in strategic competition short of militarized crisis and armed conflict, it would also exceed the strategic utility of SCEPVA.[79] Additionally, the capabilities required to support a proactive operational element need not be the likely exquisite offensive cyber operations capabilities that member states volunteer through SCEPVA. To prepare for the post-armed-conflict strategic environment(s), member states and partners ought to be more willing to contribute more "mundane" but nonetheless important capabilities that are far less likely to potentially jeopardize their intelligence assets, means, and methods.[80] A model for this organization could be NATO's Allied Special Operations Forces Command under the command of SACEUR and sourced by cyber contributions from member states.

A proactive continuous operation in substance could comprise the tasking contours of the on-going, non-Article 5 Operation Sea Guardian, albeit adapted to the context of cyberspace.[81] For example, a named operation could encompass tasks for cyberspace situational awareness; campaigns/operations to preclude, inhibit, and interdict/disrupt adversary cyber campaigns/operations, and defend and protect NATO and its member states against cyberspace-based malicious activities; identifying, locating, and disrupting the sharing of malware; and protecting critical infrastructure from adversary cyber activities. NATO allies and partners contribute to Operation Sea Guardian through "direct support" by placing assets under NATO operational command and "associated support" with assets that remain under national command. Such an approach would align with the differential cyber capability sets and capacities of member states.

Given that NATO is a defensive alliance, some may argue that a proactive operational element and its associated activities and operations would not align with NATO's purpose. The *raison d'etre* of the alliance, however, is to safeguard the freedom and *security* of all allies, against *all* threats, from all directions.[82] Cyber persistence theory argues that security in and through cyberspace comes through seizing and sustaining the initiative in cyber strategic competition to set favorable conditions (and unfavourable circumstances for adversaries), tempo, and the decision-making cycle of operational action in order to place the adversary at a disadvantage and/or force the adversary to adjust to friendly action. Therefore, to act in alignment with the alliance's stated purpose, to the degree that the alliance has the capacity and capability to do so, it ought to incorporate into its overall cyber strategy an operational element to responsibly seize and sustain the initiative.

GRAND STRATEGY SHIFTS AND TILTS

The most recent national security strategies of the United States and the United Kingdom speak of shifts and tilts to the Indo-Pacific region. Additionally, NATO's *2022 Strategic Concept* has elevated the importance of China.[83] Some have expressed concerns that these leanings ought to be reconsidered in light of the Russian-Ukraine armed conflict.

Cordesman says that U.S. national defense strategy must be "revised" to reflect the fact that U.S. efforts during the Russia-Ukraine armed conflict and its strategy for a post-armed environment "are

just as important as its efforts to strengthen its forces and collective defense efforts in Asia."[84] Similarly, Zakheim argues that many U.S. politicians and policymakers "seem to hope that whatever the outcome of Russia's invasion of Ukraine, the United States will be able to return to its main national security preoccupation—namely, the threat that China poses to American interests in the western Pacific and elsewhere around the globe." Acting on this hope, however, "would constitute a serious strategic error," Zakheim says. "Whether it wins or loses the war with Ukraine, Russia's threat to European stability will not disappear."[85]

Dan Sabbagh suggests that the emphasis on China in the U.K.'s *Integrated Review Refresh 2023* is misguided.[86] He argues that "Further boosting Britain's tiny military presence in the Indo-Pacific is not obviously good value for money for the UK's stretched armed forces—and for now, at least, the primary threat from Beijing to Britain is its ceaseless desire to steal intellectual property, not a military one."[87] Therefore, he proposes that investments in British military capability "ought to be focused on helping Ukraine and frontline Nato (*sic*) states protect themselves."[88]

The frameworks offered in this article for optimizing NATO's aggregate cyber capability and capacity for a post-armed-conflict environment could, in different ways, satisfy those who call for a stark shift to the Indo-Pacific and also those who do not. If one accepts that Russia's primary strategic threat to NATO and its member states in the immediate post-armed-conflict environment originates from cyberspace, the frameworks address that threat, thereby satisfying the concerns of those arguing for elevating the priority of Russia. The frameworks could also placate those who elevate China as the primary threat because, as Brands argues, the West "can inflict severe strategic defeat on it (China) by ensuring that Russia loses its war in Ukraine."[89] Moscow, Brands argues, "weakens the democratic world through cyberattacks and information warfare; it helps Beijing make the global internet friendlier to dictatorial rule. Joint military exercises, defense technological projects, and other aspects of Sino-Russian cooperation fuel China's challenge to U.S. power."[90] Brands's claim ought to be appended to include ensuring that Russia is precluded, inhibited, or otherwise constrained from threatening the West in and through cyberspace in a post-armed-conflict environment.

Optimizing the aggregate capacity and capability of NATO member states through a proactive operational element would provide increased security against cyber campaigns/operations from *both* Russia and China, the latter of which also targets those states in and through cyberspace to spread disinformation and illicitly acquire defense contractors' intellectual property and other sensitive government information.[91] Thus, it would assuage both those who argued that China ought to have been elevated in NATO's strategic concept and those who argued the contrary.

CONCLUSION

No matter the outcome of the Russia-Ukraine armed conflict, Russia will continue to be motivated to control the security architecture of Europe. The West's current objective of attriting Russia's conventional force generation functions could drive Russia to leverage its substantial cyber capability and capacity in the post-armed-conflict environment. This may, counterintuitively, place NATO in a bind should Russia escalate in and through cyberspace to campaigns/operations that cause armed attack equivalent effects. Even if Russia chooses to stay short of such effects, the trend of Russia's current cyber operational tempo, including groups affiliated with Russia, suggests that NATO and its member states will be subject to a significant, perhaps unprecedented, sustained volume of cyber intrusions in a post-armed-conflict environment.

A Russia-backed armed rebel observing fighting positions though firing port at his position in ruins of International Donetsk Airport (Photo by Mstyslav Chernov, 12 June 2015, Wikimedia Commons).

It would be prudent for NATO and its member states to consider preparing now for these potential futures. Member states ought to support current Ukrainian efforts or engage in their own efforts to target Russia's cyber force generation functions, and NATO should adopt policies that optimize member states' aggregate cyber capability and capacity—policies that center on a proactive operational posture inclusive of an operational element that can preclude, inhibit, or otherwise constrain Russian (and Chinese) cyber efforts in a post-armed-conflict environment. Both of these efforts would satisfy the security concerns of those in the West who prioritize Russia over China and of those who hold opposing views. PRISM

Notes

[1] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining Security in Cyberspace* (Oxford: Oxford University Press, 2022). Outside the intellectual framework of cyber persistence theory numerous additional alternative futures could conceivably be posited.

[2] See, for example, The White House, 2022 National Security Strategy, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; H.M. Government, *Global Britain in a Competitive Age: The Integrated Review of Security, Defense, Development and Foreign Policy*, March 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy; H.M. Government, *Integrated Review Refresh 2023*, March 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1145586/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf; and *NATO 2022 Strategic Concept*, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. For a comprehensive review of all European countries, see Bernhard Bartsch and Claudia Wessling, eds., *From a China Strategy to No Strategy at All: Exploring the Diversity of European Approaches* (European Think-tank Network on China, July 2023), https://www.clingendael.org/sites/default/files/2023-07/ETNC_Report_2023_final_0.pdf.

[3] Hal Brands, "Opposing China Means Defeating Russia," *Foreign Policy*, April 5, 2022, https://foreignpolicy.com/2022/04/05/china-russia-war-ukraine/.

[4] Eugene Rumer, "Putin's War Against Ukraine: The End of The Beginning," *Carnegie Endowment for International Peace*, February 17, 2023, https://carnegieendowment.org/2023/02/17/putin-s-war-against-ukraine-end-of-beginning-pub-89071.

[5] Michael Miklaucic, "Taking War Seriously," *RealClear Defense*, May 31, 2023, https://www.realcleardefense.com/articles/2023/05/31/taking_war_seriously_902610.html.

[6] Eliot A. Cohen, "It's Not Enough for Ukraine to Win. Russia Has to Lose," *The Atlantic*, May 19, 2023, https://www.theatlantic.com/ideas/archive/2023/05/ukraine-victory-russia-defeat/674112/.

[7] Anthony H. Cordesman, "How? (and Does?) the War in Ukraine End: The Need for a Grand Strategy," *Center for Strategic and International Studies*, February 24, 2023, https://www.csis.org/analysis/how-and-does-war-ukraine-end-need-grand-strategy.

[8] Dov S. Zakheim, "Russia Will Remain a Threat, No Matter How the War in Ukraine Ends," *The Hill*, February 17, 2023, https://thehill.com/opinion/international/3862054-russia-will-remain-a-threat-no-matter-how-the-war-in-ukraine-ends/.

[9] Liana Fix and Michael Kimmage, "What if Ukraine Wins? Victory in the War Would Not End the Conflict with Russia," *Foreign Affairs*, June 6, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-06-06/what-if-ukraine-wins. They also suggest that, over time, a "winning small" victory could be expanded by Ukrainian forces breaking up the land bridge that Russia has established to Crimea and regaining the territory in southeastern Ukraine that Russia seized and annexed back in 2014. They also describe a "winning big" victory that includes these same objectives but in a more compressed timeline.

[10] Justin Bronk (Royal United Services Institute) quoted in Barry Rosenberg, "3-to-5 years from now is the danger time when the US could face both China and Russia," *Breaking Defense*, July 20, 2023, https://breakingdefense.com/2023/07/three-to-five-years-from-now-is-the-danger-time-when-the-us-could-face-both-china-and-russia/.

[11] Fix and Kimmage. "What If Ukraine Wins?"

[12] Ibid.

[13] Zakheim, "Russia Will Remain a Threat."

[14] Cohen, "It's Not Enough for Ukraine to Win. Russia Has to Lose."

[15] Rudolf G. Adam, "Beyond Russia's War Against Ukraine," *GIS*, February 13, 2023, https://www.gisreportsonline.com/r/ukraine-russia-stalemate/.

[16] See Rumer, "Putin's War Against Ukraine," and Cordesman, "How? (and Does?) the War in Ukraine End."

[17] Joshua C. Huminski, "Victory in Ukraine Could Mean a Stalemate," *The Hill*, June 28, 2022, https://thehill.com/opinion/international/3539481-victory-in-ukraine-could-mean-a-stalemate/.

[18] Keir Giles, "Russian Defeat Is More Dangerous than Russian Victory," in *How to End Russia's War on Ukraine* (London: Chatham House, June 2023), 26–28, https://www.chathamhouse.org/2023/06/how-end-russias-war-ukraine.

[19] For example, in April 2022, the U.S. Federal Bureau of Investigation disrupted communication between all U.S. systems infected with Russia's CYCLOPSBLINK malware and the malware's command control infrastructure, and a U.S. Cyber Command (USCYBERCOM) "hunt forward" team deployed in Ukraine reportedly discovered and made inert malware targeting the Ukrainian railway system. See, respectively, U.S. Department of Justice, "Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)," April 6, 2022, https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation; Mehul Srivastava, Madhumita Murgia, ND Hannah Murphy, "The Secret U.S. Mission to Bolster Ukraine's Cyber Defences Ahead of Russia's Invasion," *Financial Times*, March 9, 2022, https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471, and Alexander Martin, "U.S. Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command," *Sky News*, June 1, 2022, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139.

[20] Cordesman, "How? (and Does?) the War in Ukraine End."

[21] Zakheim, "Russia Will Remain a Threat."

[22] Quoted in Sophia Sleigh, "It Will Take Years For Russia To Rebuild 'Severely Weakened' Forces, Britain Says," *HuffPost*, September 9, 2022, https://www.huffingtonpost.co.uk/amp/entry/it-will-take-years-for-russia-to-rebuild-severely-weakened-forces-british-officials-say_uk_63201cf6e4b027aa405ebdcf/.

[23] Ibid.

[24] Ibid. Additionally, Estonian military intelligence argues that if the armed conflict were to stop now (September 2023), Russia would need three to five years to restore its conventional capabilities. Holger Roonemaa and Eero Epner, "How Estonia's Military Intelligence Secretly Helped Ukraine," *VSquare*, September 15, 2023, https://vsquare.org/how-estonias-military-intelligence-secretly-helped-ukraine/."

[25] See, respectively, Kiur Kaasik, "How Estonia's Military Intelligence Secretly Helped Ukraine"; Christian Molling and Torben Schutz, *Preventing the Next War: Germany and NATO Are in a Race Against Time* (German Council on Foreign Relations, November 2023), https://dgap.org/system/files/article_pdfs/34-DGAP-Policy-Brief-2023_0.pdf; and Anna Mulrine Grobe, "Amid Slog of Ukraine War, NATO Turns Warier Eye on Russia," *The Christian Science Monitor*, November 16, 2023, https://www.csmonitor.com/USA/Military/2023/1116/Amid-slog-of-Ukraine-war-NATO-turns-warier-eye-on-Russia.

[26] Quoted in Olivier Knox and Caroline Anders, "The U.S. Has a Big New Goal in Ukraine: Weaken Russia," *Washington Post*, April 26, 2022, https://www.washingtonpost.com/politics/2022/04/26/us-has-big-new-goal-ukraine-weaken-russia/.

[27] Russia claims that its factories are producing military equipment nonstop. *The Moscow Times*, "Russian Defense Chief Says Military Factories Working 'Around the Clock,'" January 2, 2023, https://www.themoscowtimes.com/2023/01/02/russian-gas-exports-outside-ex-soviet-states-fell-455-in-2022-a79863.

[28] Quoted in Knox and Anders, "The U.S. Has a Big New Goal in Ukraine."

[29] U.S. Department of the Treasury, "Treasury Sanctions Impede Russian Access to Battlefield Supplies and Target Revenue Generators," July 20, 2023, https://home.treasury.gov/news/press-releases/jy1636. The G7 comprises Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States.

[30] See Foreign, Commonwealth and Development Office, "UK Sanctions Relating to Russia," June 30, 2023, https://www.gov.uk/government/collections/uk-sanctions-on-russia; Foreign, Commonwealth and Development Office, "Webinar: UK Sanctions Relating to Russia: Briefing by UK Government, 21 September 2022," https://www.youtube.com/watch?v=0Mb5ZL-FE9EY; and European Council and Council of the European Union, "EU Response to Russia's Invasion of Ukraine," https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/.

[31] For example, in a recent interview, Andrii Yusov, representative of the Ministry of Education and Culture, noted that "(o)pportunities for deep modernization of the production of new weapons have significantly decreased due to the introduction of sanctions. In fact, the Russians have serious problems with modern optics, electronics, chips and circuits. And today there is no unequivocal source that would enable them to solve these problems." Quoted in Angelina Strashkulych, Russia Refuses to Hand Over Many Ukrainian Prisoners of War without Any Explanation," UKRINFORM, 6 September 2023, https://www.ukrinform.ua/rubric-ato/3757717-andrij-usov-predstavnik-gur-mou.html.

[32] James M. Dubik, "The War in Ukraine Won't End When the Fighting Is Over," *The Hill*, March 9, 2023, https://thehill.com/opinion/national-security/3890975-the-war-in-ukraine-wont-end-when-the-fighting-is-over/.

[33] Ibid.

[34] Ibid and Fix and Kimmage. "What If Ukraine Wins?"

[35] "Latvian Minister: It's Wrong to Think Russia Is Weakened by War with Ukraine," *Baltic News Network*, May 23, 2023, https://bnn-news.com/latvian-minister-its-wrong-to-think-russia-is-weakened-by-war-with-ukraine-245962.

[36] Rumer, "Putin's War Against Ukraine."

[37] See Todd S. Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (New York: Cambridge University Press, 2017), and Todd S. Sechser and Matthew Fuhrman, "Crisis Bargaining and Nuclear Blackmail," *International Organization* 67, no. 1 (Winter 2013): 173-195, 179, https://www.jstor.org/stable/43282156.

[38] These may be employed independently or as part of a "hybrid threat" capability package.

[39] Gareth Corfield, "Putin's Cyber Shock Troops Turn Their Sights on NATO," *Telegraph*, April 9, 2023, https://www.telegraph.co.uk/technology/2023/04/09/russia-cyber-attack-troops-target-nato/.

[40] See Google Threat Analysis Group, "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape," Google, February 2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf. That these operations were reportedly primarily for espionage should not put policymakers at ease. As Microsoft notes, "For the past year, threat actors with known or suspected ties to the GRU, FSB, and SVR have targeted and potentially gained footholds in government, policy, or critical infrastructure sectors throughout the Americas, Europe, and elsewhere. Although most of the operations are probably espionage-focused, the GRU actors have already shown a willingness to use destructive tools outside Ukraine if instructed." Microsoft Threat Intelligence, "A Year of Russian Hybrid Warfare in Ukraine," Microsoft, March 15, 2023, https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf.

[41] See EU-CERT, *Russia's War on Ukraine: One Year of Cyber Operations*, 5, https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf; Tom Hegel and Aleksandar Milenkoski, "NoName057(16) – The Pro-Russian Hacktivist Group Targeting NATO," Sentinel Labs, January 12, 2023, https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/; Mandiant Intelligence, "KillNet Showcases New Capabilities While Repeating Older Tactics," Mandiant, July 20, 2023, https://www.mandiant.com/resources/blog/killnet-new-capabilities-older-tactics; "Unraveling Russian Multi-Sector DDoS Attacks Across Spain," Radware, August 2, 2023, https://www.radware.com/security/threat-advisories-and-attack-reports/unraveling-russian-multi-sector-ddos-attacks-across-spain/?utm_source=substack&utm_medium=email; Daryna Antoniuk, "Pro-Russian Hackers Claim Attacks on Italian Banks," *The Record*, August 2, 2023, https://therecord.media/russian-hackers-claim-attacks-on-italy; and "Dutch Organizations Targeted by DDoS Attacks," Nationaal Cyber Security Centrum, August 8, 2023, https://www.ncsc.nl/actueel/nieuws/2023/augustus/8/nederlandse-organisaties-doelwit-van-ddos-aanvallen?utm_source=substack&utm_medium=email.

[42] "Sweden Says It's Target of Russia-backed Disinformation Over NATO, Koran Burnings," *Reuters*, July 26, 2023, https://www.reuters.com/world/europe/sweden-says-its-target-russia-backed-disinformation-over-nato-koran-burnings-2023-07-26/.

[43] See Tim Starks and Aaron Schaffer, "Russian Sandworm Hackers Deployed Malware in Ukraine and Poland," *The Washington Post*, November 11, 2022, https://www.washingtonpost.com/politics/2022/11/11/russian-sandworm-hackers-deployed-malware-ukraine-poland/; and Dan Goodin, "Mystery Solved in Destructive Attack that Knocked Out >10k Viasat Modems," *ars TECHNICA*, March 31, 2022, https://arstechnica.com/information-technology/2022/03/mystery-solved-in-destructive-attack-that-knocked-out-10k-viasat-modems/.

[44] "Secretary of Defense Lloyd J. Austin III and Joint Chiefs of Staff Chairman General Mark A. Milley Hold Press Conference Following Virtual Ukraine Defense Contact Group Meeting," U.S. Department of Defense, July 18, 2023, https://www.defense.gov/News/Transcripts/Transcript/Article/3462659/secretary-of-defense-lloyd-j-austin-iii-and-joint-chiefs-of-staff-chairman-gene/.

[45] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*.

[46] This view is shared by David Van Weel, Assistant Secretary General for Emerging Security Challenges at NATO, who recently stated "Russia has made ample use of cyber capabilities before invading Ukraine, during hostilities, and it will likely continue using them after the kinetic phase of this conflict." Quoted in Alexander Martin, "NATO: Military cyber defenders need to be present on networks during peacetime," *The Record*, June 5, 2023, https://therecord.media/nato-peacetime-cyberdefense-david-van-weel-cycon?utm_medium=email&_hsmi=261219959&_hsenc=p2ANqtz-9U-ST14DVdNDbXkohb-6Zz_4QR_R-gHLXSBqk7OpsYOgjUBhRUn8wU51FneD-5bx9XbNEetmxCu4XpZLmlGOLW755CyR2Q&utm_content=261221009&utm_source=hs_email.

[47] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*, chapter 5.

[48] Bronk argues that all Russia needs to do to "break NATO" is to show that Article 5 "is a bluff." See Bronk quoted in Barry Rosenberg, "3-to-5 years from now is the danger time when the US could face both China and Russia."

[49] Cordesman, "How? (and Does?) the War in Ukraine End."

[50] Gideon Rose, "Ukraine's Winnable War," *Foreign Affairs*, June 13, 2023, https://www.foreignaffairs.com/ukraine/ukraines-winnable-war.

[51] States are gradually coming to accept that conventional force capabilities do not serve as effective deterrents for opponent's cyber exploitative campaigns short of armed-attack equivalence. To wit, the U.S. Department of Defense argues that "(c)ompetitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure." See U.S. Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. Further, the same holds for cyber capabilities. The United Kingdom and the United States have commented, respectively, that "evidence is limited for cyber operations being a primary contributor to deterrence" and "(t)he Department's experiences have shown that cyber capabilities held in reserve or employed in isolation render little deterrent effect on their own." See U.S. Department of Defense, *Summary: 2023 Cyber Strategy of the Department of Defense*, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF; National Cyber Force, *The National Cyber Force: Responsible Cyber Power in Practice*, March 2023, 10, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf.

[52] Joe Tidy, "Meet the Hacker Armies on Ukraine's Cyber Front Line," *BBC News*, April 15, 2022, https://www.bbc.com/news/technology-65250356.

[53] In response to comments by USCYBERCOM's General Paul Nakasone that the U.S. has conducted a series of operations across the full spectrum of offensive, defensive, (and) information operations in support of Ukraine, White House press secretary Karine Jean-Pierre was asked whether the offensive cyber operations were contrary to the U.S. position of avoiding direct engagement with Russia. Jean-Pierre responded, "We don't see it as such. We have talked about this before. We've had our cyber experts here at the podium lay out what our plan is. That has not changed. So the answer is, just simply, no." Quoted in Martin, "U.S. Military Hackers Conducting Offensive Operations in Support of Ukraine, Says Head of Cyber Command."

[54] Russia could, for example, appropriate the infrastructure of some of the many Russian state-sponsored or state-affiliated cyber threat groups.

[55] Evidence shows that when cyber force generation functions are targeted, they can be reconstituted relatively rapidly. The technology-centered economic sanctions on Russia may slow this reconstitution effort somewhat, but not preclude it.

[56] By 2018, 23 NATO member states had active-duty military organizations possessing capability and authority to conduct cyberspace operations. However, establishing a cyber command should not be equated with creating a robust military cyber capability needed to support a proactive operational posture, which may be considered as "the ability to effectively execute and sustain a range of cyber operations that serve tactical or strategic purposes." In this light, only a handful of NATO member states are capable of sustaining a proactive cyber operational posture. See Max Smeets, "The challenges of military adaptation to the cyber domain: a case study of the Netherlands," *Small Wars & Insurgencies* (2023): 1–20, https://doi.org/10.1080/09592318.2023.2233159.

[57] David Van Weel, "A Proactive Approach to the Cyber Domain Strengthens NATO's Deterrence and Defense Posture," *Digital Front Lines*, July 13, 2023, https://digitalfrontlines.io/2023/07/13/proactive-approach-to-the-cyber-domain/.

[58] Van Weel, "A Proactive Approach to the Cyber Domain Strengthens NATO's Deterrence and Defense Posture."

[59] A similar position is taken by the United Kingdom in *The National Cyber Force: Responsible Cyber Power in Practice* (March 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf.

[60] Van Weel, "A Proactive Approach to the Cyber Domain Strengthens NATO's Deterrence and Defense Posture."

[61] Van Weel, "A Proactive Approach to the Cyber Domain Strengthens NATO's Deterrence and Defense Posture."

[62] In this light it is instructive to consider recent remarks by a deputy minister in Ukraine's Ministry of Digital Transformation. Before Russia's invasion Ukraine had arguably made significant progress in integrating the political, military, and technical aspects of cyber security. And yet the deputy minister argued that "our big mistake" was failing to "create a dedicated cyber force … who not only responded to attacks, but also worked to prevent them." Dina Temple-Raston, Sean Powers, and Daryna Antoniuk, "Exclusive: Ukraine Says Joint Mission with US Derailed Moscow's Cyberattacks," *The Record*, October 18, 2023, https://therecord.media/ukraine-hunt-forward-teams-us-cyber-command.

[63] General Paul Nakasone, Commander, USCYBERCOM, has stated, "If we are only defending in 'blue space,' we have failed." Thus, "(s)hifting from a response outlook to a persistence force that defends forward moves our cyber capabilities out of their virtual garrisons, adopting a posture that matches the cyberspace operational environment." Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2012): 10–14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf. Quotes appear on pages 12 and 13, respectively.

[64] Shannon Vavra, "NATO Cyber-Operations Center Will Be Leaning on Its Members for Offensive Hacks," *Cyberscoop*, August 30, 2019, https://cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/.

[65] Forward in time refers to the notion that operations and activities support an anticipatory posture.

[66] Cyber National Mission Force Public Affairs, "'Committed Partners in Cyberspace': Following Cyberattack, U.S. Conducts First Defensive Hunt Operation in Albania," March 23, 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/.

[67] Cyber National Mission Force Public Affairs and United States European Command, "Partnership in Action: Croatian, U.S. Cyber Defenders Hunting for Malicious Actors," August 19, 2022, https://www.eucom.mil/article/42191/partnership-in-action-croatian-us-cyber-defenders-hunting-for-malicious-actors.

[68] U.S. Cyber Command, "Estonia, U.S. Conduct Joint Defensive Cyber Operation," December 3, 2020, https://www.defense.gov/News/News-Stories/Article/Article/2434474/estonia-us-conduct-joint-defensive-cyber-operation/.

[69] See Cyber National Mission Force Public Affairs, "U.S. Conducts First Hunt Forward Operation in Lithuania," U.S. Cyber Command, August 25, 2023, https://www.cybercom.mil/Media/News/Article/3505610/us-conducts-first-hunt-forward-operation-in-lithuania/; "'Building Resilience': U.S. Returns from Second Defensive Hunt Operation in Lithuania," U.S. Cyber Command, September 12, 2023, https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/#:~:text=FORT%20GEORGE%20G.,the%20country%20in%20May%202022.

[70] "US, Montenegro Work Together to Defend against Malicious Cyber Actors," *DoD News*, October 30, 2019, https://www.cybercom.mil/Media/News/News-Display/Article/2002939/us-montenegro-work-together-to-defend-against-malicious-cyber-actors/.

[71] US European Command Public Affairs, "U.S. and Macedonia Participate in Cyber Defense Cooperation," October 12, 2018, https://www.cybercom.mil/Media/News/Article/1660069/us-and-macedonia-participate-in-cyber-defense-cooperation/.

[72] Cyber National Mission Force Public Affairs, "'Shared Threats, Shared Understanding': U.S., Canada and Latvia Conclude Defensive Hunt Operations," May 10, 2023, https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/.

[73] Elise Vincent, "France's Cyber Defense Force Questions Role of U.S. Support in Europe," *Le Monde*, January 15, 2023, https://www.lemonde.fr/en/international/article/2023/01/15/france-s-cyber-defense-force-questions-the-role-of-us-support-in-europe_6011684_4.html.

[74] Ellen Nakashima, "China Hacked Japan's Sensitive Defense Networks, Officials Say," *The Washington Post*, August 8, 2023, https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/.

[75] Ellen Nakashima, "China Hacked Japan's Sensitive Defense Networks, (quoted).

[76] Ellen Nakashima, "China Hacked Japan's Sensitive Defense Networks.

[77] See, for example, Franklin D. Kramer, Lauren Speranza, and Conor Rodihan, "NATO Needs Continuous Responses in Cyberspace," *New Atlanticist*, December 9, 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

[78] A full listing of NATO Partners can be found at https://www.nato.int/cps/en/natohq/51288.htm.

[79] It is presumed that the SCEPVA mechanism holds relevance for only militarized crisis and armed conflict.

[80] Mikkel Storm Jensen, "Five Good Reasons for NATO's Pragmatic Approach to Offensive Cyberspace Operations," *Defence Studies* 22, no. 3 (May 2022): 467, https://doi.org/10.1080/14702436.2022.2080661.

[81] For a description of Operation Sea Guardian, which has been on-going since 2016, see North Atlantic Treaty Organization, "Operation Sea Guardian," May 26, 2023, https://www.nato.int/cps/en/natohq/topics_136233.htm, and Allied Maritime Command, "OPERATION SEA GUARDIAN," https://mc.nato.int/missions/operation-sea-guardian.

[82] "Deterrence and Defence," North Atlantic Treaty Organization, July 19, 2023, https://www.nato.int/cps/en/natohq/topics_133127.htm#:~:text=NATO%20is%20a%20defensive%20alliance,one%20of%20NATO's%20core%20tasks.

[83] See *NATO 2022 Strategic Concept*, 5.

[84] Cordesman, "How? (and Does?) the War in Ukraine End."

[85] Zakheim, "Russia Will Remain a Threat, No Matter How the War in Ukraine Ends."

[86] It has been argued that this emphasis is unlikely to abate should Labour defeat the Conservatives in the next general election expected in 2024. Peter Chalk, "The United Kingdom's Indo-Pacific Engagement," *War on the Rocks*, November 30, 2023, https://warontherocks.com/2023/11/the-united-kingdoms-indo-pacific-engagement/.

[87] Dan Sabbagh, "Sunak's Focus May Be on China, but It's Europe's Security That Is Vital for the UK," *The Guardian*, March 12, 2023, https://www.theguardian.com/politics/2023/mar/12/sunaks-focus-may-be-on-china-but-its-europes-security-that-is-vital-for-the-uk.

[88] Sabbagh, "Sunak's Focus May Be on China, but It's Europe's Security That Is Vital for the UK."

[89] Hal Brands, "Opposing China Means Defeating Russia."

[90] Brands, "Opposing China Means Defeating Russia."

[91] See Laurens Cerulus, "Von der Leyen Calls Out China for Hitting Hospitals with Cyberattacks," *Politico*, June 22, 2020, https://www.politico.eu/article/eu-calls-out-china-for-hitting-hospitals-with-cyberattacks/; Gordon Corera, "China Accused of Cyber-attack on Microsoft Exchange Servers," *BBC News*, July 19, 2021, https://www.bbc.com/news/world-asia-china-57889981; and Jonathon Greig, "Multiple Chinese APTs Are Attacking European Targets, EU Cyber Agency Warns," *The Record*, February 17, 2023, https://therecord.media/multiple-chinese-apts-are-attacking-european-targets-eu-cyber-agency-warns.

Strategic Political Sabotage and How to Tackle It

By Elisabeth Braw and Richard Newton

In January 2023 activist Rasmus Paludan, who leads a tiny, far-right, anti-Islamic party in Denmark, set out to intentionally offend Turkish president Recep Tayyip Erdogan. While some might characterize what Paludan did as acceptable civil disobedience, and Paludan may have acted out of opportunism, seeing in the debate an opportunity to get considerable attention, its effect was that of an act of strategic political sabotage intended to disrupt Sweden's efforts to join the North Atlantic Treaty Organization (NATO) alliance. The difference between strategic political sabotage and civil disobedience is important because it guides how liberal democracies may tackle the challenges of legal protest.

The assassination of the Archduke Franz Ferdinand in June 1914 was an act of political sabotage that ignited World War One. Source: Smithsonian Magazine (public domain)

Paludan's first act was to burn a copy of the Qur'an in front of Turkey's embassy in Stockholm. A week later he burned another Qur'an in front of a mosque in Denmark. The governments of Sweden and Denmark firmly denounced the burnings but noted such acts are protected

Ms. Elizabeth Braw is a Visiting Fellow at the Atlantic Council and a columnist for *Foreign Policy* and *Politico Europe*. She is the author of *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression*. **Richard Newton (PhD)** serves as Adjunct Faculty at the University of Alaska Fairbanks and is a Fellow at the Homeland Defense Institute, a security studies collaboration between the U.S. Air Force Academy and U.S. Northern Command.

under their countries' respective freedom-of-expression laws,[1] and in addition, neither nation possesses anti-blasphemy laws. Erdogan, facing a tough reelection campaign, reacted by increasing his public opposition to Sweden's bid for NATO membership. Paludan's small and legal intentional act of political theater severely harmed Sweden's otherwise straightforward accession to NATO. The same was true for subsequent Qur'an burnings by Salwan Momika, an Iraqi refugee living in Stockholm who previously served with the Iranian-sponsored Imam Ali Brigade.[2] It was only in July 2023, after NATO, the European Union, and the United States agreed to military and economic concessions unrelated to the desecration of Islam's holy text, that President Erdogan agreed to forward Sweden's NATO accession to the Turkish parliament for ratification.[3] In October, Erdogan did submit a bill to the Turkish parliament to ratify Sweden's accession, but by year's end it remained there, still a hostage to real and imagined provocations of Turkey.[4] Hungary, too, had failed to ratify Sweden's NATO accession, ostensibly because of anti-Hungarian posturing by Swedish opposition politicians and the educational sibling of Swedish National Radio.[5]

Together, these events meant that a crucial Swedish foreign-policy initiative had been sabotaged by what seemed to be an innocent combination of thin-skinned foreign leaders and domestic saboteurs (whether acting consciously or unwittingly) who had exercised their right to free speech.

Indeed, citizen participation in or fueling of such a concoction offers a promising recipe for an adversary, whether state or non-state, seeking to undermine liberal democracies through non-military means. The likelihood of malicious external meddling makes it imperative that liberal democracies be prepared and have appropriate processes and programs in place and ready to mitigate the effects of political sabotage.

The term sabotage is defined by the *Cambridge Dictionary* as a deliberate attempt to obstruct, disrupt, or destroy an opponent's equipment, facilities, policies, or actions. The term can be applied to any number of domains; for example, economic sabotage, where workers deliberately slow production, make mistakes during assembly, or damage equipment; military sabotage that destroys infrastructure critical to the war effort; and environmental sabotage, such as cutting mile-long driftnets that trap protected fish species or spiking trees to prevent deforestation. But there is also strategic *political* sabotage—sabotage by individuals or a minority group that deliberately acts to disrupt, undermine, or manipulate the political process for strategic political or ideological gains. While such activities often include unethical, if not illegal, behaviors, their perpetrators typically portray themselves as dissidents performing acts of civil disobedience to justify their actions as acceptable and legitimate, even if inconvenient and disagreeable, forms of political expression. The strategic political saboteur's objective is to obstruct or disrupt political decisions by generating enough opposition to force policymakers to reverse policy decisions. In a globalized world, with ubiquitous and near-instantaneous communications, the dilemma is that what may be legitimate and protected rights of protest in one culture might cause outsized damage to that country's relations with other nations. Countries hostile to liberal democracies, meanwhile, exploit their adversaries' democratic freedoms to fuel such sabotage and help undermine foreign policy decisions they consider detrimental to them.

It is helpful to acknowledge the similarities between strategic political sabotage and civil disobedience, while explaining why one is not the other, especially when politically motivated dissent—such as Paludan's and Momika's—seeks to blur the lines between the two. One of the most important differences is that political sabotage is generally externally

Danish anti-Islam politician Rasmus Paludan burning a quran at a rally in Nørrebro under heavy police protection. Photo by FunkMonk, September 2, 2019 (Wikimedia Commons).

focused, seeking to influence another nation's leadership from afar. Political saboteurs such as Paludan use their legal rights of free expression, often intentionally offensive to the "target audience," hoping to bring adversary perspectives to the fore of public and governmental consciousness. Civil disobedience, on the other hand, is internally focused, and perpetrators intentionally and publicly break domestic laws they deem immoral. Those engaging in civil disobedience do not impinge on other citizens' rights but merely conduct their acts of disobedience to attract attention to their causes. Most important, they accept the judicial consequences of their actions.[6] While Paludan and Momika styled themselves as civil disobedients, their acts were directed against Islamic regimes but conducted in Sweden and Denmark, where Islamic governments in the Middle East and South Asia were unable to prosecute them. Were they true civil disobedients, they would have publicly burned the Qur'ans in Istanbul, Tehran, or Baghdad and accepted the judicial consequences their actions.

Admittedly, there is overlap between political sabotage and civil disobedience, if for no other reason than well-meaning citizens confuse the two. This confusion can create an exploitable opportunity for hostile adversaries and their strategic sabotage, which, in the case of Sweden's bid to join NATO, Russia is known to have planned and supported. In December, Finnish National Broadcasting (YLE) reported that Finland's intelligence service knew of Russian plans to undermine Sweden's NATO accession by fueling disinformation campaigns disguised as legitimate protest.[7]

HISTORICAL ANTECEDENTS

Political sabotage is not new. Long before social media made it possible for anyone with a smartphone and an internet connection to offer their opinions and recommendations to a global audience,

journalists, photographers, actors, and authors were powerful influencers. The assassination of Archduke Franz Ferdinand by Gavrilo Princip in Sarajevo in June 1914 may well be one of the most ill-conceived and consequently disastrous episodes of strategic political sabotage of the 20th century.[8] During his trial, Princip characterized what he did as civil disobedience to make the case for an independent Serbia, when in fact it was an illegal and unethical action intended to disrupt Austrian-Hungarian political processes for both political and ideological gains.[9] Ironically, it resulted in a war that claimed the lives of some eight million soldiers and thirteen million civilians and brought about the fall of four great empires: Germany, Russia, Austria-Hungary, and the Ottoman Empire. The First World War also claimed the lives of over 1.2 million Serbs, the highest per capita number of casualties of any nation involved.[10]

The Qur'an desecrations and burnings by Paludan and Momika are clearly not as serious as an assassination. Paludan, though, managed to enrage Erdogan, and Momika's desecrations resulted in Sweden being condemned by the Organisation of Islamic Cooperation (OIC), the Swedish embassy in Baghdad being attacked by a mob, and violent protests unfolding in Muslim-majority Swedish neighborhoods. This prompted Erdogan to declare that Sweden's NATO accession hinged on "security in the streets of Sweden."[11] In July 2023, far-right activists in Denmark followed Swedish protesters' example and burned Qur'ans in two separate incidents, resulting in Denmark also being condemned by the OIC.

In September 2023, Hungary—beside Turkey the only country yet to ratify Sweden's NATO accession—seemed to follow Turkey's path and suspended ratification of Sweden's NATO membership on the basis of what it considered hostile manifestations in Swedish civil society. Hungarian Foreign Minister Péter Szijjártó scolded his Swedish counterpart, Tobias Billström, in a letter that was also published on Twitter by the Hungarian government.[12] Swedish politicians, complained Szijjártó, had engaged in "biased, unfair, and unjust accusations" toward Hungary, adding that now that parliamentarians "have read in the news that as part of your school curriculum provided by UR (the educational sibling of Swedish Public Radio) belonging to a state-run foundation, serious accusations and fake informations [sic] are being spread in the schools of Sweden, suggesting that democracy has been on a backslide in Hungary in the recent years." Szijjártó, though, failed to mention that opposition politicians within the Swedish Parliament had indeed been smearing Sweden's Prime Minister, Ulf Kristersson, but that this was part of a domestic dispute where the opposition compared Kristersson with Hungary's Prime Minister Viktor Orban. The educational sibling of Swedish national radio had, for its part, included negative references to the state of Hungary's democracy in its school content. Even though the Swedish government clearly was not in a position to ban such expressions, Szijjártó admonished Billström, saying the negative characterizations don't "help your continuously raised demand [for NATO accession] to be fulfilled."

When domestic provocations are intended to harm foreign policy and impugn another nation's laws, culture, or ideology, they become acts of political sabotage, even when covered by citizens' rights to free expression. When they are conducted, wittingly or not, to further an adversary's objectives, they enter the realm of gray-zone aggression. Let's consider Paludan's January 2023 Qur'an burning. The protest permit was paid for by Swedish far-right journalist, Chang Frick, who in the past has contributed to the Russian media network *RT*.[13] There was nothing illegal under Swedish law about Frick paying for the permit and Frick himself says he did so to support Kurds living in Sweden.[14] Still, given Russia's tradition of manipulating legal protests so

as to destabilize other countries' governments, the Russian connection to Paludan's protests raised questions as to the extent of Russian involvement.[15]

Another case of strategic political sabotage intended for disproportionate effect was National Security Agency contractor Edward Snowden's leak of highly classified documents to major newspapers. Snowden argued that what he did was an act of conscience because his personal concerns over domestic surveillance programs were ignored by the agency's leadership. Yet Snowden breaking the law was not civil disobedience, because he damaged the United States' credibility and standing among its allies and partners, harmed private individuals whose private information was leaked, and escaped the judicial consequences of his actions by seeking asylum in Russia.[16] Regardless of whether one considers Snowden a heroic whistleblower or a traitor, the consequences of his actions harmed the United States and aided Russia, where he was subsequently granted citizenship.[17]

STRATEGIC SABOTAGE AS GRAY-ZONE AGGRESSION

In liberal democracies, strategic sabotage is bound to happen. The freedoms citizens enjoy are undeniably a strategic vulnerability, but at the same time they are also a strength. The rights of expression, dissent, and peaceful protest ensure governments remain, as President Abraham Lincoln said at Gettysburg, of the people, by the people, and for the people. The exercise of those freedoms, though, means citizens can and will do things that harm the political order, both at home and abroad. At the extreme ends of the political spectrum, there will always be those who are quite happy to harm society in the name of their causes and protesters who willingly accept the consequences of their actions. Such positions make it rather easy for hostile regimes to exploit well-meaning, but loyal, dissidents and legitimate opposition groups through gray-zone aggression, usually malign, non-kinetic activities that seek to undermine the rules-based order without crossing a threshold that leads to open conflict. What is hard to detect, harder to attribute, and extremely difficult to respond to is outsider manipulation of legal protest. Hostile powers that support, influence, or control domestic dissent intentionally hide their involvement. Authoritarian adversaries have proven extremely adept at exploiting legal loopholes in Western democracies for their own benefit. If democratic societies are to deter acts of strategic political sabotage sponsored by hostile powers, their political leaders and security professionals must anticipate and prepare for legitimate acts that are likely to create opportunities for significant political damage. When developing strategies for deterring political sabotage, potential target countries must also consider the targets of their deterrence by communicating to the strategic saboteurs, the sponsoring hostile powers, or both, the consequences of their malicious actions. The two actors may be linked, but they will often have differing motivations, and thus the tools employed to deter must also be tailored to each targeted "audience."

Deterring a hostile power from sponsoring acts of strategic sabotage falls into the realm of statecraft: the use of tools such as diplomacy, sanctions, and public opinion to change would-be aggressors' cost-benefit calculus. The more challenging aspect of deterring strategic sabotage is the internal, or domestic, problem of dissuading citizens from conducting extreme political acts in the first place and encouraging them to consider the second or third-order effects of those acts.

Political scientists Andrew H. Kydd and Barbara F. Walter explored how activists used extreme acts, including violence, to sabotage popular political efforts that would have led to peace and stability in war-torn regions. They found that there is little that is random, irrational, or indiscriminate about what saboteurs intend. In fact, the saboteurs

know they are "playing a role," conducting acts of political theater to influence the masses and in turn shape strategic decision-making in their favor.[18]

Democratic governments have a duty to protect the rights of dissidents, activists, and sometimes even nut-cases. Burning a Qur'an is a blasphemous and punishable act in Muslim-majority countries, but that is not the case in most secular societies. As was seen in Sweden and Denmark, even though the burnings caused offense, they were not illegal, and both Paludan and Momika took advantage of their relative protection from prosecution. Swedish and Danish authorities had little official recourse other than to tolerate the offensive acts in the interest of sustaining their free and liberal societies.

Deterrence theory since the end of the Second World War has primarily focused on avoiding nuclear confrontation and major conventional war between the superpowers. Western deterrence policies and the resulting implementing strategies have been decidedly military in nature, based upon physical aspects of military strength—tanks, ships, aircraft, divisions, and corps—reinforced by arsenals of nuclear weapons. In 1966, at the height of the Cold War, Thomas Schelling wrote one of the foundational works for the study of modern coercion and deterrence theories, *Arms and Influence*.[19] That volume, which has guided many other theorists' and strategists' work, recognized that deterring an individual was a cognitive exercise and that the motivations necessary for individual deterrence were different than those necessary for deterring a nation-state that one assumes acts rationally based upon quantitative cost-benefit analyses. Individuals have the freedom to make their underlying issues personal, and thus the range of deterring actions and policies needs to emphasize the human domain where decisions are often driven by intangibles such as passion, anger, culture, isolation, powerlessness, perception, bias, and feelings.

Karl Mueller, from RAND, expanded on Schelling's work by describing deterrence as the range of preventative measures taken through a combination of denial and punitive strategies. Denial strategies, observed Mueller, are the sum of tangible and intangible actions taken to convince an opponent its objectives are unattainable. He found that denial strategies were overwhelmingly more effective than punitive strategies. Threats of after-the-fact punishment tended to be effective only when one opponent believed the other possessed and was willing to use the full range of capabilities at its disposal—capability and credibility (will).

Adapting deterrence theory to address domestic political sabotage means stepping outside Western politicians' traditional comfort zone: the rational comparisons between each nation's capabilities. When addressing political sabotage, governments should implement and employ whole-of-society approaches that address the human aspects of conflict.

DETERRING STRATEGIC SABOTAGE

Preventing acts of strategic political sabotage must be the preferred goal of deterrence and can be achieved through a combination of *preemption, education, co-option*, and *prosecution* strategies.

During the 2010's efforts to sustain and improve the peace in Northern Ireland, an independent review of the security situation revealed that the biggest threat to maintaining the peace agreement was not from sectarian paramilitary groups who had agreed to a ceasefire, but instead from individual dissidents, both nationalist and unionist, who disagreed with the political process and wanted to sabotage the effort.[20] Preempting these individual dissidents' efforts to sabotage the peace required collaboration by the Northern Ireland Executive, the police, domestic intelligence services, tax agencies, and the different factions. The governments

declared their intent to ensure the peace, used the appropriate tools available to the different groups, and then communicated the collective intent and the results through the courts and the media. For the most part, preemption succeeded in keeping a lid on attempts at political sabotage.

Most Western societies already have a range of legal and ethical tools within their community policing and domestic antiterrorism laws, as well as acceptable forms of open-source information gathering. Law enforcement, domestic intelligence agencies, and citizens' groups enable governments to influence potential saboteurs and anticipate possible adverse activities. In societies with traditions of civil liberty and the rule of law, it can be difficult for law enforcement agencies to be preemptive. In a contest for influence, it is, instead, an engaged citizenry that often creates awareness of the motivations and contexts that push activists to take adverse actions, and who then help governments avoid or mitigate acts of strategic political sabotage.

We don't know if Swedish diplomats informed the government of Turkey before Paludan's planned Qur'an burning or if their counterparts in Budapest were even aware that Orban would take exception to Swedish opposition politicians' unflattering use of his name in what was an internal Swedish debate. We also don't know if, given that Erdogan was facing a contested reelection campaign, it would have made any difference explaining to Turkey's leadership that burning a Qur'an, while condemned by Swedish politicians, is a protected right under Swedish law and could not be legally stopped. In both volatile and less volatile situations, there is always value in informing an external government that may be targeted by activists.

Media Literacy for You(th)" Project's Youth Exchange Was Held in Kaunas, Lithuania, on 01 – 11 February 2023. Photo by International Labor Association, February 11, 2023.

Strategic political sabotage has the power to shock sensibilities, disrupt leaders and societal routines, and influence populations to support policies contrary to the overall good. The power of education, though, is that when artfully, ethically, and consistently delivered, it can stiffen the population against the effects of malicious influence by raising awareness of political extremism, illustrating the dangers posed by information bias, and building resilience among the population to recognize and resist malign influence, disinformation, and deceptive practices.[21]

Moscow's robust international propaganda efforts after its illegal annexation of Crimea in 2014 and again in 2022 served as a wake-up call for Western nations that had previously downplayed Russian disinformation campaigns. Moscow weaponized two key pillars of liberal democracy, free speech and free media, to shape the Crimea narrative in its favor.[22]

Lithuania, which shares a common border with Russia, had previously suffered from Russian disinformation. The Lithuanian leadership mobilized governmental, educational, social, and private sector organizations and institutions to blunt the impact of Russian propaganda. This Baltic nation used its existing laws to insulate the public from Russian state media and began a public education campaign to raise awareness and created an information literacy program among its most vulnerable citizens—minorities, the elderly, and youth. They also used the judicial system to punish those who intentionally spread false damaging information.[23] By encouraging grassroots efforts to counter

Loyalist banner and graffiti on a building in the Shankill area of Belfast, 1970. Photo by Fribbler (Wikimedia Commons).

Russian disinformation, debunk false claims, and spread truthful counter-narratives, Lithuania proved the power of an educated population and sent a powerful message demonstrating its ability to resist external efforts to sabotage domestic policies and programs, while also preparing its population for future malign influence from Moscow.

Internally, government authorities can choose to deny strategic saboteurs' quest for legitimacy and credibility by controlling or ignoring the intended message, or instead they might meet the activists halfway. By co-opting the saboteurs' messaging and working toward compromise solutions, governments have the power to create acceptable outcomes all parties can agree to. Political scientist Markus Holdo, from the University of Lund in Sweden, has examined anti-establishment discourse and political co-option as means of influencing social change. He concludes that co-opting activist groups and individual dissidents by cooperating and collaborating with them offers an effective means of controlling opposition minorities and encouraging them to work within the authority's agenda in the hope that both sides might remain politically relevant.[24]

One of the most successful cases of political co-option is the 1998 Good Friday Agreement that ended Northern Ireland's 30-year sectarian conflict. Prior to that agreement, every other attempt at compromise and negotiation had been sabotaged by radicals from both parties who failed to trust the other sides' intentions or their own leaders' abilities to implement the terms of the various negotiated agreements.[25] By the late 1990s, citizens in both the nationalist and the unionist camps were exhausted by the violence and by the cost of policing Northern Ireland. The Good Friday Agreement between the governments of Ireland and the United Kingdom, as well as the four major political parties, co-opted the sectarian paramilitary groups, got the political leaders to agree to ceasefires and laying down their weapons, and brought the militants into the political process. While the ensuing twenty-five years have not been without challenges, the peace has held in Northern Ireland.

When skillfully done, co-opting an opposition group can avoid future harmful acts that might damage a nation's policies or standing. The decisive aspect is whether the political act aids a hostile power and can be linked to that power. Awareness of domestic extremists' agendas and any links to unfriendly regimes offer acceptable criteria for determining if politically-motivated acts of protest are an appropriate vulnerability to be tolerated or if the acts are credible threats to national security and regional stability. Democracies thus have two tasks: they must constantly, legally, and appropriately monitor groups and individuals likely to engage in acts of political sabotage, and they must, also within the rules of law, address any evidence that domestic activists are acting with or for the interests of hostile powers.

Prosecuting a strategic saboteur after the fact falls outside the definition of deterrence by denial. Instead, it is a punishment strategy that hopefully will deter future acts of political sabotage. Paradoxically, punishing political sabotage, especially when given global visibility through modern communication tools, can enable political saboteurs to amplify their messages, extend their causes' lifespans, and exert significant control over their intended messaging. Governments must carefully balance between prosecuting illegal acts and enabling the public "microphone" political saboteurs crave. Much like efforts to suppress civil disobedience, efforts to thwart political sabotage must be subject to rules of evidence and due process. Most important, however, is that legitimate acts of political expression cannot, and should not, be prevented in liberal democracies. If, however, the government does find it necessary to prevent acts of political sabotage, it must be demonstrated that the acts violated the country's national security laws and be clearly attributed to a hostile power.

CONCLUSION

Strategic political sabotage is so powerful because it occupies the nexus of freedom of expression and gray-zone aggression. Without an illegal act or a hostile power nexus, activists whose protests harm their country's policies or international standing enjoy freedom-of-expression protections. If, however, such acts are undertaken with the support of a hostile power, they then constitute gray-zone aggression—efforts by a hostile power to cause harm through non-kinetic means that stay below the threshold of conflict. To deter potential gray-zone aggression it is imperative that a nation identify and preemptively disrupt hostile sponsors by denying the saboteurs political, financial, and social support, as well as pursuing after-the-fact investigation and attribution that places blame and imposes consequences for any meddling, where appropriate.

To effectively avoid the harm of political sabotage, governments must monitor links between activists and foreign powers. Once alerted to impending political sabotage the government can then execute its deterrent strategies and programs that combine techniques of preemption, education, cooption, and prosecution to mitigate potential harmful effects while also protecting the guarantees of democratic freedom. This can include changing the location of the permitted demonstration, educating the public about external meddling and possible interference in domestic protests, and collaborating with nongovernmental organizations (NGOs) to correct disinformation by hostile activists and to preempt malign state and non-state actors bent on sabotaging legitimate political processes.

Governmental and societal understanding and acceptance of the rights of appropriate political protest remain central to preserving democracy. Governments and citizens must ensure awareness of political protesters' likelihood to break laws and any possible connections to hostile powers. Activists who reflect opposition elements of society must carefully evaluate the consequences of their actions and the potential national harm their acts of sabotage might cause. Together, governments and societies require proactive thought and engagement on the topic of strategic political sabotage if they are to effectively protect themselves from actors and actions intended to undermine the stability, standing, and well-being of their societies. PRISM

Notes

[1] In 2019, 18 of 20 nations in the Middle East and North Africa had laws criminalizing blasphemy and enforced those laws to varying degrees, including the death penalty. Virginia Villa, "Four-in-ten countries and territories worldwide had blasphemy laws in 2019" (25 Jan 2022), https://www.pewresearch.org/short-reads/2022/01/25/four-in-ten-countries-and-territories-worldwide-had-blasphemy-laws-in-2019-2/. A significant number of European nations still have such laws on the books, https://end-blasphemy-laws.org/countries/europe/.

[2] Momika's is an interesting case. He not only burns Qur'ans for publicity, but also rants against Islam and livestreams the events on TikTok, earning about $270 per video. Burak Bir, "Salwan Momika: Quran burnings for freedom or money?" (7 Sep 2023), https://www.aa.com.tr/en/world/salwan-momika-quran-burnings-for-freedom-or-money/2981044#.

[3] Sweden agreed to support Turkey's accession process to the European Union and will also support visa liberalization within the EU's Schengen Zone. The United States will sell Turkey new F-16 fighter jets and help modernize the F-16s Turkey already owns. https://www.aljazeera.com/news/2023/7/11/why-turkey-changed-its-stance-on-swedens-nato-membership-2.

[4] Patrick Wintour and Lili Bayer, "Turkey's president submits bill to ratify Sweden's NATO membership," *The Guardian* (23 Oct 2023), https://www.theguardian.com/world/2023/oct/23/turkey-submits-bill-to-ratify-sweden-nato-membership.

[5] Jack Detsch, "Hungary is Not Out to Scuttle Sweden and NATO," *Foreign Policy* (18 Sep 2023), https://foreignpolicy.com/2023/09/18/hungary-sweden-turkey-orban-nato/; Justin Spike, "Hungary in the spotlight after Turkey approves Sweden's bid to join NATO," *PBS News Hour* (24 Oct 2023), https://www.pbs.org/newshour/world/hungary-in-the-spotlight-after-turkey-approves-swedens-bid-to-join-nato.

[6] Lewis H. Van Dusen, Jr., "Civil Disobedience: Destroyer of Democracy," *American Bar Association Journal*, vol. 55 (Feb 1969), p. 123.

[7] "Russia planned Islamophobic campaigns in Finland, Sweden to delay NATO membership" (4 Dec 2023), https://yle.fi/a/74-20063396.

[8] https://www.britannica.com/event/World-War-I.

[9] Srećko Horvat, "First world war: was Gavrilo Princip a terrorist or a freedom fighter?" *The Guardian* (15 Apr 2014), https://www.theguardian.com/commentisfree/2014/apr/15/first-world-war-gavrilo-princip-terrorist-freedom-fighter-revisionism.

[10] Biljana Radivojevic and Goran Penev, "Demographic Losses of Serbia in the First World War and Their Long-Term Consequences," *Economic Annals*, vol. LIX, no. 203 (Oct-Dec 2014), p. 39.

[11] https://www.oic-oci.org/topic/?t_id=39325&t_ref=26550&lan=en (31 Jul 2023).

[12] *Letter from Ministry of Foreign Affairs and Trade to H.E. Mr Tobias Billström, Minister for Foreign Affairs* (14 Sep 2023), https://twitter.com/zoltanspox/status/1702299045878747421?s=20.

[13] Jennifer Rankin, "Burning of Qur'an in Stockholm funded by journalist with Kremlin ties," *The Guardian* (27 Jan 2023), https://www.theguardian.com/world/2023/jan/27/burning-of-quran-in-stockholm-funded-by-journalist-with-kremlin-ties-sweden-nato-russia.

[14] Erdogan has demanded that Sweden extradite a number of militant Kurds who have been given political asylum in Sweden.

[15] Jolanta Darczewska and Piotr Zochowski, *Active Measures: Russia's Key Export* (Warsaw, Poland: Centre for Eastern Studies, Jun 2017), pp. 29–30.

[16] David Pozen, "Edward Snowden, National Security Whistleblowing, and Civil Disobedience," *Lawfare*, (26 Mar 2019), https://www.lawfaremedia.org/article/edward-snowden-national-security-whistleblowing-and-civil-disobedience.

[17] Charles Maynes, "Putin grants Russian citizenship to Edward Snowden," *NPR* (26 Sep 2022), https://www.npr.org/2022/09/26/1125109303/putin-edward-snowden-russian-citizenship.

[18] Andrew Kydd and Barbara F. Walter, "Sabotaging the Peace: The Politics of Extremist Violence," *International Organization*, vol. 56, no. 2 (Spring 2002), pp. 264–65.

[19] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).

[20] Hristin Archick, *Northern Ireland Peace Process: Background and Challenges* (Washington, DC: Congressional Research Service, 8 Mar 2019), p. 19.

[21] "Cognitive Biases," https://thedecisionlab.com/biases; "Breaking Harmony Square," https://harmonysquare.game/en.

[22] Vytautas Kersanskas, *Deterring disinformation? Lessons from Lithuania's countermeasures since 2014* (Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats, Apr 2021), p. 7.

[23] Kersanskas, pp. 10–12.

[24] Markus Holdo, "Cooptation and non-cooptation: elite strategies in response to social protest," *Social Movement Studies*, vol. 18, no. 4 (2019).

[25] Archick, p. 3.

Cybersecurity on Retainer

Supporting National Incident Response Capability Through the Private Sector

By Andrew S. Pasternak and Rachel R. Gaiser

In a recent issue of *Foreign Affairs*, Chris Inglis and Harry Krejsa argued that the current state of affairs in the cyber ecosystem needs to be fixed, with too much risk pushed down to users, small businesses, and local governments. What is needed instead, they argue, is "a new social contract for the digital age," one that changes the current cybersecurity paradigm between the public and private sectors. This paradigm shift would include governments and large firms shouldering more of the burden, transitioning to a more "collective, collaborative defense."[1] This kind of paradigm shift is even more crucial for response to severe cyber incidents, defined in the *National Cyber Incident Response Plan's* (NCIRP) Cyber Incident Severity Schema (CISS) as an incident or group of incidents "likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties."[2, 3, 4]

Mr. Andrew S. Pasternak is a Senior Policy Advisor in the Office of the National Cyber Director. **Ms. Rachel R. Gaiser** is an Advisor at the Cybersecurity and Infrastructure Security Agency. The authors completed this article in their personal capacity and prior to beginning their positions in their respective offices.

The United States has been fortunate so far that no cyberattack has matched the level of a severe cyber incident, but this may not always be the case. State and non-state actors continue to improve their offensive cyber capabilities, threatening the critical infrastructure vital to the United States. Ransomware gangs attack organizations fundamental to everyday life, from city governments to hospitals to pipelines. The return of great power competition to interstate relations between the United States, the People's Republic of China (PRC), and the Russian Federation is, at this point, treated as a fact in U.S. national security policy.[5] With great power competition comes the remote yet real possibility of great power conflict, increasing, in turn, the likelihood of a severe cyber incident.

During a severe cyber incident, the public expects the government to defend the Homeland, including critical infrastructure disruption of which would affect national security, economic stability, or public health and safety.[6] The technical capacity to respond to severe cyber incidents is vital for the federal government to mitigate the effects on the nation's security. At the time of this writing, however, the government cannot provide non-federal entities Digital Forensics and Incident Response (DFIR) services at scale, nor is there a mechanism for the government to rapidly coordinate and deploy private sector DFIR services to prioritized critical infrastructure partners.[7] Over 700,000 cybersecurity positions are unfilled in the United States, including approximately 40,000 vacancies in the public sector. With the higher salaries offered by the private sector, it seems unlikely that the federal government will be able to develop the necessary DFIR capacity internally any time in the near future.[8]

With the government unlikely to internally develop the DFIR capacity needed to respond to severe cyber incidents, policymakers should consider paying to retain private sector DFIR capacity. A Cybersecurity Retainer Program (CRP) would allow the government to rapidly expand DFIR capacity during a severe cyber incident. A CRP would also incentivize private sector partners to maintain DFIR teams optimized for national security incident response services and improve readiness by training and exercising with CRP teams before a severe cyber incident occurs.

This article first assesses the current strategic environment, including how DFIR services are provided and the challenges with providing DFIR services during severe cyber incidents. The following section details the concept of the CRP and compares it to two alternative options: a civilian cybersecurity reserve and the use of the Defense Production Act. The final section examines issues that must be considered and further researched if the government is to develop the CRP, including costs and who can access DFIR services.

UNDERSTANDING THE CURRENT STRATEGIC ENVIRONMENT

Private sector entities and state and local governments without DFIR capabilities rely primarily on private cybersecurity vendors for DFIR services when a cyber incident occurs. These vendors can hire personnel and charge clients at rates reflecting the demand for these services. Organizations can obtain these services ad hoc or through a retainer agreement. Many vendors provide incident response activities, though the capability of these vendors can vary significantly.[9] The National Cyber Incident Response Plan highlights the role of the private sector during severe cyber incidents, with the private sector providing for the security of its networks and often providing support or assistance to federal agencies.[10]

Great power competition, and with it the remote yet real possibility of great power conflict, increases the likelihood of severe cyber incidents, with U.S. competitors demonstrating the capability and intent to target civilian infrastructure. The PRC, for example, has demonstrated the capability

to target U.S. critical infrastructure, including compromising thousands of organizations simultaneously and targeting U.S. infrastructure to develop cyberattack capabilities.[11, 12, 13] The People Liberation Army's 2020 *Science of Military Strategy* (SMS) calls out "national information infrastructure" as a critical target for "cyber electromagnetic space warfare,"—a phrase that includes cyber warfare as one of its primary forms.[14, 15, 16] Finance, energy, and transportation are mentioned explicitly in the SMS, though other infrastructure sectors are likely targeted. The SMS also uses the 1999 campaign of bombing Yugoslavia by NATO as an example of successfully targeting civilian infrastructure, saying that switching from military to civilian infrastructure crushed the will of the Yugoslav Federation. This example is given in a section on cyberspace, suggesting that the authors believe offensive cyber operations could have a similar effect.[17]

While the almost exclusively private sector arrangement is typically beneficial given the private sector's resources, severe cyber incidents, most notably those occurring during a conflict, would challenge the ability of the private sector to respond due to the issues of scale, prioritization, and coordination. Severe cyber incidents could affect hundreds or thousands of organizations. Cybersecurity vendors exist within a business model that could prioritize organizations for restoration differently than would the federal government, leaving vital infrastructure operators without needed assistance. Some level of communication and coordination currently exists across prominent cybersecurity vendors through organizations such as Information Sharing and Analysis Centers and the Cybersecurity and Infrastructure Security Agency(CISA)'s Joint Cyber Defense Collaborative (JCDC), but not nearly on the scale to allow coordinated and prioritized incident response activities during an extended period of intensified malicious activity.[18, 19]

During severe cyber incidents, the general public and private sector expect the government to take a more prominent role in coordination and cyber incident response, ensuring the safety of government operations and the nation's critical infrastructure. The problem with this expectation is that even if hiring, training, and retaining cybersecurity personnel were not an issue, the small number of

CAD design for new facility for Cybersecurity and Infrastructure Security Agency. Source: Government Services Agency

government personnel with the skillset needed for DFIR operations makes it highly unlikely the federal government will ever be able to undertake incident response activities at scale. In the Fiscal Year 2021 enacted budget, CISA had 607 positions designated for cyber operations programs, projects, and activities. Threat Hunting, which includes the hunt and incident response services provided by CISA, comprised 181 of these positions.[20] The number within Threat Hunting that could undertake incident response services is smaller. Threat Hunting's workforce is supplemented by contractors that provide the added technical capability. Still, the small numbers highlight how challenging it could be for CISA to respond to incidents within federal networks during severe cyber incidents, let alone incidents at critical infrastructure entities.

The Department of Defense (DOD) also retains DFIR capabilities that may assist during severe cyber incidents outside of conflict. During a conflict, however, DoD is unlikely to have the personnel to perform DFIR activities for key critical infrastructure partners. As of 2022, U.S. Cyber Command's Cyber Mission Force comprises 133 teams, a subset of which are Cyber Protection Teams intended to defend the Department of Defense Information Network and critical infrastructure.[21] The National Guard's cyber force has over 2,200 personnel and has previously assisted in critical infrastructure cyber defense, though the number able to participate in DFIR operations is a smaller subset.[22] During a conflict, DOD network defenders will have to respond to increased malicious activity against DOD networks, limiting the availability of DOD cybersecurity personnel to respond to cybersecurity incidents at critical infrastructure entities.

The federal government, like practically all organizations in the public and private sectors, has been attempting to overcome an acute cybersecurity workforce shortage. According to a 2022 Federal Cyber Workforce Management and Coordinating Working Group report, over 700,000 cybersecurity positions remain unfilled in the United States, including approximately 40,000 vacancies in the public sector.[23] This high number of vacancies in the U.S. cyber workforce includes the highly technical personnel needed for DFIR activities. The federal government and other organizations have understood the growing workforce shortage for years, but despite numerous efforts, they still need to close the workforce gap.[24] On top of this, the federal government's cybersecurity workforce skews older: less than 6 percent are under 30, while over 30 percent are over 55.[25]

The reasons for this workforce shortage in the federal government are discernible. Private sector employers typically offer higher salaries and can hire employees quickly.[26] Federal wages are typically lower, and a candidate can take months or years to be hired after the initial job offer, depending upon the bureaucratic and security requirements of the position. For example, a 2022 report from CISA's Cybersecurity Advisory Committee found that the agency took an average of 198 days to complete the onboarding process after a candidate received an offer.[27] Once government agencies hire and train cybersecurity personnel, retaining this workforce presents difficulties, with higher salaries and appealing opportunities within the private sector enticing many to leave.

CISA and other agencies are taking steps to improve the development and retention of a cybersecurity workforce, with mixed results. It is not likely, however, that the federal government will be able to develop and maintain the capability to respond to the increased malicious cyber activity likely to occur during a severe cyber incident. The federal government will need to rely extensively on private sector capacity to secure the nation's critical infrastructure. Nevertheless, there is currently little infrastructure to increase the government's DFIR capabilities through coordinating and directing private sector capabilities during a severe cyber incident.

DEPLOYING PRIVATE SECTOR CAPABILITY THROUGH A CRP

Given the small size of the federal government's DFIR capability and the likelihood that improving hiring and retainment practices, while helpful, will not resolve the problem, other means of obtaining the capacity needed during a severe cyber incident must be considered, and this requires looking to cybersecurity vendors in the private sector. Rather than trying another hiring or personnel retention program that only marginally improves the situation, a Cybersecurity Retainer Program would allow the government to maintain an extensive incident response capacity for severe cyber incidents that can be deployed rapidly and sustained at a relatively low cost.

A CRP would function similarly to the retainer services provided by cybersecurity vendors and other industries, with some differences. The federal government, through CISA or another agency, provides annual funding to selected cybersecurity vendors via approved contractual processes. These vendors then provide DFIR response capabilities when requested. Unlike typical retainers, CRP funding ensures that cybersecurity vendors maintain the DFIR capability needed by the government during a severe cyber incident. DFIR teams would be available for rapid deployment to the government for extended periods that could last months or even years.

Similar federal programs allow the government to retain services for times of conflict that would otherwise be unavailable. One example is the Maritime Security Program (MSP), run by the Department of Transportation's Maritime Administration (MARAD). While Military Sealift Command and MARAD maintain cargo vessels to support military operations, maintaining a cargo fleet large enough to sustain operations during a large-scale conflict would be extremely expensive without any certainty that the ships would ever be used. Rather than pay large sums to build and maintain such a fleet, MARAD provides ship operators with a financial retainer for 60 ships; in return, the operators will provide the ship to the U.S. government during times of war or national emergency.[28, 29] A 2009 study of the program ordered by the Department of Transportation, 13 years after the beginning of the program, found that the MSP had a clear positive impact on the number of U.S.-flagged vessels and their availability for military use, as well as the availability of mariners to operate these vessels.[30]

While cybersecurity and maritime shipping may seem completely different, they share two fundamental similarities: the cost of maintaining the capability is high, and most of the capacity is in the private sector. MSP is a prime example of using government funding to ensure capacity during a time of need while avoiding the higher cost of owning the capacity during peacetime. A cybersecurity retainer program would provide a similar solution, providing the government with a way of increasing capacity that can be quickly deployed against threats and incidents.

Establishing a CRP will incentivize private sector partners to work with the federal government to maintain DFIR teams optimized for national security incident response services. These teams will benefit from working together before any severe cyber incident occurs, allowing them to respond more effectively when called upon by the government. While the CRP, unlike the MSP, is not needed to maintain sufficient capacity in the private sector, it could be used to incentivize the maintenance and growth of private sector capabilities valuable during a severe cyber incident.

Another benefit of the CRP for both the private sector and the government is the ability to regularly conduct cybersecurity exercises by combined government and CRP DFIR teams. Research shows that regularly exercising cyber security incident response plans and other scenarios helps DFIR teams improve overall readiness to respond to incidents, including improving collaboration and coordination between team members.[31] For example, incorporating CRP

DFIR teams into CISA's biennial Cyber Storm Exercise—the most extensive government-sponsored cybersecurity exercise—would provide the CRP DFIR teams with a holistic introduction to working with federal, state, local, territorial, and tribal partners.[32] Although the government may only fully activate CRP DFIR teams during a severe cyber incident, exercising different scenarios will provide CRP DFIR teams with needed context and familiarity by coordinating with thousands of stakeholders across the government.

ALTERNATIVES TO CRP PROVIDE FEWER BENEFITS

Voluntary and compulsory options exist for the federal government to tap into private sector capabilities during a conflict. We will discuss below two CRP alternatives: the development of a civilian cybersecurity reserve and the use of the Defense Production Act during a conflict. While these options provide benefits, neither offers the same ability as the CRP to rapidly scale and deploy DFIR capabilities at the outset of a severe cyber incident.

Civilian Cyber Reserve

The Civilian Cyber Security Reserve Act was a bipartisan bill introduced in 2021 that proposed permitting CISA to create a pilot civilian reserve program. CISA would develop a reserve of up to 30 members to activate during a severe cyber incident. When activated, civilians in the program would be considered members of the federal civil service.[33]

Given the program's small size and the status of reservists as federal civil servants, CISA's probable goal would be to integrate those in the reserve program into CISA operations, boosting existing technical teams, including DFIR teams. The bill represented a novel approach to increasing government capacity during a time of need and built off a military reserve model with various degrees of international success.[34]

If fully staffed with effective technical personnel who can quickly integrate into CISA operations—far from a given—reserve personnel could improve CISA capabilities to a limited degree. Even with the understanding that the program put forward in the Civilian Cyber Security Reserve Act is a pilot program, it seems highly unlikely that an even more extensive program would put a dent in the capability needed to defend private, state, and local government networks during a severe cyber incident. This added capacity will likely be needed to defend federal networks, limiting their availability for critical infrastructure network defense. Any incident response-focused reservists would also be leaving their respective private sector teams during a conflict, affecting the capability of those private sector organizations to provide DFIR services.

The difficulty of integrating reserve personnel into existing operations could also hinder the effectiveness of a reserve program. Technical personnel within CISA already have demanding, high-tempo positions, which reduces available time to work with reservists, understand their capabilities and personalities, and determine how they can best be deployed when activated. This issue becomes more acute as the size of any reserve program increases, especially for an agency such as CISA beginning with limited technical staffing.

Finally, while the reserve program did not allocate any additional funds, the cost of a cyber reserve program needs to be considered. Given the current recruitment issues due in part to the higher salaries in the private sector, any cyber reservist would likely require pay commensurate with the time required. Between individual income, additional administrative costs such as travel, equipment, and security clearances, and uncertainty about the scalability and effectiveness of the program, it is unclear if the return on investment would be comparable to other programs such as the CRP.

Defense Production Act

As noted in the Cyberspace Solarium Commission's report, the Defense Production Act (DPA) provides the President with expansive authority to prioritize resources and services to promote the national defense. However, current DPA planning does not account for cybersecurity services.[35,36] Congress added critical infrastructure protection and restoration to the definition of national defense within the Defense Production Act in 2003.[37]

Utilizing the DPA to ensure private cybersecurity vendors prioritize government contracts would scale government capability. The DPA does not conflict with the idea of a CRP and can complement it by providing additional capacity if needed. Relying solely on the DPA will prevent the government from rapidly scaling incident response capacity during a severe cyber incident or in the lead-up to and beginning of a conflict. Once the decision is made to invoke the DPA, the government will need to identify which cybersecurity vendors to call upon, assess the capabilities of these organizations, and determine how to deploy and coordinate the DFIR teams and other services provided by these vendors. This will take time. Given the rapid pace at which cyber operations may unfold at the beginning of an armed conflict, opportunities to limit operational impacts from malicious cyber activity may be missed.

Some of this activity, such as identifying vendors and coordination mechanisms, can be undertaken before a conflict. The Cyberspace Solarium Commission recommended a similar path, suggesting that the government convene incident response vendors to understand their capacity and procure standby contracts.[38] While this recommendation is a vital step forward, it is effectively like developing a CRP without the additional coordination and capability development a formal program provides. The government will still be able to utilize the DPA to increase DFIR capacity. However, maintaining a CRP will give the government the increased resource capacity to shape, coordinate ahead of any severe cyber incident, and rapidly deploy.

DEVELOPING THE WAY FORWARD

While the authors believe that a Cybersecurity Retainer Program can optimally provide the expanded capacity the federal government would require during severe cyber incidents, further work is needed to understand the associated requirements, costs, and potential risks.

The government must decide what kind of incident response capacity is required and how many incident response teams to include in the CRP. For example, the government will want to maintain an incident response capacity specializing in industrial control systems and operational technology. Ultimately, the size and composition of the CRP will be determined by several factors, including funds provided by Congress, threats as determined by the Intelligence Community, identified risks to U.S. critical infrastructure, and private sector capabilities.

While decisions on the kind and size of the incident response capacity will ultimately drive costs per DFIR team, the CRP can be cost-beneficial compared to the government's civilian cybersecurity budget. For comparison, as of 2022, the Maritime Security Program pays companies $5.3 million per vessel for 60 vessels, totaling $318 million.[39] The MSP provides funds to maintain the sealift capacity and employment for approximately 2,400 merchant mariners. The CRP would be a fraction of this cost, as it is not needed to maintain any physical infrastructure, nor are the funds necessary to support what is already a robust market. Instead, CRP funding is intended to solely maintain DFIR teams that will be prioritized for government use when needed.

Like all government programs, oversight will be crucial to maintaining the effectiveness of the

CRP. The government will need to ensure that those wanting to join the program can provide the skillsets and capacity required and will continue to do so. Program administrators must also decide on various administrative requirements, such as any security requirements associated with DFIR team members. The CRP will require similar oversight to other programs, with the government specifying the program's requirements and vendors demonstrating regularly how these requirements are being met.

The government will also need to make clear what entities would qualify for assistance from CRP vendors during a severe cyber incident. The goal of the CRP is not to replace existing private sector DFIR capacity but to ensure some of this capacity is available and prioritized for those organizations whose disruption could have national security impacts. CISA is currently undertaking efforts to identify "Systemically Important Entities," which can be a first step to identifying those organizations to prioritize for CRP assistance during a severe cyber incident.[40] A CRP would also incentivize entities designated as systemically important to collaborate with the government.

Entities receiving CRP assistance would need to be reassured that their sensitive information is being protected and that the government is not seeking to use a CRP vendor's access to investigate or otherwise examine them. To affirm that the role of the CRP is to assist critical infrastructure entities—not to investigate or punish them—it will be vital to develop data safeguard measures such as standard liability releases, confidentiality protections, and vendor prohibitions on sharing CRP recipient's non-essential, voluntarily-provided information with the federal government. The government should develop a methodology for deciding the share of the cost of DFIR services paid for by the victim of a severe cyber incident. Government expenditures during an armed conflict, for example, would increase dramatically, and saving even small amounts can ensure the longevity and flexibility of the program. Some organizations, such as Fortune 500 companies, can bear the costs of access to the CRP if such access is even needed. Other organizations may face ruinous costs if not given assistance, and cybersecurity insurance may not be able or willing to cover severe incidents, especially acts of war.[41, 42] Although beyond the scope of this article, a well-developed methodology for deciding cost-sharing will reduce government expenses while ensuring systemically important entities receive the DFIR services necessary to restore operations at a reasonable cost.

CONCLUSION

Preparing to defend the homeland in cyberspace during a severe cyber incident requires the government to have the capacity to respond to cybersecurity incidents on its networks and the networks of critical infrastructure operators. As laid out in this article, it seems unlikely that the government will be able to scale its limited DFIR capacity in the near future and will rely on the private sector to provide this capacity.

Ensuring the government has the capacity needed during severe cyber incidents requires efforts beyond the baseline government-private sector collaboration consisting of information sharing and coordination done today. A CRP would provide the government with the DFIR capacity needed during a national emergency, promote its maintenance in the private sector during peacetime, and provide an avenue to plan better and exercise this DFIR capacity. While the best future is one where this capability is never needed, a CRP provides the government the capacity to respond to cyber incidents, building the collective, collaborative defense that will improve the nation's resiliency. PRISM

Notes

[1] Chris Inglis and Harry Krejsa, "The Cyber Social Contract: How to Rebuild Trust in a Digital World," *Foreign Affairs*, February 21, 2022, https://www.foreignaffairs.com/articles/united-states/2022-02-21/cyber-social-contract.

[2] The CISS is a scale used by CISA to provide a repeatable and consistent mechanism for evaluating the risk severity of an incident. The scale has a 0-5 scale, with 0 being the least severe and 5 the most severe. Level 4 are severe incidents. Level 5 are emergency incidents described as "an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens."

[3] Department of Homeland Security, "National Cyber Incident Response Plan," December 2016, 8, www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[4] Cybersecurity and Infrastructure Security Agency, "CISA National Cyber Incident Scoring System (NCISS) | CISA," September 30, 2020, https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss.

[5] The word "competition" is used 44 times in the 2022 *National Security Strategy*, with the first section being called "the competition for what comes next." See: White House, *National Security Strategy*, October 2022, 6, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[6] "Presidential Policy Directive—Critical Infrastructure Security and Resilience," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[7] For an explanation of DFIR, see: Crowdstrike, "Digital Forensics and Incident Response Explained," October 12, 2022, https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/.

[8] Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce: A Call for Collective Action*, September 2022, 6, https://www.cisa.gov/sites/default/files/publications/State_of_the_Federal_Cyber_Workforce_Report_09.14.2022.pdf.

[9] Prateek Bhajanka and Wam Voster, "Market Guide for Digital Forensics and Incident Response Services," *Gartner*, September 21, 2021, https://www.gartner.com/doc/reprints?id=1-27NMS8JH&ct=211015&st=sb.

[10] Department of Homeland Security, "National Cyber Incident Response Plan," December 2016, 15, www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

[11] The White House, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

[12] United Kingdom National Cyber Security Centre, "U.K. and allies hold Chinese state responsible for pervasive pattern of hacking," July 19, 2021, www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking.

[13] Cybersecurity and Infrastructure Security Agency, "Alert (AA21-201A), Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013," Department of Homeland Security, last revised July 21, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-201a.

[14] China Aerospace Studies Institute, trans. *Science of Military Strategy*. National Defense University of the People's Liberation Army (PLA), 2022, 235, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf.

[15] Elsa B. Kania and John Costello, "Seizing the commanding heights: PLA Strategic Support Force in Chinese military power," *Journal of Strategic Studies* 44:2 (2021), 226.

[16] Joe McReynolds, "China's Military Strategy for Network Warfare," In Joe McReynolds, ed., *China's Evolving Military Strategy*, Washington, DC: The Jamestown Foundation, 2017, 209.

[17] China Aerospace Studies Institute, trans. *Science of Military Strategy*. National Defense University of the PLA, 2022, 151-152, 263, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf.

[18] "National Council of ISACs | About ISACs," n.d. https://www.nationalisacs.org/about-isacs.

[19] "Joint Cyber Defense Collaborative | CISA," n.d. https://www.cisa.gov/jcdc.

[20] Department of Homeland Security, *Cybersecurity and Infrastructure Security Agency Budget Overview, Fiscal Year 2023 Congressional Justification*, 2022, 114, https://www.dhs.gov/sites/default/files/2022-03/Cybersecurity%20and%20Infrastructure%20Security%20Agency%20%28CISA%29_Remediated.pdf.

[21] U.S. Cyber Command, "Cyber 101—Cyber Mission Force," November 1, 2022, https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/#:~:text=The%20Cyber%20Mission%20Force%20(CMF,defense%20of%20U.S.%20national%20interests.

[22] Whitney Hughes, "National Guard provides critical cybersecurity for midterm elections," U.S. Army, November 7, 2022, https://www.army.mil/article/261806/national_guard_provides_critical_cybersecurity_for_midterm_elections.

[23] Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce: A Call for Collective Action*, September 2022, 6, https://www.cisa.gov/sites/default/files/publications/State_of_the_Federal_Cyber_Workforce_Report_09.14.2022.pdf.

[24] William Crumpler and James A. Lewis, *The Cybersecurity Workforce Gap*, Center for Strategic and International Studies, January 2019, 1–2, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf.

[25] Federal Cyber Workforce Management and Coordinating Working Group, *State of the Federal Cyber Workforce*, 6.

[26] Scott Rosenberg, "Cybersecurity's public-private salary gap," *Axios*, August 30, 2022, https://www.axios.com/2022/08/30/cybersecurity-public-private-salary-gap.

[27] CISA Cybersecurity Advisory Committee, *Report to the CISA Director: Transforming the Cyber Workforce*, June 22, 2022, 2, https://www.cisa.gov/sites/default/files/publications/June%202022%20CSAC%20Recommendations%20-%20TCW.pdf.

[28] "Part 296 – Maritime Security Program (MSP)," Code of Federal Regulations, Title 46 (2018): § 296, www.govinfo.gov/content/pkg/CFR-2018-title46-vol8/xml/CFR-2018-title46-vol8-part296.xml.

[29] Maritime Administration, "Maritime Security Program," Department of Transportation, last updated August 1, 2022, www.maritime.dot.gov/national-security/strategic-sealift/maritime-security-program-msp.

[30] Econometrica, Inc, *Final Report: Maritime Security Program Impact Evaluation*, Maritime Administration, July 2009, 1-3, www.maritime.dot.gov/sites/marad.dot.gov/files/docs/resources/3776/msprevisedfinalreport-transmitted07-24-09.pdf.

[31] Giddeon N. Angafor, Iryna Yevseyeva, and Ying He, "Game-based Learning: A Review of Tabletop Exercises for Cybersecurity Incident Response Training," *Security and Privacy* 3, no. 6 (November 2020), https://doi.org/10.1002/spy2.126.

[32] For more information on Cyber Storm, see: "Cyber Storm: Securing Cyber Space | CISA." Accessed January 18, 2023. https://www.cisa.gov/cyber-storm-securing-cyber-space.

[33] U.S. Senate, *Civilian Cybersecurity Reserve Act*, S 1324, 117th Congress, introduced in U.S. Senate April 22, 2021, www.congress.gov/bill/117th-congress/senate-bill/1324.

[34] Marie Baezner, *Study on using reserve forces in military cybersecurity: A comparative study of selected countries* (Zurich: Center for Security Studies, April 2020), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-03-military-cybersecurity.pdf.

[35] Angus King and Mike Gallagher, *Cyberspace Solarium Commission*, March 2020, 63, https://www.solarium.gov/.

[36] *Defense Production Act*, U.S. Code 50, §4511, https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter55&edition=prelim.

[37] Defense Production Act Reauthorization of 2003, Public Law No. 108-195, 108th Congress, December 19, 2003, https://www.govinfo.gov/content/pkg/PLAW-108publ195/pdf/PLAW-108publ195.pdf.

[38] Angus King and Mike Gallagher, *Cyberspace Solarium Commission*, March 2020, 63.

[39] U.S. Department of Transportation, *Budget Estimate Fiscal Year 2023: Maritime Administration*, 2022, 5, https://www.transportation.gov/sites/dot.gov/files/2022-03/MARAD_Budget_Estimates_FY23.pdf.

[40] Sara Friedman, "Easterly: CISA plans to move forward with 'systemically important entities' work regardless of legislation," *Inside Cybersecurity*, January 8, 2023.

[41] The cybersecurity insurance industry has had difficulty maintaining current policies, with the Treasury Department looking into ways to shore up the industry. See: Daphne Zhang, "As Cyber Insurance Dries Up, Treasury Department Eyes a Backstop," *Bloomberg Law*, October 7, 2022, https://news.bloomberglaw.com/insurance/as-cyber-insurance-dries-up-treasury-department-eyes-a-backstop.

[42] Josephine Wolff, "Who Pays for an Act of Cyberwar?" *Wired*, August 30, 2022, https://www.wired.com/story/russia-ukraine-cyberwar-cyberinsurance/.

Space As Warfighting Domain

From Education To An Enhanced Global Space Strategy

By Jonathan Bescheron and Pierre Gasnier

Space, one might say, is not as far away as it used to be. From the pioneers and the first technical capabilities of the 1960s to today's increasingly common tweets from Elon Musk about the nth launch of SpaceX, a huge evolution has occurred in the domain. Yet in many ways, it has been so subtle an evolution that few people really consider how their daily life is linked to space.

Missions to the moon, the mining of asteroids for minerals, and visible Internet constellations are but a few examples of how space will dovetail with human objectives over the coming decades. And these examples further illustrate both the expansion of new frontiers and the accompanying, ever increasing stakes in a resurgent, space-centric great power competition (GPC). For while this new "space race" spans economic, environmental, communication, and scientific spheres, its effects are increasingly being felt in the military domain.

Inevitably, due to this rapidly evolving situation, it becomes important to enhance awareness among both military and civilian leaders—current and future—regarding the issues related to the new "space race." To do so, it is necessary to rethink the educational

Lt. Col. Jonathan Bescheron and **Lt. Col. Pierre Gasnier**, both authors are members of the French Air and Space Force.

framework related to space and, accordingly, reform professional military education (PME) to better train leaders in the multiple, interrelated domains of politics, economics, diplomacy, and industry. Once this objective has been reached, states will have a more comprehensive global space strategy, integrating the military component. Additionally, this would enhance cooperation between the defense and commercial space sectors, in turn contributing to reinforcing resiliency and security for both.

This article begins with an overview of the new space environment and the distinctive characteristics of this dual-sector currently facing a marked democratization. However, and despite the very real need to consider the current framework of space-related legal issues and their potential evolution over the coming decades, our focus here will be on PME as it pertains to education regarding space. Once the requisite elements of this revised PME are established, this article will continue by identifying how the French military considers the issue, striving to develop a better understanding of space as a competitive environment, or even a warfighting zone. Finally, we will conclude with a few proposals for attaining space superiority while simultaneously increasing national resiliency.

THE EXPANSION INTO "NEW SPACE"

An Exponential Development: "New Space"

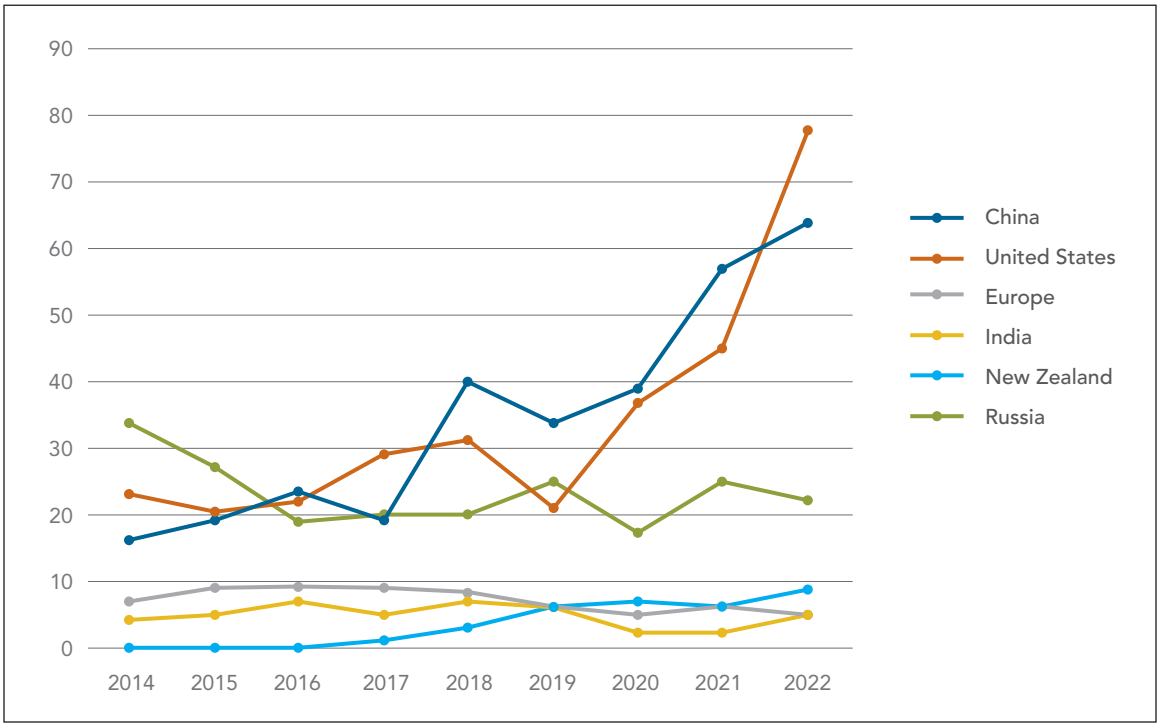
Space has of late become democratized. Access to Low Earth Orbits (LEO) has been simplified with the appearance of less expensive launchers and the emergence of non-state actors (such as commercial industry) meeting military and civilian needs. We have moved far beyond the first conquest missions and now face expanding industrial development worldwide involving a host of new actors.

This emerging commercial space industry—as opposed to government-funded space programs—includes, today, smaller firms as well as the traditional aerospace actors. Focused on developing new technologies and services while increasing access to space, these actors present new perspectives regarding the use of space, including notions such as reusable vehicles and space tourism, all predicated upon reducing costs to increase the use of space. Consequently, the number of satellites has doubled within the last five years and will only continue to increase: according to different space agencies, an estimated 30,000 satellites are predicted to be in orbit by 2030, many dedicated to providing capabilities that improve our everyday lives.[1] This compels us to redefine space as a sort of "commodity" and, further, clearly identify different users—military, industrial-technological, corporate, and civilian—in order to separate the related systems and stakes. Certain political systems in place nowadays keep close watch on space technologies, and the space stakes range now from the globally strategic to the quotidian: positioning systems, international trade markets, intelligence gathering, and scientific research, to name but a few.

As a direct consequence of this democratization, access to outer space (above 50 km in altitude) requires only low-tech tools to attain certain objectives. As an example, newer space actors, such as India and Japan, are now able to launch nanosatellites from relatively simple rockets. Longstanding GPC powers now must deal with such users in this formerly restricted or far less easily accessed area, thus increasing competition between state as well as non-state (private) actors. This "weak against the strong" strategy introduces a new kind of competition, one that threatens direct confrontation along with the more traditional GPC.

The increasing democratization of space is the result of the simultaneous expansion of related sectors, the military and the commercial. Further, today's industrial actors are outpacing government development in the domain, obtaining contracts owing to their greater competitiveness and agility.

Figure 1. Evolution of the number of rocket launches



Dual-Sector Space

Previously, space was managed militarily via national state agencies such as NASA, as governments had both military and scientific/exploratory interests in space. This paradigm generated different schools of thought, each with its own goals and related stakes. "The first one saw space largely in scientific and explorative terms. … The other schools of thought saw the future of outer-space exploration and exploitation in terms of the natural rivalry between societies and states common to history. Space could not be divorced from the political reality of the world."[2]

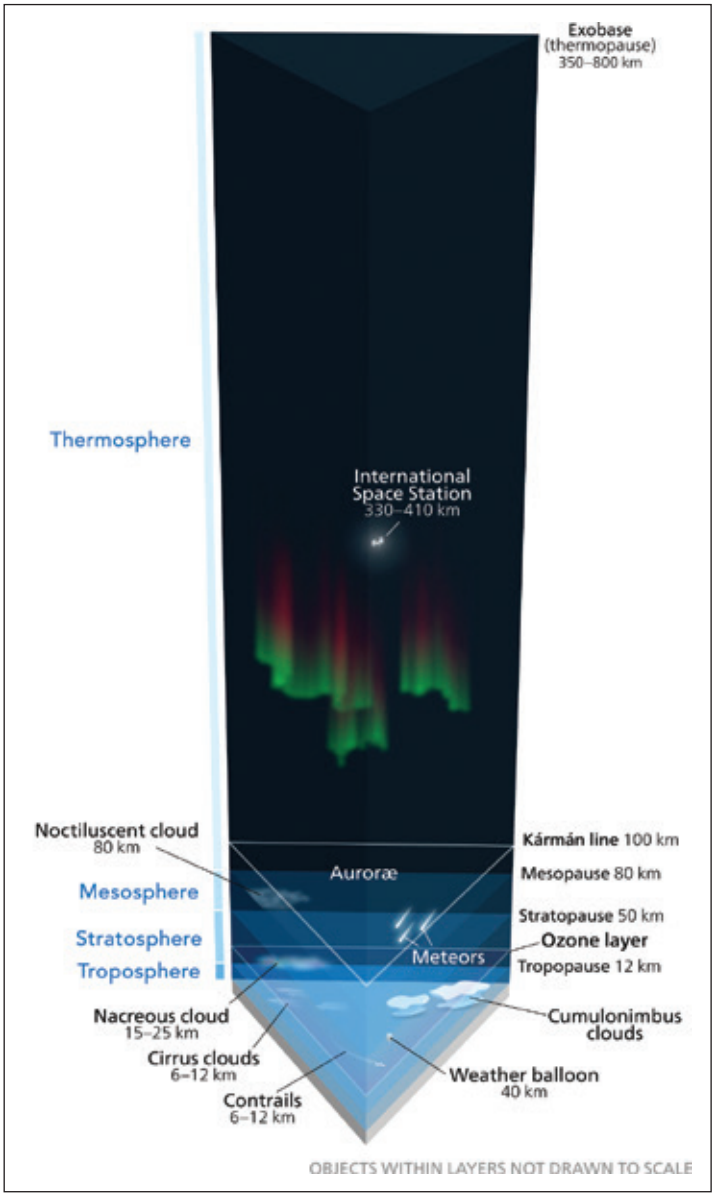
Moreover, during the Cold War, GPC reached its apex between the two blocks led respectively by the United States and the Soviet Union. Ballistic missile development, based on Werner von Braun's V2 program, prioritized both intelligence and deterrence. Thus, the creation of the National Reconnaissance Office (spy satellites), the development of early warning capabilities, and the expansion of GPS as a dual-use PNT technology (Positioning-Navigation-Timing, initially for military yet used worldwide today) are but a few examples of this transition of space technology from state issues to common use. In France, the first Ariane rocket was based on the development of the ballistic missile program. It is now the primary space launcher for national and European interests.

According to the Outer Space Treaty of 1967, outer space is of common interest to all humanity: "The exploration and use of outer space, including the moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind."

As our ancestors did centuries ago with the conquest of the sea, considering superiority at sea to be tantamount to control of the world, the principle of "first come, first served" is de facto applied to space by certain countries, like the United States, of course, but also Luxembourg and the United Arabian Emirates. For such countries, resources in outer space can be exploited according to their own needs and agendas. Indeed, dating to 2015, the U.S. Space Act allows any U.S. citizen to exploit space resources: "A U.S. citizen engaged in commercial recovery of an asteroid resource or a space resource shall be entitled to any asteroid resource or space resource obtained, including to possess, own, transport, use, and sell it according to applicable law, including U.S. international obligations."[3]

Meanwhile, many companies and international organizations are focusing on space and starting new programs or are developing new technologies while improving existing ones. The examples of Space X and Rocket Lab show clearly how states today have come to rely on commercial firms. Yet space can still federate actors around a common cause: many international or private entities, such as the United Nations (UN), are structuring their strategies around space issues. One example, the UN project Space2030, is even considered to be a "driver for peace," advocating for peaceful international cooperation in the domain.

Figure 2. From Earth to deep space - "first in, first served"

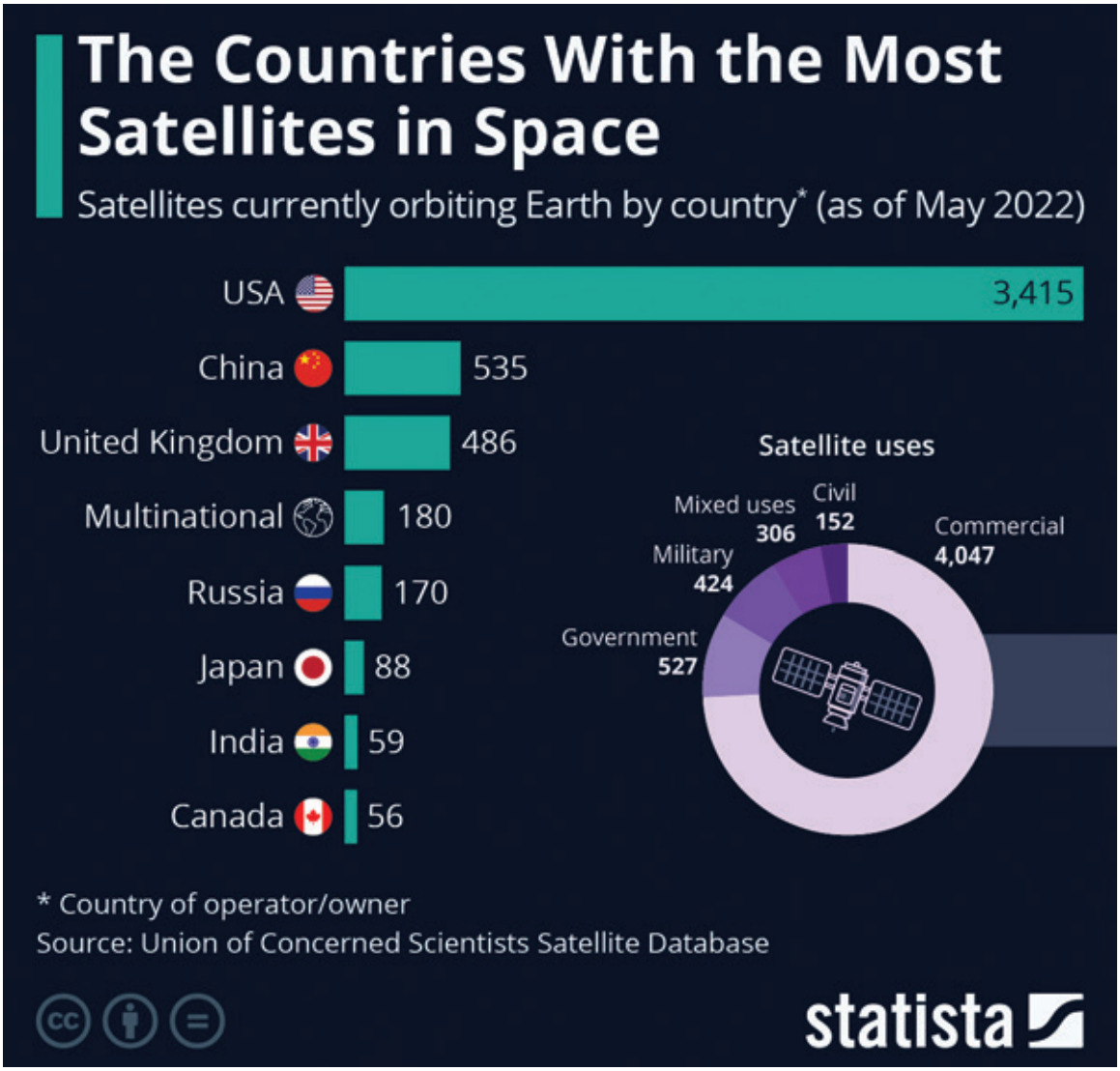


Such oversight or coalition-building has existed since the very beginning of the space race. For example, the International Telecommunication Union has long overseen coordination and allocation of frequency spectrums and orbits in space; although, in actuality, the original GPC countries were the only ones to use the space allocated spectrum for many years. With the development of new actors, resources such as frequencies and orbits

will become rarer; indeed, we are already in an era of increased competition and contestation for the space-relevant spectrum. Worldwide, examples of positioning technologies, such as GPS/Galileo frequency allocation or the privately held Starlinks constellation are well-known. Former U.S. President Donald Trump confirmed this notion of "first come, first served" by Executive Order on 6 April 2020:[4] "Outer space is a legally and physically unique domain of human activity, and the United States does not view it as a global commons."

Furthermore, space resiliency relies today on dual capabilities wherein the commercial space sector is part of military strategy, even for the GPC countries that have a commercial sector. Existing partnerships between NASA/DARPA and SpaceX or

Figure 3. Comparison of the number of satellites by country



between DGA (*Direction Générale de l'Armement*, in charge of the equipment plan of the French forces) and Airbus or Thales illustrate how deep this duality is entwined with resiliency.

An Enlarged GPC

For a long time, only the traditional GPC countries were able to develop space programs. The democratization of space technology, alongside new opportunities presented by this domain and the increased will toward national sovereignty, have encouraged other countries to develop their own space programs. Beyond the Indian and Japanese programs, the United Arab Emirates, for instance, are developing quite ambitious space programs to increase their international reputations as a medium space power. The Hope mission aims directly at Mars and Khalifa satellites provide autonomous Earth observation capabilities. Such medium-sized space powers now can launch, develop, and control satellites.[5]

Another good example of space duality is the Iranian space program based on its ballistic missiles program, designed to enhance Iran's capabilities and gain autonomous access to space for their own satellites. By upgrading their rockets, they increase the range and payload of their ballistic missiles equipped with conventional or, in a likely near future, nuclear warheads. In November 2022, the Iranian government announced the construction of a hypersonic ballistic missile, offering more possibilities and capacities to the Iranian government in the space domain.

Beyond competition between more or less "Great" states, we must not overlook non-state actors able to apply the above-referenced "weak against strong" strategy with potentially devastating consequences on national or international structures. In this context, space appears as a potential new warfighting domain, one central to the defense of sovereignty and the protection of state interests.

Clausewitz saw war as an extension of politics by other means; similarly, this consideration of space as an extension of the warfighting zone must be considered for its geo-political implications. As Florence Parly, former Minister of the French Armed Forces, explained: "…space has become a space of conflict. We must not be naive; we must be able to protect what is vital for the functioning of our transportation systems, our air systems, our hospitals ... and what is essential for the proper functioning of our forces." This is why it is important to differentiate between the warfighting domain and the war zone, from competition to confrontation.

This all-important link between sovereignty and state interests is particularly true in space. In modern warfare, space-based services are essential, controlling and conducting operations; indeed, targeting, communications, and navigation are all reliant on space-based support to varying extents. This was exemplified in 1990 during the first Gulf War, a modern symmetrical conflict, where the massive use of space assets led the U.S. armed forces to victory against the third largest army in the world in only a few weeks.

Accordingly, over the past decades many competitors have developed courses of action to destroy or disable space assets, such as GPS jamming, anti-satellite missiles (ASAT), rendezvous and proximity operations (RPO), and space projectiles. On 24 February 2022, Russia demonstrated that it had mastered such strategies by paralyzing, via cyber-attack, many control terminals of the Ukrainian satellite network just one hour before launching its initial offensive.

Of course, it is also necessary to consider the economic and financial aspects of this new space-related GPC. The development of new space capacities increases competition between states in many tangential sectors, such as the requisite mastery of technologies related to the management of mass data gleaned from observation satellites. The processing

and analysis of such data by means of artificial intelligence is also becoming necessary because of the immense quantity of data being produced and collected. This mastery is closely related to the economic and financial investment capacities of the respective powers, and national sovereignty is at the heart of such issues.

Moreover, growing dependency on space capabilities leads to increased vulnerabilities with replacement of Earth-based capabilities by space-based ones, primarily to cut costs but at the risk of decreased resiliency. Competitors, adversaries, or malign actors can easily identify these vulnerabilities and develop counterstrategies to limit states' operational effectiveness. With space contestation seen in this light, the question arises: what might be the consequences of this on freedom of action within the domain?

As with other environments—land, sea, or air—obtaining and maintaining freedom of action in space seems to be perquisites to countries and actors first establishing, then guaranteeing superiority. The latter superiority entails physical and non-physical lines of communication: space infrastructure, access to space, control and management of orbits, to name but a few; and "lawfare"—a contraction of law and warfare—is at the heart of this freedom of action. While drawing up an exhaustive list of the legal stakes is beyond the scope of this article, we can underline some of the major elements central to such a study.

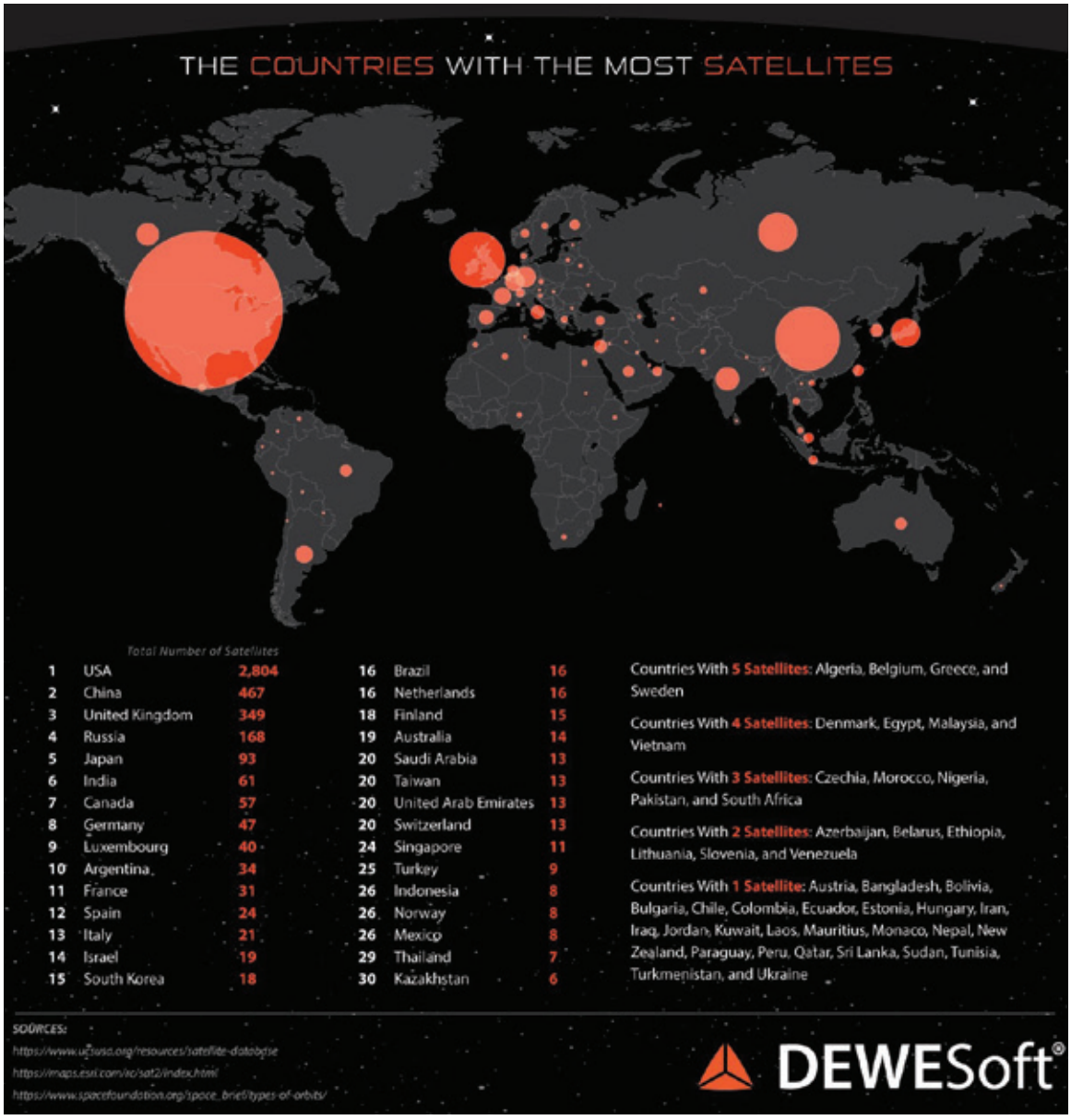
The last treaty on space dates to 1967. Since that time, and as stated above, the use of space has become increasingly democratized and the principle of "first come, first served" governs this domain. This is consistent with strategies underpinning GPC because it does not limit the actions of the (Great) countries concerned. However, for medium power states or those countries that do not have space capabilities, the development of a "lawfare" strategy can be used to influence or obtain rights in the use of space, as predicted by Jonathan Klein in 2019: "The less capable will use their influence to propose international treaties and resolutions to limit the status of the most capable powers." Further, certain new situations underscore the lack of related legislation, and the need for it. For example, what constitutes an offensive maneuver in space? Or, what is the acceptable minimum distance between our own satellites and those of our competitors? Finally, the issue is that states, especially great powers, might be expected to act in what their government or leaders deem that state's best interests.

Both the French Defense Space Strategy and the U.S. Space Force have addressed this topic. The United States perspective is as follows: "We will actively use interactions, consistent with applicable law, to shape norms of behavior that enhance national security and reduce the opportunities for a competitor or potential adversary to misinterpret intentions."[6] The issue also relates to the problem of Space Traffic Management (STM) and the need to establish common rules to ensure the safe use of orbits. These rules may be decided by an international regulator, as the International Civil Aviation Organization (ICAO) has done for aviation. The ICAO serves as an example of successful cooperation, even during the Cold War. In this new space age, regulating the use of space is fast becoming a necessity to safely sharing this domain.

Further consequences on the freedom of action and use of this domain remain to be established, considering the main issue of potential "space area denial" through congestion or saturation by space debris. As explained by Jacques Arnould, "The stakes of the space war, whether it is the war by space, for space or in space, are not only a question of territories and borders to defend, but also a game of interests to preserve, to conquer."[7]

As defined above, the new space must be considered as a set of issues "inherent" to national security. Whether it is a question of space as a venue

Figure 4. Increase of States owning satellites



for national intelligence gathering (e.g., communications, surveillance, navigation) or dealing with space debris—considered an enormous threat to national space capabilities—space is truly changing the competition between states, or powers both great, medium and small. Therefore, the ability of leaders to understand all the issues related to the space environment is becoming increasingly crucial for any actor seeking to attain or maintain its place in this rapidly evolving GPC.

PME AND SPACE EDUCATION: WARFIGHTING DOMAIN AND POTENTIAL WAR ZONE

Space Expertise: from Specialization to Generalization

Space-related expertise was once reserved for those in scientific and engineering fields, as extensive scientific training was required to understand this environment and develop capabilities to exploit it. Of course, possessing a solid knowledge base attained through scientific training remains important owing to the increasing complexity of space and its many (inter)related issues. In the military domain, space capabilities must facilitate the planning and control of operations in all environments, not just in space. The number of trained personnel within the space-related fields must increase to meet this new need. Concurrently, PME must evolve to provide scalable training to match tactical, operational, and strategic requirements at all echelons of the hierarchy. According to General Philippe Lavigne, former French Air Force Chief of Staff, PME must not only keep pace with technical evolutions but also the associated human stakes, "and, in parallel, [requires] conceptual reflection on employment, recruitment, and the establishment of training to meet these needs, and this at all levels."

Originally not widespread, training on space matters within the French military has evolved from a strategy of scientific preparation restricted to a few specialists to the implementation of a shared military culture regarding space. At the same time, the military command strives to develop an environment of trust with space experts, such as those working within universities or industry. The French Air and Space Force has forged a particular link with the third dimension and, beyond, with deep space. The first French astronaut, Jean-Loup Chrétien, was a fighter pilot in the French Air Force; and our most recent astronaut, Sophie Adenot, is a test pilot just recently out of the French War College. Indeed, today all officers of this force undertake space courses in the French Air and Space Force Academy (FASFA).

French Air and Space Force Academy (FASFA)

As in certain U.S. academies, such as the Air Command and Staff College with its Schriever Scholars Program or the West Space Seminar at the Air War College, increased awareness of space can be seen within the FASFA PME programs. The education of French officers is clearly evolving to cover the range of military issues and specialties, providing trainees with general space training, at a minimum, or more scientific and technical training, depending on the career to which they aspire. And while FASFA PME programs used to include space mechanics for all trainees during the first three years at the academy, today's training has been redesigned to cover all officers; meaning, in the French Air and Space Force model, career officers, contracted officers, and internal granted officers.

The FASFA PME courses include a basic, one-day course on space intended for all officers, not only career officers. It covers the Force's current and future capabilities in space, basic notions of space operations—i.e., how space can support other military components—and orbital mechanics. The intent here is to make all officers aware of the key space-related issues regarding their future military assignments: space mobility, space contestation, and space threats, for example. In addition, officer cadets are introduced to space imagery, battle damage assessment, and site surveillance. More advanced courses are available to career officers. These are interspersed throughout the three years of FASFA PME and cover all recruitment profiles, from the scientific to the more literary. During their first year at the academy, student officers take

a three-day Space and Defense Seminar (SPADS), strategizing on space issues and thereby enabling students to better face challenges to space-based service delivery in real-world situations. "Games" are organized to cover many topics: space situational awareness, rendezvous with satellites, and uncontrolled atmospheric reentry of spacecraft back to Earth. Over the course of this seminar, students have the opportunity to not only meet members of the French Space Command and the French Planning and Controlling Operations Center (*Centre de Planification et de Conduite des Opérations*, or CPCO), but also executives from the space industry and the French Study Space Center (*Centre National des Etudes Spatiales*, or CNES). Finally, an entire day of conferences and round tables facilitates discussion on current and future space topics.

SPADS is evolving to integrate North Atlantic Treaty Organization (NATO) participants, such as U.S. Air Force personnel serving as mentors, or joint officers (French Navy or Army), the objective being the creation of a first step toward a joint military-space community. Today, it also aims to prepare a segment of military general officers, sensitizing them to the main space-related stakes—hugely important, given their high level of responsibility within the French military.

Beyond those courses aiming to develop a first level of space competence, Master-level classes enable student officers to delve more deeply into space as a competitive and transversal domain. Significantly, these courses include a period of practical work: For example, students may participate in the development of a ground-space interface or another project done in collaboration with industrial partners such as Thales or Northrup. Master-level courses go far deeper into the space environment, developing knowledge that is more robust, having been developed for a more science-focused population. During the second and third years at the academy, students follow at least 50 hours of space courses, addressing very technical domains such as thermal and optical rules, space engineering, and space environment constraints. These additional hours of courses are divided into three parts:

- Image technology: for instance, how to exploit and improve space imaging via new technologies and artificial intelligence;
- Communications: covering all issues surrounding SATCOM, such as time of visibility, mega-constellations, and antenna centers;
- Roundtables: discussions with space, scientific, and military domain Subject Matter Experts (SMEs) from, for example, ONERA (*Office Nationale d'Etudes et de Recherches Aérospatiales*) for radar, CNES for geolocation, and the French Space Command (PME).

This dedicated space course option eventuates in an end-of-study internship of four to five months. One of the main partnerships is with the United States Air Force Academy, involving studies on space propulsion and space surveillance. This exchange continues a collaboration initiated more than 50 years ago between our two Air Force academies, thus consolidating our ability to operate together in future space operations.

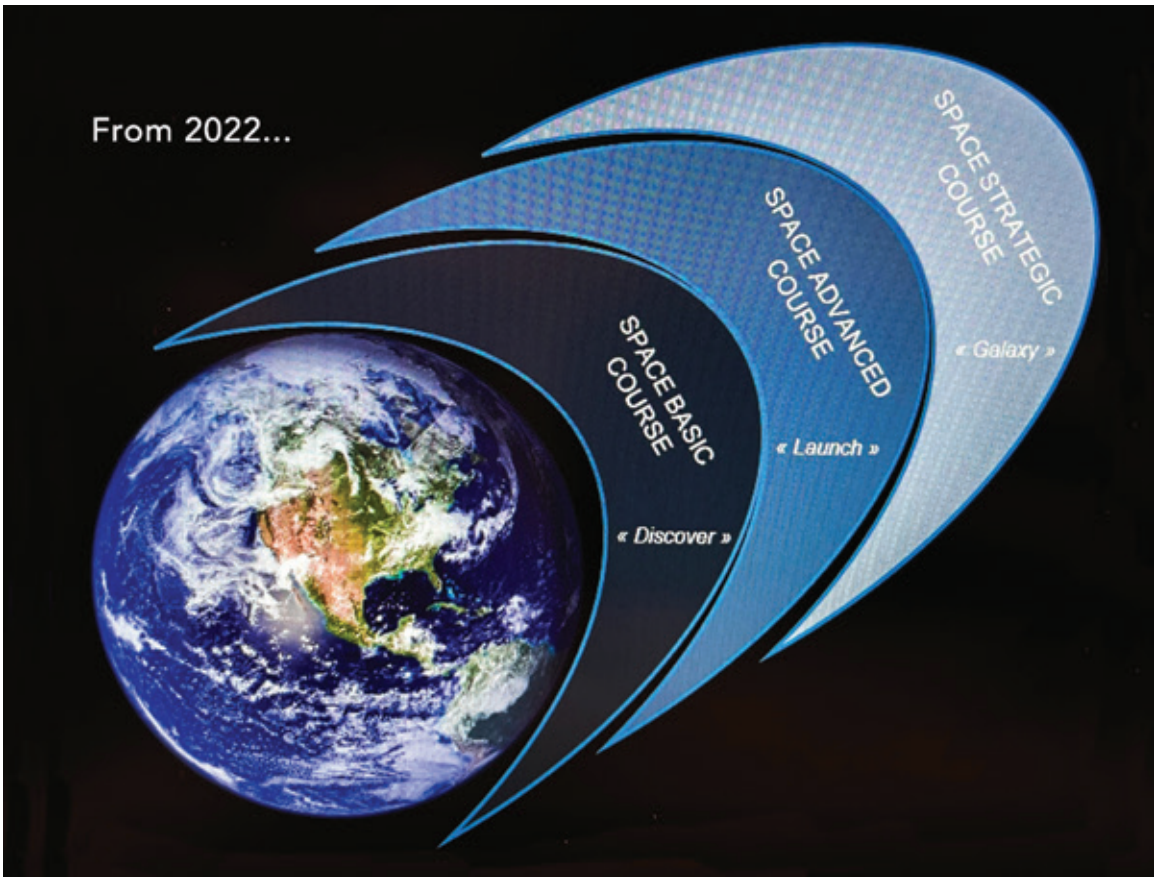
Thus, the French Air and Space Force continues to upgrade its space course program with the objective to instill an initial, more general knowledge of space in its trainees. Different projects remain works-in-progress. For example, a proposed course of study would integrate student officers into a space seminar organized by different French aeronautical schools or academies. Some French military space experts are already involved in this seminar, bringing their expertise to the students of civil engineering. The goal here is: begin integrating into the space community future-facing industrial-military partnerships.

French Space Command

PME is also evolving within the French Space Command, with a dedicated structure in place to educate personnel working on space operations. This training, provided by the Center for Military Space Operations (*Centre de Formation aux Opérations Spatiales Militaires*, or CFOSM), offers three different courses to upgrade trainee comprehension of the space environment: basic, advanced, and strategic courses.

The three-day basic course deals with more general space stakes. The main goal is to provide a global comprehension for people working in support of space operation specialists. The advanced course is at the heart of French PME. Its objective is to give a full spectrum vision of space operations to people involved in this domain. This course is open to all French officers, from each branch, as well as selected specialists from within the foreign office. (The last of these courses, the strategic course, is detailed below). Specialists in specific domains deliver these courses. Many officers of the French Space Command are involved, such as specialists in space operations, legal issues, and space device programs. In addition, civilian specialists are invited to supplement perspectives with their own points of view. For example, CNES personnel might detail the increasingly problematic issue of space traffic management.

Figure 5. What to teach, when to teach - a French space PME project



A MULTI-DOMAIN SPACE EDUCATION

Recent increased awareness of Air and Space Force needs to be reinforced elsewhere, via other PME components. Indeed, neither the Navy nor Army integrate space stakes in their officer academies. At best, those young officers follow a single conference introducing generalities about space. These military academies continue to educate their officers for their first employment at a tactical level where space assets are still considered mere tools used in support of an operation. However, the French Navy is increasing its operational preparation, especially regarding threats such as a space black out. Indeed, assuring resiliency is critical regarding potential space contestation—a failed rendezvous with a French satellite, for instance, could lead to the delay or cancellation of an entire maritime operation.

The French War College aims to prepare future military leaders, especially as regards operative planning. To do so, different planning courses are developed around strategic scenarios to enable student officers to face a global and multi-domain war-game, using NATO Comprehensive Operations Planning Directive (COPD) doctrine, which defines space as a global component (operational domain) in NATO operations through the Allied Joint Doctrine for air and space operations—AJP-3.3. Although these training scenarios integrate the space domain as a supporting component and not as a domain in its own right, they nonetheless allow future military leaders to develop space-relevant skills and ways of thinking within the joint environment of the War College. Meanwhile, the main difficulty remains imagining our future space capabilities during this technological transition phase for the French military: anticipation is constrained by the evolving French space environment, caught between reality and its future objectives.

It is interesting to note that the French War College involves its student officers in French space exercises such as ASTERX23, organized by the French Space Command. Indeed, some students assume operative functions and responsibilities within the space operations center. Their feedback will be worthwhile in developing space expertise at this level. In addition, certain exchange officers are able to follow space courses delivered by the U.S. Air War College in Montgomery, Alabama. Via those courses, they develop and hone their ways of thinking regarding space issues.

For its part, each year the French War College integrates civilian auditors into the different courses it provides. This melting pot enables student officers to expand their minds by dealing with space industry executives on issues of strategy, resiliency, and superiority within their civilian environment. This is an effective way to consolidate space defense culture, a common objective perpetuated via the French IHEDN (Institute for Advanced Studies in National Security) [8] structure. The IHEDN is comprised of officers of the rank of military lieutenant colonel or higher and high-ranking civilian (corporate) executives. Under the command of the French headquarters, IHEDN directly contributes to generating a national defense spirit around French military and industrial skills. Space is one of the Institute's main topics, enabling its civilian and military members to debate these strategic questions.

Concerning space as a joint domain, it is important to prepare military joint leaders to integrate the space stakes into their current and future operations. The French Air and Space Force has recently considered creating a dedicated space profile in its human resources division to generate a pool of experts on space. Creating such a dynamic profile of a career is sure to attract and retain top-level talent.

As we have seen, each aviator takes a dedicated course in the Air and Space Force Academy. The other armed forces consider space at a joint component level, primarily as supporting means; therefore,

their officers only receive education regarding the space stakes once joining specific units or commands related to space. However, the French Navy recently asked the French Space Command to integrate the "space advanced course" during the first part of naval officers' operational careers. In this way, many naval officers will gain a far better understanding of the space stakes.

Beyond being a "supporting" domain for each military component, space is also a supported one. Indeed, a given space operation may require specific component effects to reach its objectives. This means space operations are multi-domain and must be managed at a joint level. In the French military organization, dedicated officers for military space operations are integrated in a "J space cell" at the joint level in the French CPCO. This organization needs military staff able to understand both their specific environment (Army, Navy, Air Force) as well as the space domain. Today, the CFOSM contributes to educating those joint officers, but primarily through "on-the-job" training. Finally, it is interesting to note that today's "J space boss," previously an airman, is now in charge of "informing" the French Chief of Staff on military space stakes via different meetings or written productions.

Still other ways have been developed to consolidate this shared willingness to generate a kind of space community in both military and civilian environments. Indeed, the French Air and Space Force deploys certain of its officers, who might be assigned to the space domain, into prestigious aeronautical French academies to enhance their skill levels in this specific field. For one year, those officers follow in-depth technical training, especially pertaining to space, within renowned schools such as SUPAERO or SUPELEC. Once returned to the Air Force, these officers constitute a real force in making space mastery more efficient. Furthermore, this year of technical space education allows those officers to establish relationships with future civilian space engineers, a network that will only grow in strength and influence over the years.

As far as the political domain and space issues, the French government began showing a greater interest in space in the early 2000's. At this time, some working groups began to list major risks, both real and potential, facing the French state. However, given that all ministries are concerned, this seems to have resulted in a recent change in mindset of the French Secretary for National Security and Defense. This department, under the control of the French Prime Minister, oversees national security and defense issues concerning the various ministries. Today, with space vulnerabilities a major concern at every strategic level, it is paramount to consider the space stakes while clearly identifying the risk matrix for each ministry. For this reason, and to serve this purpose, the Space Affairs Desk was created one year ago to force all ministries to address their weaknesses concerning space issues. This mission is directly linked to the recent French National Resiliency Strategy and will take many months before its work is done. Its work is this: forcing political structures to (re)think space, anticipate issues, and devise strategies that integrate space as an opportunity for success, thereby mitigating the related risks of failure.

PERSPECTIVES ON ATTAINING SUPERIORITY IN SPACE

Defending National Interests: Develop a "Global Strategy"

As mentioned, applications based on satellites are becoming more and more vital for many strategic sectors, and the loss of such capacities could paralyze a country, especially when there are no alternatives. This statement implies the need to integrate space stakes into what General André Beaufre has called a "total strategy."[9] Developed at the political level, this strategy is necessary to design

and prepare for full-scale conflict. This overall strategy is subdivided to encompass four main domains: military, economics, diplomacy, and politics.

In France, only a military strategy is well-developed through the National Strategic Review and the Space Defense Strategy. Stakes identified at the military level should lead to identifying national risks directly linked to space concerns in other departments under the aegis of the prime minister.

Integrate Risks into a Global Risk Management Strategy.[10]

Each French department has a high-ranking official dedicated to defense and the security of its vital infrastructures. However, historically, the law limits their actions to the physical. For example, they can prevent a physical intrusion into a nuclear plant but they cannot legally pursue a cyber-intrusion, according to the French document titled *"sécurité des activités d'importance vitals"* that deals with the security of vital importance activities (SAIV).[11] Thus, an attack against a vital satellite cannot automatically be considered an attack against vital infrastructure, as this would require a more flexible interpretation of "lawfare" issues. The evolution of the SAIV is in progress, attempting to bring French law into line with European law. Nevertheless, according to M. Mario Pain, Deputy Senior Defense Official at the Ministry of Ecological and Solidarity Transition, the risks linked to dependence on the space environment are only beginning to be studied, including, in particular, the consequences of a space "blackout" on the continuity of services.

Raise Space Awareness in all Ministries

Today the comprehension of the space stakes differs greatly between each state agency. Nevertheless, comprehension is the first step in elaborating a dedicated general strategy in each domain—military, economics, diplomacy, and politics—as detailed by General Beaufre. In 2019, the French Space Defense Strategy discussed the creation of a Space Academy to instill space expertise through different kinds of education, and not only for space experts but also for high-ranking managers. According to then Minister of the Armed Forces Florence Parly, "The expertise and training on offer at the Space Academy will be open to interdepartmental partners." This ambitious program entails partnership among the French Air and Space Force Academy, the Space Command, and the renowned *Ecole supérieure d'aéronautique* (an aeronautical engineering school, known as SUPAERO). Unfortunately, this project has been put on hold due to the difficulty in agreeing on the academy model and the mode of governance between these three entities. These difficulties should be rapidly resolved to give future leaders the opportunity to develop a common space culture and, together, envision a general strategy.

PROPOSITION 01: Establish a global matrix focusing on all the national risks linked to the space domain, enabling associated actors to define/redefine an inter-ministry space strategy as part of a global National Resiliency Strategy.

PROPOSITION 02: Resume the French space academy project, possibly by developing new partnerships with our allies (USAFA, for instance), in order to create a base of space-related KSA (Knowledge, Skills, and Abilities) for our future leaders.

DEVELOPING SPACE EXPERTISE

Develop an Interdepartmental Space Education Structure

As General Philippe Adam, Chief of the French Space Command, explains: "This increase in power requires the training of specialists, in association

with our allies, and the development of activities and exercises, such as the space exercise AsterX."

Using National Guard capabilities for Space Force Command may be an interesting way to ease the burden on active forces in those domains. By National Guard capabilities, we mean civilian space experts hired under military status for a specified period. Having a National Guard engaged in space activities would provide the ability to link up with innovative concepts, equipment, and ideas through its private sector members with many years of experience, often gained via careers within the same companies that build space and counter-space systems for states. Alliances can also be formed within this National Guard. These would help establish an environment of trust and help shape a coherent space strategy among allies; or a kind of space alliance to counter opponents' domination initiatives, much like the U.S. Space Partnership Program, or SPP.[12] In France, the National Guard could go further in the recruitment of civilian elites in order to foster knowledge sharing between the French Air and Space Force and the European Space Agency (ESA), consolidating those space centers of excellence previously mentioned. Furthermore, this National Guard status could help maintain a high level of confidentiality for future military space operations. However, it would be necessary to reflect on the prioritization of the employment of such personnel in case of simultaneous needs by the military and the private sector.

In the meantime, CFOSM is developing a strategic space course to fill the gap between expert and generalist training. The first edition is expected in September 2023. Beyond tactical issues, military forces are used to analyze risk and opportunities at the strategic level. The objective of this course is to explain strategic stakes in space to military, industrial, economic, and political leaders. Organized around roundtable discussions, it allows for high-level networking and a shared national understanding of the issues.

The development of a revised PME should thus engender a space community uniting experts and informed leaders sharing a common vision of the space stakes; further, this space community must span, at a minimum, those four domains identified by General Beaufre. Beyond technical expertise, having a "global strategy" in space will require strong political commitment. An understanding of this domain at the political level is a key point that this space community could help implement.

PROPOSITION 03: Develop a space community between military and civilian space structures by developing a National Guard incorporating civilian space experts.

CREATING OPPORTUNITIES FOR INDUSTRY AND COMMERCIALIZATION

As General Charles De Gaulle said in June 1940, "Struck down today by mechanical force, we will be able to overcome in the future with a superior mechanical force." De Gaulle clearly understood the link between industry and operational superiority. Industrial capabilities may also be linked with commerce, trade, and business to build a great economic power that can be used to prepare the armed forces. That is why, following the invasion of Ukraine, President Emmanuel Macron stated his desire to develop a war economy through better cooperation between the defense industry, the financial sector, and the armed forces.

In the new conception of space, many commercial entities are developing new services. The defense environment has the opportunity to develop a "trust circle" to take advantage of this new triptych of innovation: new capacities; resiliency; and subsidiarity. The French Space Command is not yet deeply involved in incorporating the defense industry

into its strategy; therefore, to right this, a dedicated structure was established to keep innovation at the heart of the defense space strategy.[13] Called LISA,[14] the structure's mandate is to ensure, within the ecosystem of national civil actors, dual solutions based on space technologies to meet the needs of the four armed forces. To this end, main actors within the space industry were invited to participate in the space exercise called AsterX, in 2022. This "win-win" partnership provides the opportunity for the military to explain to them the space stakes, such as that maneuverability in space is a pre-requisite to the freedom of action mentioned above, one of Marshal Foch's three principles of war. The role of this Commercial Integration Cell (CIC) could be tailored to take advantage of synergies, both in the technical field and in the conception of space maneuvers.

PROPOSITION 04: Consolidate synergy between military and industrial structures by involving space industries in the military space environment—especially via common space exercises—as participants and mentors.

DEVELOPING RESILIENCY IN COMMAND AND CONTROL

In accordance with its Defense Space Strategy, France will develop defensive and offensive capabilities in space by 2030, based on the ARES[15] major effects program. This will be based on a renovation of the GRAVES and SATAM surveillance systems and the launch of the experimental satellite called YODA,[16] the first steps toward a patrol satellite. Command and control being essential to ensure the efficiency of space operations, the C2 structure will have to evolve to adapt to the challenges of massive data fusion, AI-based decision support, and the need for supercomputers to track and control satellite trajectories.

This evolution will only be possible through reliance on experts trained in the requisite fields. While it is obvious that the defense industry plays, and will continue to play, an essential role, the armed forces will have to be vigilant to ensure the internal operationalization of these systems. The use of an adapted National Guard and the recruitment of commissioned officers in highly specialized fields, such as big data or artificial intelligence, should therefore be prioritized.

Beyond the military domain, President Macron has already tasked his prime minister with elaborating a national resiliency strategy, one that incorporates space resiliency. This inter-departmental project will lead to a better understanding of space dependency through a space blackout exercise and the elaboration of an interdepartmental space doctrine.

In France, space resiliency is quite different from space defense. That is why it is also important to discuss space defense before defining an effective C2 structure. The Department of Defense has the authority to command and control military space operations to defend their own satellites; however, does it also bear responsibility for protecting commercial ones? This is not clear in the written prerogatives defining the Space Defense Strategy. This observation illustrates the need to clarify the legislation governing the action of the state in space. This is also why improvement of the command and control structure is closely linked to this topic. U.S. Space Force General B. Chance Saltzman, Chief of Space Operations, has clearly identified this link by recently stating: "We have a responsibility to secure the space domain to defend U.S. service members in harm's way. … A resilient force is one that can withstand, fight through, and recover from attacks."[17]

The French military has established two higher levels of command: CPCO, considering space as a supporting actor in their joint operations, and the French Space Command, aiming to conduct space operations by requesting joint

support from the other components. It would be interesting to build the operative level of the French Space Command so that it would be able to elaborate space operations, including joint courses of action to achieve shared objectives. In this conception of space operations, the J-space would remain the interface between the Space Force and the Joint Operation Center. Enabling joint actions for a space operation, they would no longer be in charge of the joint effect plan. This transfer of command might well improve the French space command and control process to attain more efficient effects and conduct joint space operations led by space command and control experts.

Additionally, multinational cooperation remains essential to enhance national resiliency and to improve our own command and control structure. Today, this cooperation looks well developed through bilateral and multilateral actions. As was recently seen during the official meeting between President Biden and President Macron, bilateral cooperation with our United States partner is essential to bridge gaps in French space warfare expertise. The United States has a huge advantage in this domain; therefore, the French Air and Space Force, especially via its Space Command, is very interested in involving its officers in space-related PME sharing. The recent JPME partnership between the U.S. Space Force and Johns Hopkins University may be a good opportunity for bilateral cooperation. The main goal of this would be to acquire new abilities and experience through attending courses and participating in space exercises. Today, the National Security Space Institute (NSSI) opens its SPACE 200 course to French students. Upon graduation, they are able to apply operational expertise at the joint level, gaining a far better understanding of resiliency in a contested space environment. In the near future, expanding access to the SPACE 300 course could prove very beneficial in educating senior military officers in charge at the strategic level. Beyond space courses, participation in U.S. space exercises such as the Shriever Wargame would allow French military space experts to gain firsthand experience in space warfare.

Regarding the multilateral environment, France is included in a quorum of "5 eyes and France/Germany" under the Combined Space Operations (CSPO) initiative. This group of participating countries is key in the multi-domain space environment facing high operational, legal, and capacity stakes. It facilitates communications on interoperability through materiel capability and space doctrine. In the contested domain that space is, and will remain, it is also a good way to arrive at shared views on major lawfare issues.

Simultaneously, the implementation of the NATO Center of Excellence (COE) on Space in Toulouse, in the south of France, will be a significant challenge yet will provide opportunities to share experiences and discuss space doctrine. At the same time, the evolution of the AJP 3.3 "Allied Joint Doctrine for Air and Space Operations" is also in progress and may lead to a better comprehension of joint space stakes, especially those based on the expertise of U.S. partners. The evolution of this doctrine is essential to further developing military integration into the space stakes. For instance, AJP 3.3 states the need to understand "how military space operations can be integrated in military operations to achieve alliance security objectives,"[18] yet does not detail how military operations, and other "traditional" components, can also be integrated into military space operations.

PROPOSITION 05: Define a strong space C2 structure, from the strategic to the tactical level. Explain the role of each space entity, especially those among the Space Force (Space combatants, capacities) and Operation Command (Joint strategic effects).

PROPOSITION 06: Reinforce space cooperation within a bilateral (especially U.S./FRANCE) or multinational environment to develop global space doctrine regarding the C2 domain (interoperability) and space education sharing, and to reinforce shared resiliency through space superiority.

CONCLUSION

We have seen the increased stakes inherent in a new space race, whether among the traditional great power competititors or emerging countries. As today's space environment is a dual one, split between national and commercial issues, it becomes all the more important to clearly define the conflicting interests and motivations of the public and private sectors.

Simultaneously, states continue to develop their space strategies, first by establishing new military structures such as space forces or commands, then via the consolidation of Professional Military Education programs. France is not too far behind in this domain and, as a longstanding space pioneer, the country continues building its National Resiliency Strategy, involving all domains and services pertaining to space issues and stakes.

However, France will not be able to meet the major challenges ahead on its own. In fact, no country will be able to do this, hence the importance of continuing existing international alliances while forging new ones, optimizing space structure interoperability and future space operations.

As was recently seen with the Chinese balloon[19] event over the United States, developments both "to and in" space are growing increasingly common and illustrate the need to anticipate every actor impacting space and its raised stakes, whether diplomatic, political, military, or private. Otherwise, traditional actors risk being surprised in this new, high-stakes space competition.

Based on our research as well as extensive discussion with civilian and military experts, we grow ever more convinced of how crucial it is to reinforce our common interests and strengthen our partnerships within space to assure our mutual national superiority.

Prepare leaders, develop joint strategy, consolidate resiliency. PRISM

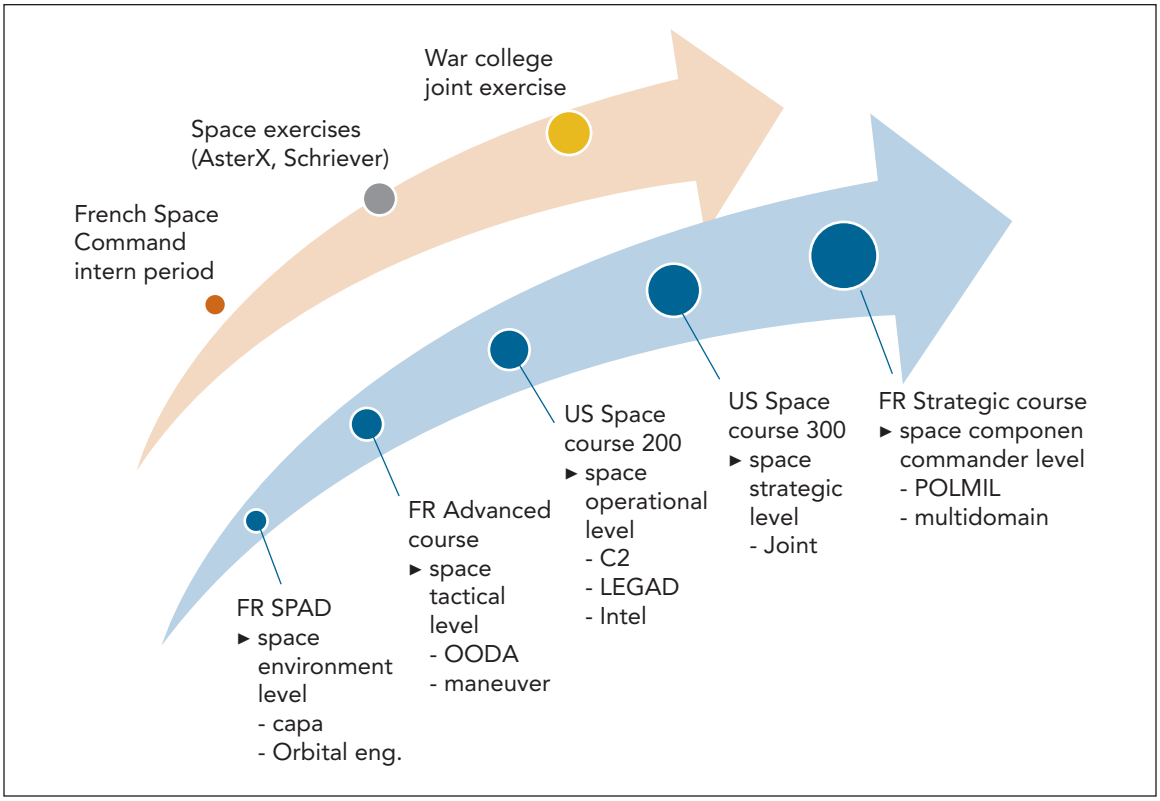
APPENDIX 1 – SUGGESTED SPACE PROGRAM FOR CAREER OFFICERS

As two officers currently finishing our Joint War College studies, we would like to propose here what we envision as a dedicated PME program to prepare and educate future military leaders.

Based on our own tactical and operational experience regarding courses existing today, we have conceived of a sort of space education timeline that we believe would be useful in addressing space issues in war and dealing with the stakes existing around space C2, especially in a joint and strategic environment.

Our paper is, in parallel, based on our own involvement in some of the larger joint exercises the French military has conducted over the last thirty years. For the first time in our military history, a space component was engaged in these operations. As war college students, we have been involved in the different structures of the SPOC (Space Operation Center), from the "combat plan" division to the "combat operation" one. We have learned a great deal regarding domains related to space and we have transmitted much advice, based on our operational experience, to young space experts. The results were remarkable after just three weeks, achieving effective knowledge-sharing dedicated to space operations. We are proud to have taken part in such operations, and to have experienced firsthand the difficulties and issues we have identified in this paper.

Figure 6. Suggested space PME for French career officers



ACKNOWLEDGMENTS

The authors warmly thank the following eminent persons for offering their time and expertise in domains relevant to this paper:

Major General Philippe Pottier, Director of the French War College;

Brigadier General Thierry Auboin, Deputy Director of the French War College;

Navy Captain Christophe Merieult, French SGDSN;

Colonel Guillaume Bourdeloux, French Space Command;

Colonel Pierre Conchon, French CPCO J-space;

Colonel Jérôme D'Oliveira, French Space Command;

Lieutenant Colonel Vincent Lochet, French Space Command;

Navy Commander Alexis Hourlier, French Space Command;

Major Corentin Jimenez, French Air and Space Force Academy;

Major Yann Bidaux, French Space Command;

Captain Béatrice Hainaut, space research specialist at IRSEM;

First Lieutenant Justine Mignonat-Lassus, French Space Command;

Professor Xavier Pasco, director of FRS (French Foundation for Scientific Researches);

Laura André-Boyet, French Air and Space Force National Guard member and astronaut instructor at the European Space Agency;

Yves Préaux, French Naval Academy;

Emilie Cléret, Director of English Foreign language of the French War College; and last but not least, James Reese, English professor.

Notes [Most of these do not contain basic information]

[1] Xavier Pasco, Director of the *Fondation pour la recherche stratégique,* a foundation studying strategic stakes.

[2] Wilson W.S. Wong and James Fergusson, Military Space Power, « A guide to the issues. »

[3] U.S. Commercial Space Launch Competitiveness Act, 25/11/2015.

[4] Jacques Arnould, *La guerre de l'espace aura-t-elle lieu ?* l'Harmattan 2022, 75. Jacques Arnould is a scientist and oversaw ethical issues for CNES.

[5] Deganit Paikowsky, « The Space Club – Space Policies and Politics," paper presented at the 60th International Astronautical Congress, Daejon, Republic of Korea, October 2009.

[6] General John W. Raymond, Chief of Space Operations' Planning Guidance, November 9, 2020, https://media.defense.gov/2020/Nov/09/2002531998/-1/-1/0/CSO%2520PLANNING%2520GUIDANCE.PDF.

[7] Jacques Arnould, Icarus' Second Chance : The Basis and Perspectives of Space Ethics, Springer Vienna, 2011.

[8] *Institut des Hautes Etudes de la Défense Nationale.*

[9] General André Beaufre was a French expert on strategic stakes.

[10] Admiral Rolland, conference at Ecole de guerre, December 2022.

[11] SAIV: Security of vital importance activities

[12] Christopher Stone, Space Partnership Program between the USA and allied countries, The Mitchell Institute for Aerospace Studies.

[13] Colonel Quéant, Chef de la division capacité, Commandement de l'Espace, interviewed in Smart Space. *L'innovation au coeur de la stratégie spatiale de défense* (04 11 2022).

[14] *Laboratoire d'Innovation Spatiale des Armées.*

[15] *Action et Résilience dans l'Espace.*

[16] *Yeux en Orbite pour un Démonstrateur Agile.*

[17] General B. Chance Saltzman, Chief of Space Operation, U.S. Space Force.

[18] NATO, AJP-3.3, Allied Joint Doctrine for Air and Space Operations, Edition B, Version 1, April 2016.

[19] "U.S. declassifies balloon intelligence, calls out China for spying," *The Washington Post* (February 9, 2023).

The Russia-Ukraine Crisis

How Regional Conflicts Impact the Global Economy

By Nayantara Hensel

The conflict between Russia and Ukraine highlights how regional challenges in the military and political environment can lead to global challenges in the economic environment. The negative impact of the war on Ukraine's agricultural, minerals, and energy sectors further demonstrates Ukraine's key role in supplying the global community, as well as the need for collaboration between developed and developing countries in sustaining supply within these key sectors, despite continued tensions.

This article assesses the impact of the conflict on Ukraine's production and exports in the agricultural, minerals, and energy markets and evaluates the success and failure of recent solutions in sustaining Ukraine's important role, including the Black Sea Initiative. It also examines alternative solutions for production and trade, as well as opportunities for further growth. Finally, the article emphasizes the need for international cooperation in maintaining the supply and transport of products from Ukraine's key sectors, which, in turn, reinforces the health of the global community and provides the foundation for global security.

UKRAINE'S AGRICULTURAL SECTOR

Ukraine's Agricultural Exports Prior to the Black Sea Initiative

The conflict between Russia and Ukraine, which began in February 2022, has had a significant impact on the global agricultural market. Almost one-third of global exports of wheat and barley and 75 percent of global exports of sunflower oil are from Russia and Ukraine. Indeed, 400 million people globally rely on Ukrainian food supplies. Unfortunately, the conflict has put a number of countries at risk.[1]

In 2021 Ukraine exported 10.5 percent of global wheat, of which 40.7 percent was exported to African nations and 55.1 percent to Asia. Ukraine's top nations for wheat exports were Egypt (the largest global

Dr. Nayantara D. Hensel is the former Chief Economist for the U.S. Department of the Navy and is the author of *The Defense Industrial Base: Strategies for a Changing World* (Routledge, 2015). She is the Chief Economist and Senior Advisor for Seaborne Defense LLC and is a member of the Secretary of the Air Force's Advisory Group.

importer), Indonesia, Bangladesh, Turkey, Yemen, and the Philippines. Ukraine provided 40 percent of global exports of sunflower oil and seed in 2021, with the top importing countries including India, China, the Netherlands, Spain, and Italy, and exported 12.8 percent of global corn. In recent years, about 60 percent of the European Union (EU)'s corn imports have been from Ukraine.[2]

Prior to Russia's invasion of Ukraine in February 2022, Ukraine exported 6 to 7 million tons of grain per month. By June 2022, Ukraine's exports had dropped to 2.2 million tons. By July 2022, approximately 22 million tons of grain were trapped within Ukraine because of the conflict. Almost one-third of Ukraine's corn production is in areas occupied by Russia, while one-third of its wheat production is in regions that have been affected by the conflict—the regions of Donbas, Zaporizhzhia, Odesa, and Kherson.[3]

Russia and Ukraine had different perspectives regarding why their exports declined with the onset of the conflict. Russia argued that there were obstacles to its grain and fertilizer exports due to banking and shipping industry sanctions from the West, as well as due to the concerns of foreign shipping companies transporting the exports. Consequently, Russia emphasized the need for the lifting of sanctions to supply global markets with grain, although the sanctions did not include food. Ukraine, on the other hand, argued that Russia was damaging its agricultural infrastructure and fields, as well as gaining control of its grain and selling it to Syria instead of Egypt and Lebanon, which refused to purchase it. Russia argued that exports could resume when Ukraine removed the mines in the Black Sea and maritime vessels could be checked for weapons. Concerns regarding whether Russia would resume exports if mines were removed, as well as the degree to which vessels could obtain insurance coverage, were key issues.[4]

Not surprisingly, with the onset of the Russia-Ukraine conflict in February 2022, wheat prices increased by 45 percent during the period of January through March 2022, while the price of vegetable oil increased by over 40 percent and other key substances, such as fish, meat, milk, and sugar, experienced double-digit price increases, which contributed, in turn, to higher global inflation and higher prices in restaurants and grocery stores. Countries such as Spain that import grain for animal feed from Ukraine experienced a 10 percent increase in the price of grain following the first 2 days of the attack on Ukraine by Russia. Fears also rose that export restrictions by countries to protect their domestic supplies would further increase global food prices. Nevertheless, although the Russia-Ukraine crisis caused food prices to increase, other factors also drove the price increases in 2021 and 2022, including poor U.S. and Canadian wheat harvests, the damage from droughts in Brazil on soybean harvests, the impact of droughts in the Horn of Africa, and the impact of significant heat waves on Indian wheat in March 2022.[5]

Impact of the Conflict on Ukraine's Agricultural Farmland

The Russia-Ukraine conflict has had a significant impact on Ukraine's agricultural markets, which—in addition to transportation issues for agricultural exports—has led to a reduction in crops in terms of both planting and storage. Crop reductions were impacted by damaged equipment, as well as shortages in seed, fertilizer, and labor. Indeed, Harveat—one of Ukraine's key agricultural firms—had 98,000 acres destroyed in the Donetsk region, while other agricultural firms, such as AgroGeneration, Kernel, UkrLand Farming, and Agroprosperis, experienced significant financial losses.[6]

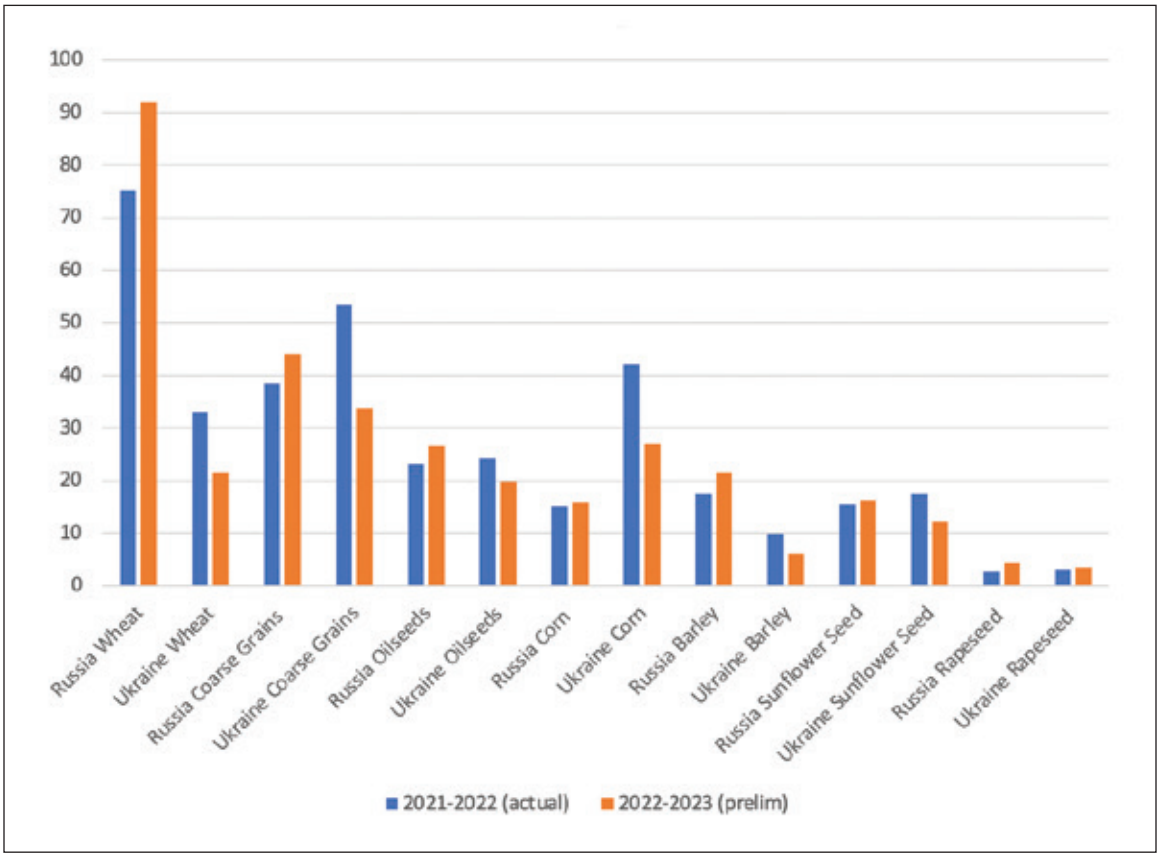
Data from the United Nations (UN) Food and Agriculture Organization (FAO)'s nationwide survey of Ukraine's agricultural sector in January and February 2023 provided insights regarding agriculture in Ukraine, including the front-line

regions in the northeast, east, and southeast. About 93 percent of Ukrainian crop-producing agricultural enterprises experienced higher production costs and almost 90 percent experienced reductions in revenue since the conflict began; over 80 percent of those with higher costs indicated cost increases of over 25 percent. Over three-quarters of livestock-producing agricultural enterprises experienced higher production costs, while over 60 percent experienced declining revenue. The crop producers were challenged by difficulties in accessing fertilizers, seeds, and pesticides, while livestock producers faced shortages in vaccines and feed. Both crop and livestock producers faced challenges in accessing markets and in handling substantial fuel and electricity price increases, which were reflected in the losses and damage of $3.8 billion ($2.71 billion in crops and $1.13 billion in livestock). As a result, nearly 40 percent of the agricultural firms followed strategies of diversifying their businesses and using smaller amounts of fertilizers, pesticides, and seeds, as well as finding different output markets. Indeed, 28.6 million acres of land were planted with grain in 2022, which was a significant decline from 40 million acres in 2021. Moreover, the costs of transportation of grain, which were four to six times greater than prior to the conflict, made grain production more costly such that farmers seeded less. Estimates as of May 2023 suggested that 40 percent less wheat was seeded in 2023 than in 2022.[7]

Agricultural activities were particularly challenging for those dealing with contamination of portions of farmland with unexploded ordnance; this affected 12 percent of agricultural firms. Over 60 percent of the damage occurred in the front-line regions.

Burnt wheat field in Illinivka, 2023-07-17 (Wikimedia Commons).

Table 1. Russian and Ukrainian Agricultural Products



Source: Underlying data from U.S. Department of Agriculture (USDA) Foreign Agricultural Service. "World Agricultural Production," Circular Series WAP 10-23, October 12, 2023, 24, 27, 28, 37, 38. Data is in million metric tons.

Not surprisingly, while almost 8 percent of livestock and crop producers in Ukraine ceased operations, almost 90 percent of them were in the front-line areas. Moreover, various types of agricultural firms experienced closures—for example, between 2021 and 2022, the number of producers of perennial fruit in Ukraine declined by 27.5 percent and the number of pasture-oriented producers declined by 20.4 percent. Front-line regions experienced decreases in grain and vegetable oil crops of 19 percent, compared to the western and central regions, both of which experienced minor increases of 2 percent. Ukraine's southern Kherson province was among the most heavily mined, but it has also been among the greatest areas of Ukrainian wheat production.[8]

Table 1 highlights the reduction in Ukraine's wheat, coarse grains, and oilseed production relative to the growth in Russia's production.

As efforts continued in 2022 to lessen the blockage of Ukrainian exports, much of Ukraine's grain remained in its silos, and concerns increased regarding crowded storage facilities and continued fighting. The destruction of silos in the east and south by the Russian military further depleted the silo capacity from 75 million tons to 60 million tons, of which 20 percent was in areas occupied by Russia.[9]

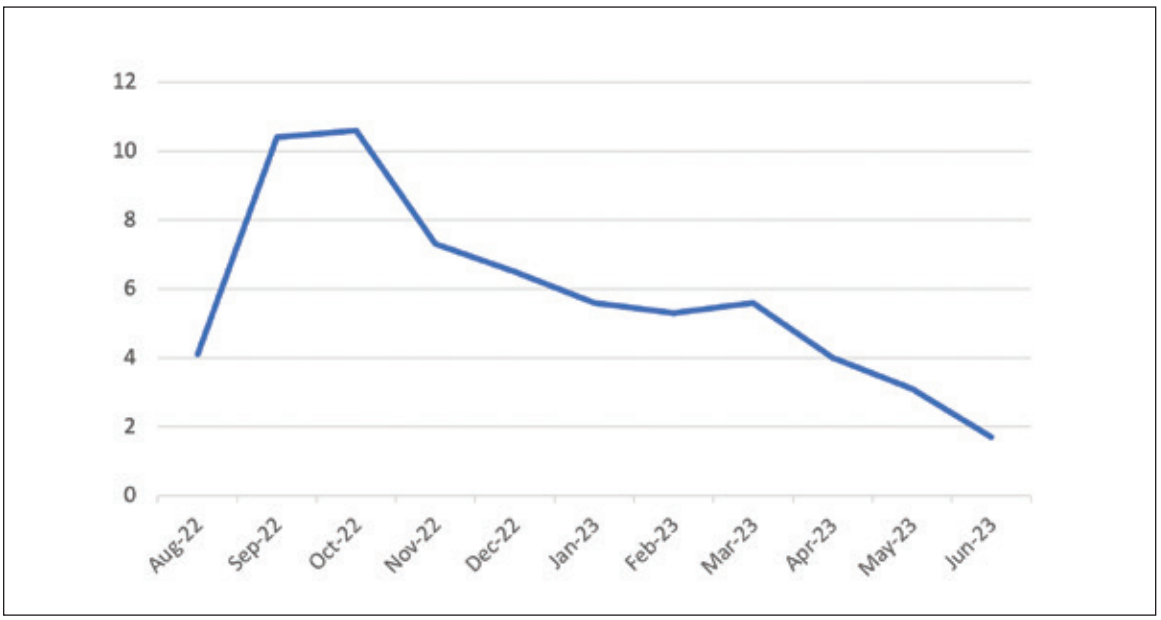
The Black Sea Initiative

With increasing global food shortages and rising prices, the reopening of Ukraine's Black Sea ports to export food was important for the global community. The Black Sea Initiative was signed on July 22, 2022, by Russia and Ukraine, with the UN and Turkey as brokers. It was unusual in that it was the result of cooperation between two intermediaries and two countries in conflict to enable the shipment of humanitarian products, such as food, to countries in need and enabled Ukraine to provide around 32 million tons of food overseas through a Black Sea corridor that was 3 nautical miles in width and 310 nautical miles in length. The Initiative allowed resumption of Ukrainian exports of grain and other foods. The cargo traffic went to and from the Ukrainian ports of Odesa, Yuzhny/Pivdennyi, and Chornomorsk. The initial duration of the Black Sea Initiative, which began on July 22, 2022, was 120 days. It was extended on November 18, 2022, for 120 days, then extended again on March 17, 2023, for 60 days, and, finally extended for a third time on May 18, 2023, for 60 days.[10]

The Joint Coordination Centre (JCC) was created in Istanbul to implement the Initiative. The JCC procedures required incoming vessels to be inspected off Istanbul to make sure that they were empty, then the vessels would traverse the maritime corridor to Ukraine for loading of commodities. The returning vessels would also be examined at the inspection area near Istanbul. Russian naval vessels searched incoming and outgoing ships for weapons at the Bosporus Strait, located at the entrance to the Black Sea. The JCC also handled the safety of the vessels through the monitoring of ships which were in radio communication when in range with Ukraine and Turkey.[11]

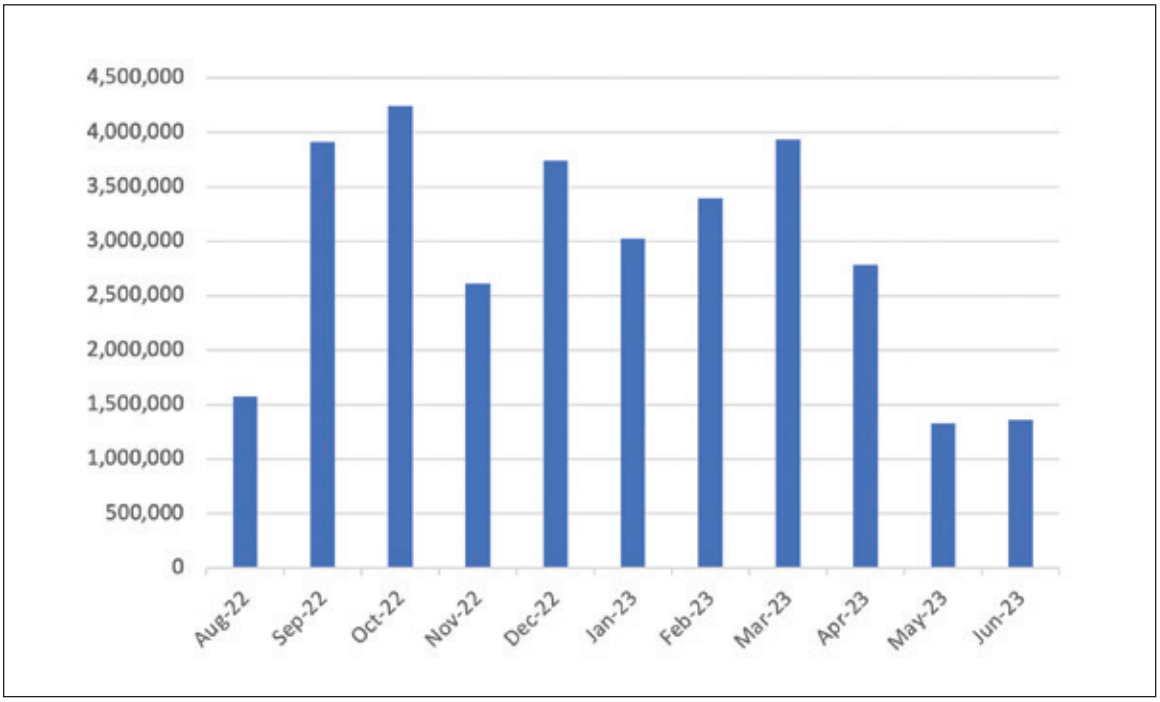
The Initiative significantly increased traffic through the Black Sea to the global community.

Table 2. Daily Average Per Month of Inbound and Outbound Inspections of Ukrainian Vessels inder the Black Sea Initiative: August 2022 to June 2023



Source of underlying data: UN. "Update from the Office of the UN Coordinator for the Black Sea Grain Initiative," June 15, 2023.

Table 3. Ukrainian Exports in Metric Tons Under the Black Sea Initiative: August 2022-June 2023



Source of underlying data: UN. "Update from the Office of the UN Coordinator for the Black Sea Grain Initiative," June 15, 2023.

Shipments began on August 1, 2022 and by mid-September, 3 million tons of grain had been exported by Ukraine while food prices declined. By April 2023, the UN suggested that the prices of food had fallen over the previous 12 months, partially due to the Black Sea grain shipment agreement, as well as to strong harvests in Russia and Brazil. Nevertheless, many countries continued to face high prices and food shortages.[12]

As time passed the exclusion of the port of Yuzhny/Pivdennyi from the Initiative and the longer time spent on inspections led to a reduction in food exports from the ports. The daily average of ships inspected was less than 5 in April, May, and June 2023, down from the daily average of 11 inspections per day in October 2022, as shown in Table 2. Moreover, monthly exports were 1.3 million metric tons in May 2023, which was a significant reduction from the peak of 4.2 million metric tons in October 2022,[13] as shown in Table 3.

In July 2023, Russia suspended the Black Sea Grain Initiative. While fertilizer and foods were exempt from sanctions, Russia wanted to end restrictions on insurance and shipping that had limited its agricultural exports, as well as sanctions on Russia's state-owned agricultural bank. The UN's suggestion of Russia's creation of a subsidiary of Rosselkhozbank, Russia's state-owned agricultural bank, that could use the SWIFT payment system (from which all Russian banks had been disconnected in June 2022) was not acceptable to Russia, which wanted Rosselkhozbank itself be reconnected to SWIFT. Moreover, a number of possibilities for processing Russian payments for fertilizer and food exports through the African Export-Import Bank and JPMorgan Chase did not come to fruition.

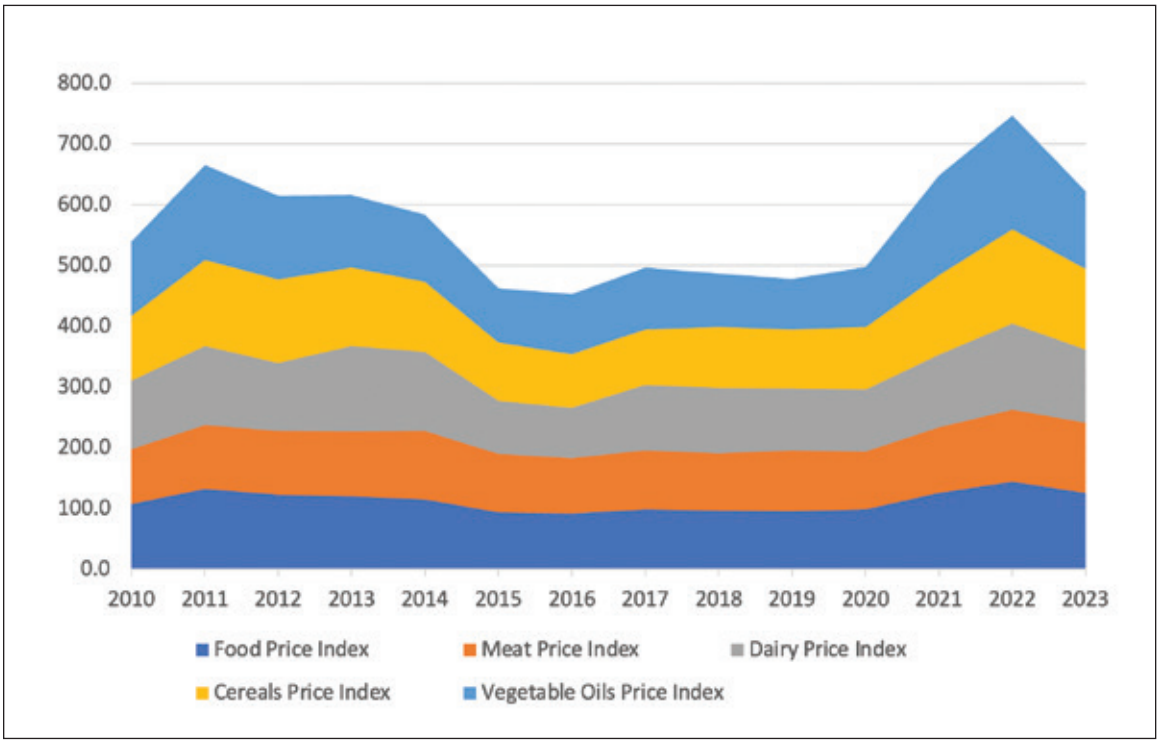
Russia agreed to restart the Black Sea Initiative only if its demands were met. In addition, Russia was concerned that its exports of ammonia—an important fertilizer input—had not begun under the deal; however, the UN argued that this was due to a damaged pipeline.[14]

The Impact of the Initiative

As of mid-June 2023, the Black Sea Grain Initiative had enabled 31,902,478 metric tons of grain and other foodstuffs to be exported to 45 countries from the 3 Ukrainian Black Sea ports. Although Russia argued that the Black Sea agreement supported the economies of wealthier nations, data from the UN's Joint Coordination Centre indicated that 43 percent of Ukraine's food exports went to developed countries and 57 percent went to developing countries, with the top 10 largest importers being (in order): China, Spain, Turkey, Italy, the Netherlands, Egypt, Bangladesh, Israel, Tunisia, and Portugal. The UN data indicated that 17 million metric tons of corn were exported by Ukraine under the Initiative, followed by wheat (9 million metric tons), sunflower meal (2 million metric tons), sunflower oil (2 million metric tons), barley (1 million metric tons), soybeans (1 million metric tons), and rapeseed (1 million metric tons).[15]

Although Russia argued that Ukraine did not export more grain to low-income countries (one of the reasons why Russia indicated that it would not extend the Initiative), data from the Black Sea Grain Initiative indicates that 625,169 metric tons of grain

Table 4. Annual UN FAO Food Price Indices: 2010-2023



Source: Underlying data is from the UN FAO Food Price Indices Data, https://www.fao.org/worldfoodsituation/foodpricesindex/en, released October 6, 2023, and accessed October 17, 2023

were shipped from Ukraine via the World Food Programme to Kenya, Somalia, Ethiopia, Sudan, Afghanistan, and Yemen between July 2022 and mid-June 2023. The World Food Programme had received 80 percent of global wheat from Ukraine due to the Initiative as of July 2023, which exceeded Ukraine's 50 percent share in 2021 and 2022.[16]

Table 4 shows the historical trends in the UN FAO Food Price Indices, including the substantial increase in prices following Russia's invasion of Ukraine, and the decline in food prices with the Black Sea Initiative and with additional global efforts to locate other food sources. By July 2023, when the Black Sea Initiative was terminated, most of the UN FAO Indices showed declines from the signing of the Black Sea Initiative in July 2022—the FAO Food Price Index declined by 11.7 percent, the Meat Index declined by 4.5 percent, the Dairy Index declined by 26.4 percent, the Cereal Index declined by 14.5 percent, and the Vegetable Oil Index declined by 23.1 percent.[17]

Alternative Routes

Despite the increase in key agricultural exports from other countries, Ukraine's agricultural exports have continued to be highly important to the global population. Nevertheless, with the termination of the Black Sea Initiative, Russia no longer provided safety assurances for ships, resulting in the increased potential of Russian strikes on Ukrainian ports or potential detonations of Russian mines located along shipping routes.[18] This section discusses possible solutions to promote Ukraine's export capabilities, including transit by road, rail, or barge along the river to the seaports of other countries.

A key alternative to the Ukrainian ports involved shipments by rail. Ukraine had 12 rail crossings enabling it to transfer goods to Moldova, Romania, Slovakia, Hungary, and Poland. Nevertheless, the difference between Ukraine's broad-gauge tracks (1,524 mm wide) and the narrower gauge used in Europe (1,432 mm wide) made rail transport difficult as freight cars must be switched at the crossing point. Moreover, rail network capacity constraints resulted in more grain remaining in transit countries—Bulgaria, Hungary, Poland, Slovakia, and Romania—rather than being transported to ports for shipping onward. This resulted in their markets becoming oversupplied and contributed to sharp declines in local food prices, with a negative impact on their respective farming sectors. A second alternative involved transit by trucks; however, trucks often faced delays due to the long lines at border crossings.[19]

Since the beginning of the conflict, some Ukrainian products traveled by rail or river barge to seaports. The five ports used for Ukrainian exports were Reni, Izmail, and Cernavoda on the Danube River, and Sulina and Constanta (both Romanian seaports) on the Black Sea. Constanta is the largest Black Sea port; however, increased Ukrainian trade made dock space more limited and put pressure on Romanian facilities, since it was also the primary outlet for grain exports from Slovakia, Hungary, Serbia, Bulgaria, and Romania. About 40 percent of the products shipped out of Constanta arrived via barges from the Danube River, while the remaining 60 percent were transported by road and rail. Izmail, a port in southern Ukraine, is an alternative route to the Black Sea ports. When Ukrainian grain and other exports reached Izmail, they were placed on a vessel which sailed down the Danube River to the Black Sea port of Constanta. By late September 2023, Ukraine had increased its grain exports along the Danube River from Izmail and Reni, with 65 percent of Ukraine's grain exports going through those ports. Nevertheless, the challenges of increasing Ukrainian exports through Romania were also driven by attacks from Russian drones on Ukraine's grain areas near the Romanian border and along the Danube. As of September 2023, Ukraine also began exporting grain through some Croatian ports.[20]

Black Sea shipments from Ukrainian ports no longer continued to be a significant source of Ukrainian exports following the expiration of the deal on July 17, 2023, as Russia declared that vessels heading to the Ukrainian ports would be considered "potential carriers of military cargo and party to the conflict,"[21] stating further that all Black Sea cargo ships destined for Ukraine would be considered military targets. As of September 2023, only two ships with grain exports left a Ukrainian Black Sea port and traveled successfully through Bulgarian and Romanian territorial waters to avoid attacks from Russia.[22]

Russia began targeting Ukrainian ports on July 18 and continued strikes on the 19th, damaging port infrastructure and grain terminals in Chornomorsk and Odesa. Russian attack sites also included key ports on the Danube, such as Reni, where grain silos and hangars were extensively damaged in July, August, and September 2023. Damage from the August attacks temporarily closed Reni. The port of Izmail and Zatoka Bridge, which enabled trucks carrying grain to enter Izmail, suffered multiple drone attacks, including a 3-hour attack on September 7 which damaged significant infrastructure and storage facilities. Attacks on the port of Chornomorsk led to the destruction of 60,000 tons of agricultural products. As of September 2023, over 270,000 tons of grain had been destroyed by Russian attacks on the Danube ports. Not surprisingly, freight rates between Izmail and the Romanian port of Constanta doubled between early July and late August 2023, as did shipping and insurance costs.[23]

Concerns Following the End of the Initiative

When the Initiative ended, global grain prices increased. Some analysts suggested that the suspension of the agreement would result in only a temporary increase in the prices of food products due to the increase in corn and wheat exports by other countries, such as Brazil. Others argued that suppliers outside of Ukraine could experience higher costs for transiting food products to developing countries due to the greater distances in travel which could result in higher food prices for those countries. The termination of the Black Sea Initiative further reduced sources for World Food Programme aid for countries with food shortages, such as Afghanistan, Somalia, and Ethiopia. FAO's July 2023 report noted that 45 countries needed support and food assistance. Fortunately, Brazil produced more corn in 2023, and Argentina and Europe have been expanding their shipments of wheat, which could help to partially balance the decline in Ukraine's grain exports.[24]

In contrast to the demand from developing countries for continued Ukrainian agricultural production, farmers in several EU countries were concerned about Ukraine oversupplying their agricultural markets and reducing their prices and incomes. EU restrictions, which began in May 2023, banned imports of Ukrainian maize, rapeseed, wheat, and sunflower seeds to Romania, Slovakia, Bulgaria, Hungary, and Poland, although the commodities could be exported through their countries to other countries.[25]

The EU Commission decided in mid-September 2023 not to extend its import ban, especially since Ukraine promised to introduce an export licensing system and to exercise export controls. While the five countries were concerned about the impact of food oversupply with Ukrainian products on prices, Romania, which did not have a unilateral ban prior to the EU's initiative in May, planned to wait until Ukraine provided a plan to limit export surges before it put forth a unilateral ban. Hungary, Slovakia, and Poland introduced their own restrictions on imports of Ukrainian grain. In mid-September 2023, Ukraine announced that it intended to sue Slovakia, Poland, and Hungary in the World Trade Organization regarding their bans on imports of key Ukrainian commodities.[26]

While Ukraine has been significantly damaged in food and livestock production, as well as in access to trade routes, there have been some opportunities for continued, but slow, progress in its agricultural sector. Data from the UN FAO indicated that 20 percent of the agricultural workers responding to its survey on Ukraine's agricultural industry received some form of financial support in the previous 3 to 6 months, of which over 50 percent of agricultural producers in the front-line region received some assistance. Indeed, 90 percent of respondents in the Donetsk region and over 50 percent of respondents in Sumska received some aid. Almost two-thirds of the smaller agricultural producers surveyed in Ukraine received cash assistance, and almost 30 percent reported receiving pesticides, fertilizers, seeds, and other agricultural inputs.[27]

UKRAINE'S MINERAL AND ENERGY SECTORS

While Ukraine has historically been a key global producer in the agricultural sector, it has also played a strong role in the global mineral and energy sectors. Despite significant opportunities for further development within these sectors, growth has been limited by the Russia-Ukraine conflicts. This section discusses some of the challenges and opportunities for Ukraine's mineral and energy industries.

Analyses of Ukraine's mineral and energy sectors suggest that 65 percent of Ukraine's coal deposits, 33 percent of its mineral deposits, 42 percent of its metals, 20 percent of its natural gas deposits, and 11 percent of its oil deposits are now controlled by Russia. Russian control of these deposits is partially the result of the current conflict and the 2014 conflict between Russia and Ukraine, and partly from Ukraine's 8-year conflict in the east with Russian-backed separatists. Ukraine has faced difficulties in accessing the southern and eastern regions with significant resource deposits due to the presence of Russian troops. Indeed, between February 2022 and the late summer of 2022, Russia obtained control of a significant number of Ukrainian deposits: 9 oil fields, 14 propane sites, 27 natural gas sites, 41 coal fields, 2 titanium ore sites, 6 iron ore deposits, 2 zirconium ore sites, and 1 site each of uranium, gold, lithium, and strontium, as well as a large limestone quarry used for Ukrainian steel production.[28]

Challenges and Opportunities for Ukrainian Minerals

Ukraine has a significant minerals sector—it has 8,700 surveyed deposits with 117 minerals, with the value of the deposits ranging between $3 trillion and $11.5 trillion. The Ukrainian Geological Survey cited 15 critical metals and minerals of which Ukraine has substantial deposits. These include: lithium, titanium, cobalt, niobium, nickel, beryllium, tantalum, chrome, molybdenum, zirconium, gold, lead, zinc, graphite, and hydrocarbons.[29]

Ukraine mines a number of critical minerals and has continued to do so during the current conflict, although its mining capabilities and global rankings declined between 2021 and 2022 due to the impact of the military conflict in key geographic locations. Indeed, of the 18 minerals that Ukraine mines, 6 of them showed a decline in production ranking. These include: alumina (Ukraine declined from eighth globally in 2021 to sixteenth globally in 2022), clay kaolin (declined from sixth globally in 2021 to ninth globally in 2022), graphite (declined from eighth to thirteenth), manganese concentrate (declined from sixth to seventh), titanium sponge (declined from fifth to sixth), and titanium rutile concentrate (declined from third to fifth). In comparing the 12 critical minerals which were produced by both Russia and Ukraine, Ukraine showed a decline in its ranking of global production in 3 of them, while Russia's ranking in global production declined for only 1 of them—graphite.[30]

Fortunately, however, Ukraine retained its global production ranking for other minerals between 2021 and 2022. Ukraine remained the fifth largest producer of gallium, the sixth largest producer of bromine, the sixth largest producer of iron ore, the seventh largest producer of magnesium metal smelter products, the ninth largest producer of titanium ilmenite concentrate, the ninth largest producer of pig iron, the tenth largest producer of peat, the eleventh largest producer of clay bentonite, the thirteenth largest producer of lime, the fourteenth largest producer of raw steel, and the twenty-first largest producer of salt.[31]

Ukraine has a number of deposits that could provide opportunities for further development. Nevertheless, the locations of the deposits in areas of conflict, as well as the limitations on funding and labor force, have limited expansion.

Titanium

Titanium is a key mineral for Ukraine and is important in construction of planes, ships, machines, and missile technology.[32] Ukraine and Russia are among the seven countries producing titanium sponge. The conflict resulted in Ukraine's titanium sponge production declining from fifth globally in 2021 to sixth globally in 2022, while Russia remained third globally in production.[33] Moreover, Ukraine's titanium exports sharply declined as a result of the Russia-Ukraine conflict; Ukraine experienced an almost 40 percent decrease in titanium exports during January through October 2022 compared to the previous year.[34]

Ukraine, unlike Russia, has been a significant producer of titanium mineral concentrates including ilmenite and rutile. These concentrates are used primarily in producing the titanium dioxide pigment which is found in plastics, paper, and paints. Prior to the 2022 invasion, Ukraine was Russia's primary source of titanium mineral concentrates, which supported Russia's titanium metal industry. Ukraine is tenth in terms of global ilmenite reserves and was ninth in ilmenite production in 2021 and 2022. Ukraine is fourth in terms of global rutile reserves; it tied for third in rutile mine production in 2021 but declined to fifth globally in 2022. Russia is not a significant producer of ilmenite or rutile.[35]

The 32 blocks and fields of titanium ore in Ukraine are in the north, northeast, and south-central regions. Only a quarter of the total reserves in the form of heavy mineral sands deposits are being mined, while the remainder is in hard-rock deposits. Nevertheless, Russia could take over significant portions of Ukraine's titanium industry; in the months immediately following Russia's invasion, two titanium ore sites in Ukraine were seized by Russia. Moreover, prior to the invasion, in 2021, Russian defense companies purchased a 49 percent share in Ukraine's Zaporizhzhia Titanium and Magnesium plant and, in December 2021, the CJSC Ukrainian Chemical Products company sold its titanium plant in Crimea to the Russian company Titan.[36]

Ukraine, however, plans to further develop its titanium industry. The Ukrainian firm Velta announced in May 2023 that it would build a metallic titanium powder plant in the United States and that it intended to build a titanium mining facility in Ukraine after the conflict ends. It is also developing a titanium facility in the Czech Republic. Moreover, the U.S. defense spending bill in 2022 requested that the State Department explore the potential use of Ukraine's titanium.[37]

Steel and Iron

Ukraine, which has the fifth largest reserves of iron ore, remained the sixth largest producer of iron ore and the fourteenth largest producer of raw steel in 2021 and 2022,[38] although steel production declined with the destruction of key Ukrainian steel mills when Russia gained control of Mariupol. Nevertheless, the largest Ukrainian deposit of iron ore in the Kryvyi Rih basin is still under Ukrainian

Azovstal iron and steel works, Ukraine, 27th August 2021 (Wikimedia Commons).

control, despite the shelling. Exports of metallurgy ore declined by almost 60 percent between 2021 and 2022 because of Russia's seizure of key mining operations. During the first half of 2023, Ukraine exported only 2.5 million tons of metallurgical products, in contrast to its exports of nearly 20 million tons in 2021. The main destinations of Ukraine's steel and iron exports are Slovakia, Romania, and Poland, from which they can be further transported.[39]

Graphite

Graphite is important in the production of electric vehicle (EV) batteries, as well as brake linings and other products. Ukraine has the opportunity to become a significant global producer of graphite, as its Zavalievsky deposit is among the largest in Europe, although Ukraine's global production ranking declined from eighth in 2021 to thirteenth in 2022. While there are six deposits of graphite

reserves, currently only one is under production. As of August 2023, Russia had control of two graphite deposit sites, although four other graphite deposit sites remain under Ukrainian control.[40]

Lithium

Ukraine is estimated to hold 500,000 tons of lithium oxide—among the largest deposits in Europe—which is also important for EV batteries. Nevertheless, because of the conflict with Russia, the deposits have not been mined. Ukraine's key sources are in the south central and southeast regions—Polokhivske field and the Dobra block in the Kirovohrad region, as well as two fields which are near/at the front lines of the conflict—Shevchenkivske field in the Donetsk region and the Kruta Balka block in the Zaporizhzhia region.[41]

Rare Earths, Global Phosphate Ore and Co-Products

The deposits of rare earths, which are used in a variety of defense and non-defense products, are in Ukraine's northwest, southeast, and south-central regions. As of August 2023, however, Russia had control of three Ukrainian rare earth deposits sites. The Novopoltavske deposit in southeast Ukraine, which was discovered in 1970, is among the largest global phosphate ore deposits, and it also contains co-products of rare earth elements, tantalum, niobium, and strontium. While there is no extraction of the significant sand and hard rock deposits of scandium and zirconium, which are also co-products, the six deposits of beryllium, tantalum, and niobium have some non-commercial production in the Malyshevske and Vovchanske fields in southeast Ukraine.[42]

Zinc, Lead, and Polymetallic Deposits

Although Ukraine does not have production plants for zinc, copper, and lead concentrates, it does extract zinc, lead, and their alloys through metallurgical processing of materials containing lead. Zinc and lead reserves are largely located in polymetallic deposit ores. The polymetallic fields and blocks are in the southwest and south-central/southeast regions of Ukraine. Production is carried out in the Muzhiyivske field in southwest Ukraine, although there are seven fields. Twenty-year licenses for exploration and production have been for sale through e-auctions.[43]

Additional Key Minerals

Ukraine has deposits of a number of other key minerals but with only limited domestic production. Among Ukraine's estimated reserves of other important minerals are: cobalt (8,800 tons), chromium oxide (453,000 tons), and nickel (215,000 tons), as well as measured/indicated resources of copper (95,000 tons) and chromium oxide (3.1 million tons). A significant share of explored and potential areas of nonferrous metals is in the Ukrainian Crystalline Massif and in the northwest and south-central regions. Although Ukraine does not currently produce copper, the Ukraine Volyn, Zhytomyr, and Rivne regions have 150 copper deposits. In addition, Ukraine has 12 silicate nickel fields that contain cobalt.[44]

Potential Solutions for Development of Ukrainian Minerals

Despite the challenges faced by Ukraine in its conflict with Russia, Ukraine has significant opportunities in raw materials in key regions that can be further developed with increased funding and through collaboration with other countries. Ukraine signed a Memorandum on Strategic Partnership in the Raw Materials with the EU in July 2021, which increased the confidence of global mining companies to begin applying for exploration permits. In late 2021, Ukraine began auctioning exploration permits for reserves of lithium, nickel, cobalt, and copper. In December 2022, Ukraine passed legislation to increase interest in developing its

mineral industries. In addition, for the first time, the European Raw Materials Week in November 2022 included representation of Ukraine, and the European Commission and Ukraine held a forum for investors to discuss opportunities in the mining sector. Furthermore, Ukraine held another investment forum at the Ukrainian Recovery Conference in London in June 2023. Ukrainian President Volodymyr Zelensky has encouraged foreign investment in Ukraine through the Advantage Ukraine project, which, as of February 2023, had resulted in $9 billion in investment and 50 feasible investment projects in energy and mineral fields.[45]

CHALLENGES AND OPPORTUNITIES FOR THE UKRAINIAN ENERGY SECTOR

Ukraine has significant deposits in the energy sector; however, the development of mining and production has been limited by the conflict with Russia. Key portions of areas with energy resources are in southern and eastern Ukraine, which are at risk from Russia's invasion or are under Russian control. These areas contain 72 percent of Ukraine's natural gas, 50 percent of its oil, and most of its reserves and production facilities for coal. The bulk of Ukraine's hydrocarbon reserves are in the Carpathian region in the west, the Dnieper–Donetsk region in the east (which produces 90 percent of Ukraine's natural gas), and the Black Sea–Sea of Azov region in the south (which produces 10 percent of natural gas). Although Ukraine began a significant oil and gas privatization program in 2013, the plan was severely limited by Russia's annexation of Crimea in 2014, as well as by military conflict in the Donbas region.[46]

Natural Gas

Ukraine has the second largest proven gas reserves in Europe at 1.1 trillion cubic meters (tcm)—a 0.6 percent share of global gas reserves. Russia, however, has 13.6 tcm of natural gas, which is 7.2 percent of global gas reserves. Nevertheless, four-fifths of Ukraine's reserves are east of the Dnieper River, which runs through the center of the country,[47] and are thus at risk due to the conflict.

About 30 percent of Ukraine's domestic gas consumption comes from imports. While Ukraine had historically imported much of its natural gas from Russia, Ukraine ceased natural gas imports after Russia annexed the Crimean Peninsula and has been importing natural gas from other European countries.[48]

Approximately 70 percent of Ukraine's domestic natural gas consumption comes from its own natural gas production. Although Ukraine and Russia have global shares of natural gas production of 0.4 percent and 15.3 percent, respectively, it is not surprising that both Ukraine and Russia experienced declines in natural gas production between 2021 and 2022 of 6.6 percent and 11.9 percent, respectively,[49] due to the EU shifting away from Russian gas, the impact of the Russian conflict on Ukraine, and pipeline issues.

Ukraine plays an important role in transiting Russian energy exports to Europe. While Russia's use of Ukrainian pipelines provides Ukraine with transit fees, it also may have provided Ukraine with some protection against airstrikes. Ukraine has the largest global natural gas transit infrastructure. As of 2021, Ukraine's transportation network of natural gas included 13 underground storage facilities (the second-greatest storage capacity in Eurasia and Europe, with Russia having the greatest) and 28,000 miles of pipeline. The traditional pipeline systems passing through Ukraine are the Bratstvo (Brotherhood) pipeline, which travels through Ukraine to Slovakia, then divides into two directions to provide natural gas to nations in northern and southern Europe; the Soyuz (Union) pipeline, which connects Russia's pipelines to central Asia, as well as providing exports to countries such as Slovakia, Hungary, and Romania; and the

Trans-Balkan pipeline, which traverses Ukraine from Russia to Turkey and Balkan countries.[50]

The Ukrainian gas transmission system enabled Moldova and six EU countries to obtain Russian gas between July 2022 and June 2023. Fifteen billion cubic meters of natural gas (on an annualized basis) transited through Ukraine during the first half of 2023, of which 12 bcm (annualized basis) was transported to the EU and 2.6 bcm was transported to Moldova. In contrast, an average of 90 bcm annually was transported through Ukraine between 2008 and 2019. Austria obtained the greatest volume of 5.1 bcm of Russian gas through the Ukrainian corridor, followed by Italy (3.5 bcm), Moldova (2.2 bcm), Slovakia (1.8 bcm), Hungary (0.5 bcm), Croatia (0.4 bcm), and Slovenia (0.2 bcm). Not surprisingly, however, the volumes on the Ukrainian gas pipelines decreased between July 2022 and June 2023, partially driven by Russia's curtailment of supply due to political tensions, fewer gas shipping requests from European customers along the route, greater use of the TurkStream corridor by countries such as Hungary, and issues with payment by countries such as Moldova.[51]

Concerns have arisen regarding the use of Ukrainian gas pipelines because of political tensions. In December 2019, Russia's Gazprom, the Gas Transmission System Operator of Ukraine (GTSOU), and the Ukrainian gas company Naftogaz signed a 5-year contract for Russian gas to transit through Ukrainian pipelines. Although Gazprom initially paid the fees based on the transit volumes under the contract, GTSOU and Naftogaz began an arbitration against Gazprom before the International Court of Arbitration in September 2022 due to Gazprom not continuing to pay the fees. Not surprisingly, the actual gas volumes were lower relative to the volumes under contract: contract volumes were 65 bcm in 2020 and 40 bcm each year for 2021 through 2024, while the actual volumes declined from 55.8 bcm in 2020 to 41.6 bcm in 2021 to 19 bcm in 2022.[52] GTSOU also halted the flow of gas through Sokhranivka in May 2022, which was one of two Ukrainian entrance locations for Russian gas transiting through Ukraine, arguing that Ukraine had little control over the physical infrastructure in areas occupied by Russia, and expressing additional concerns regarding gas theft issues. Trade flows through Sudzha, the other entrance location, remained fairly stable during the second half of 2022, with some changes driven by Gazprom's European customers.[53]

The role of the Ukrainian pipelines in Russian gas transport faces additional challenges. First, the vulnerability of significant areas in which the Ukrainian gas pipelines and compressor stations are located due to military strikes is a key issue, as well as the impact of the potential Russian capture of Sudzha, the only operating Ukrainian pipeline entrance location. Second, Russian gas shipments through Ukraine could be halted either by Russia or Ukraine in retaliation against attacks or perceived offenses. Third, Russia's threat of sanctions against Naftogaz could become reality, due to Naftogaz's initiation of arbitration proceedings.[54]

If the contract were not renewed in 2024, European countries would only be able to receive Russian gas through the TurkStream entry point at Strandzha, which would significantly reduce EU gas imports and could lead to higher gas prices and further disruptions. While Russia had hoped that the NordStream 2 pipeline would replace gas transit through Ukrainian pipelines, Nordstream 1 and 2 were damaged in September 2022 and are not operational.[55]

The nonrenewal of the contract would result in Ukraine losing its transit revenues from Russian gas unless it finds new opportunities for transit volumes. Naftogaz's CEO emphasized the need for European countries to reduce their consumption of Russian gas and highlighted the importance

of alternative uses of Ukraine's significant gas transmission infrastructure, storage facilities, and reserves in supporting EU countries.[56]

European countries have planned to reduce Russian gas imports by further developing their own liquefied natural gas (LNG) terminals (e.g., Germany), as well as obtaining LNG imports from other countries (such as the United States and Qatar). In addition, many of the countries receiving gas flows through Ukrainian pipelines have significantly greater import capacity through alternative routes, as well as opportunities to switch fuels or receive gas from neighboring countries.[57]

Oil

Although, as of 2021, Ukraine had 400 million barrels in proven oil reserves, Ukraine largely imported petroleum from Belarus, Russia, and Germany. Ukraine has one refinery—the Kremenchug facility—which uses crude oil imported from Kazakhstan and Azerbaijan.[58] Ukraine's oil refinery throughput has decreased significantly over the years—in 2011, its throughput was 206,000 barrels daily; by 2013, it was 85,000 barrels daily, and by 2022, it had dropped to 53,000 barrels daily. Ukraine's oil refinery throughput, which had a global share of 0.1 percent in 2022, declined between 2021 and 2022 by 26.7 percent, while Russia, which had a global share of 6.8 percent in 2022, declined by only 3.3 percent.[59]

Ukraine's main role in the oil sector is as a transit source for Russia's exports of crude oil through the southern branch of the Druzbha pipeline to the Czech Republic, Hungary, and Slovakia. In 2022, Russia transported 300,000 barrels of oil per day via the Druzbha oil pipeline, providing Ukraine nearly $180 million in transit fees from the pipeline. Other Ukrainian pipelines transiting crude oil include the Samara-Lisichansk pipeline and the Nizhnevartovsk-Lisichansk-Kremenchuk-Odesa pipeline.[60]

Coal

In 2020, Ukraine had the sixth-largest global coal reserves (3.2 percent of global reserves). Although it has 151 operating mines, its coal production has declined significantly over the years. In 1985, Ukraine produced 170 million tons annually; by 2005, production was down to 61.4 million tons, and, by 2015, it produced 30.4 million tons.

The seizure of coal between 2014 and 2017 by Russian-backed separatists in eastern Ukraine led to Ukraine importing more coal. While Ukraine imported only 20 percent of its coal in 2010, its coal imports increased to about 45 percent by 2019. With the conflict with Russia beginning in 2022, Ukrainian coal production further declined, from 24.9 million tons in 2021 to 16.5 million tons in 2022.[61]

Prior to the 2022 conflict, the bulk of coking and thermal coal production in Ukraine occurred at the Lviv-Volyn Coal Basin in west Ukraine, the Donetsk Coal Basin in east Ukraine, and the Dnieper Coal Basin in central Ukraine. Nevertheless, about 30 billion tons of hard coal deposits with a value of $11.9 trillion are in areas controlled by Russia, including nearly 80 percent of Ukraine's coal deposits and all of its black coal (anthracite).[62]

Potential Solutions for Hydrocarbons

Despite the challenges faced by the conflict with Russia, as well as shortages in funding, Ukraine has continued to expand its hydrocarbon areas. In addition to relaunching the Yuzivska shale gas site in eastern Ukraine, Ukraine e-auctioned 11 concession licenses between 2020 and 2022. It also plans to stimulate the western areas by relaunching the hydrocarbon Oleska area and further exploring the Volyn-Podillya petroleum area. Ukraine also has a large unexplored "Dolphin" natural gas deposit off Ukraine's southern coast in the Black Sea, in addition to another large natural gas deposit in the western region of Ukraine's Carpathian Mountains.[63]

CONCLUSION

The impact of the Russia-Ukraine conflict on the global economy highlights how regional challenges in the military and political environment can lead to global challenges in the economic environment. The interlinkages between developed and developing countries in key sectors—agriculture, minerals, and energy in particular—emphasize the need for collaboration between countries in the wake of increasing supply constraints due to these rising tensions.

Ukraine's traditional agriculture, mineral, and energy assets meet important global needs. Nevertheless, historic and current tensions with Russia have limited Ukraine's ability to sustain and further develop its production in these key sectors, which has had a significant global impact. The conflict has led to the destruction of Ukrainian farmland; severe limitations on its transport through Black Sea ports; challenges in transporting products through rivers, highways, and non-Ukrainian ports; the capture of important mineral and energy deposits; the lack of funding and safety for further development of deposits; and reduced current and future opportunities for use of Ukraine's vast natural gas transit infrastructure.

Despite these challenges, Ukraine has attempted to find solutions to maintain its critical role in the global economy. In an effort to export at least a portion of its agricultural products following the termination of the Black Sea Initiative, Ukraine has increased transit along rivers to Romanian ports and continued rail and truck transit to other countries. It has continued to emphasize exploration and mining of key minerals through collaboration with the EU to stimulate investor funding, has engaged in auctioning concession licenses for energy deposits, and has assessed alternatives for its natural gas transit infrastructure and gas storage capabilities if the agreement with Russia is not renewed.

In conclusion, the challenges from this conflict emphasize the importance of the key resources of particular countries on global health and economic welfare. It further highlights the need for continued collaboration between countries in providing investments to vital sectors, as well as in supporting trade routes to transmit important products to the global community. Greater cooperation between countries can help to sustain global populations and industries, which, in turn, provides the foundation for global security. PRISM

Notes

[1] Chan, Kelvin, and Paul Wiseman. "How did Russia-Ukraine war trigger a food crisis?" *AP News,* June 18, 2022.

[2] Maciejewska, Agnieszka, and Katarzyna Skrzpek. "Ukraine Agricultural Exports—What is at Stake in the Light of Invasion." *S&P Global Market Intelligence*, March 7, 2022; Wilson, Joseph, Samy Magdy, Aya Batrawy, and Chinedu Asadu. "Russian war in world's 'breadbasket' threatens food supply." *AP News*, March 6, 2022.

[3] Arihova, Hanna. "Anxiety grows for Ukraine's grain farmers as harvest begins." *Associated Press*, July 10, 2022; Muggah, Robert. "Russia's Resource Grab in Ukraine." *Foreign Policy*, April 28, 2022.

[4] Chan, Kelvin, and Paul Wiseman. "How did Russia-Ukraine war trigger a food crisis?" *AP News*, June 18, 2022.

[5] Chan, Kelvin, and Paul Wiseman. "How did Russia-Ukraine war trigger a food crisis?" *AP News*, June 18, 2022; Wilson, Joseph, Samy Magdy, Aya Batrawy, and Chinedu Asadu. "Russian war in world's 'breadbasket' threatens food supply." *AP News*, March 6, 2022.

[6] Muggah, Robert. "Russia's Resource Grab in Ukraine." *Foreign Policy*, April 28, 2022.

[7] Food and Agricultural Organization of the United Nations. "Ukraine: Impact of the War on Agricultural Enterprises," 2023. https://www.fao.org/documents/card/en/c/cc5755en; Kullab, Samya. "Ukraine farmers surrounded by risks, from mines to logistics." *Associated Press*, May 7, 2023.

[8] Food and Agricultural Organization of the United Nations. "Ukraine: Impact of the War on Agricultural Enterprises," 2023. https://www.fao.org/documents/card/en/c/cc5755en

[9] Chan, Kelvin, and Paul Wiseman. "How did Russia-Ukraine war trigger a food crisis?" *AP News*, June 18, 2022; Arihova, Hanna. "Anxiety grows for Ukraine's grain farmers as harvest begins." *Associated Press*, July 10, 2022.

[10] "The Black Sea Grain Initiative: What it is and why it's important for the world." *UN News*, September 16, 2022; "Ukraine grain deal: why is Russia pulling out?" *TodoBooking News*, July 17, 2023; "How is Ukraine exporting its grain now the Black Sea deal is over?" *BBC News*, September 26, 2023; Bonnell, Courtney. "Why allowing Ukraine to ship grain during Russia's war matters to the world." *AP News*, July 15, 2023; "One year of the Black Sea Initiative: Key facts and figures." *UN News*, July 10, 2023.

[11] "The Black Sea Grain Initiative: What it is and why it's important for the world." *UN News*, September 16, 2022; "Ukraine grain deal: why is Russia pulling out?" *TodoBooking News*, July 17, 2023; "How is Ukraine exporting its grain now the Black Sea deal is over?" *BBC News*, September 26, 2023; UN, "Update from the Office of the UN Coordinator for the Black Sea Grain Initiative," June 15, 2023.

[12] "The Black Sea Grain Initiative: What it is and why it's important for the world." *UN News*, September 16, 2022; Wiseman, Paul, and Evelyne Musambi. "Food prices fall on world markets but not on kitchen tables." *AP News*, April 27, 2023.

[13] "One year of the Black Sea Initiative: Key facts and figures." *UN News*, July 10, 2023.

[14] Bonnell, Courtney. "Why allowing Ukraine to ship grain during Russia's war matters to the world." *AP News*, July 15, 2023; "Ukraine grain deal: why is Russia pulling out?" *TodoBooking News*, July 17, 2023.

[15] UN, "Update from the Office of the UN Coordinator for the Black Sea Grain Initiative," June 15, 2023; "How is Ukraine exporting its grain now the Black Sea deal is over?" *BBC News*, September 26, 2023; Bonnell, Courtney. "Russia halts landmark deal that allowed Ukraine to export grain at time of growing hunger." *AP News*, July 17, 2023; "One year of the Black Sea Initiative: Key facts and figures." *UN News*, July 10, 2023; data from UN Black Sea Grain Initiative Joint Coordination Center Data, accessed October 16, 2023.

[16] "Ukraine grain deal: why is Russia pulling out?" *TodoBooking News*, July 17, 2023; "One year of the Black Sea Initiative: Key facts and figures." *UN News*, July 10, 2023.

[17] Underlying data from the UN FAO Food Price Indices Data, accessed October 17, 2023.

[18] Bonnell, Courtney. "Russia halts landmark deal that allowed Ukraine to export grain at time of growing hunger." *AP News*, July 17, 2023.

[19] "The bottlenecks on alternative routes to export Ukrainian grain," *BBC News*, July 21, 2022. "Ukraine grain deal: why is Russia pulling out?" *TodoBooking News*, July 17, 2023; Kullab, Samya. "Ukraine farmers surrounded by risks, from mines to logistics." *Associated Press*, May 7, 2023; Arihova, Hanna. "Anxiety grows for Ukraine's grain farmers as harvest begins." *Associated Press,* July 10, 2022.

[20] "How is Ukraine exporting its grain now the Black Sea deal is over?" *BBC News*, September 26, 2023; Dumitrache, Nicolae. "US, Europe eyeing ways to improve Ukraine's grain exports." *AP News*, April 26, 2023; Payne, Julia, and Alan Charlish. "Poland, Hungary, Slovakia to introduce bans on Ukraine grains." *Reuters*, September 15, 2023**;** Horton, Jake, and Erwan Rivault. "Satellite images reveal damage to Ukraine grain ports." *BBC News*, September 8, 2023.

[21] Kirby, Paul. "Ukraine war: Russia strikes Ukraine grain after ending sea deal." *BBC News*, July 19, 2023.

[22] "How is Ukraine exporting its grain now the Black Sea deal is over?" *BBC News*, September 26, 2023.

[23] Kirby, Paul. "Ukraine war: Russia strikes Ukraine grain after ending sea deal." *BBC News*, July 19, 2023; Horton, Jake, and Erwan Rivault. "Satellite images reveal damage to Ukraine grain ports." *BBC News*, September 8, 2023.

[24] "How is Ukraine exporting its grain now the Black Sea deal is over?" *BBC News*, September 26, 2023; "Russia threatens to pull out of Ukraine grain deal, raising fears about global food security." *PBS News Hour,* July 12, 2023; Bonnell, Courtney. "Why allowing Ukraine to ship grain during Russia's war matters to the world." *AP News*, July 15, 2023.

[25] Payne, Julia, and Alan Charlish. "Poland, Hungary, Slovakia to introduce bans on Ukraine grains." *Reuters*, September 15, 2023; "Ukraine says it will sue Poland, Hungary and Slovakia over food import bans." *Reuters,* September 18, 2023.

[26] "Ukraine says it will sue Poland, Hungary and Slovakia over food import bans." *Reuters*, September 18, 2023.

[27] Food and Agricultural Organization of the United Nations. "Ukraine: Impact of the War on Agricultural Enterprises," 2023. https://www.fao.org/documents/card/en/c/cc5755en.

[28] Brennan, David. "Russia Threatens 'Dozens of Billions' in Ukraine Gas, Minerals: Minister." *Newsweek*, February 6, 2023; Faiola, Anthony, and Dalton Bennett. "In the Ukraine war, a battle for the nation's mineral and energy wealth." *Washington Post,* August 10, 2022.

[29] Muggah, Robert. "Russia's Resource Grab in Ukraine." *Foreign Policy*, April 28, 2022; Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine. "Ukraine Investment Opportunities in Exploration and Production." https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf, 2023.

[30] Based on analysis of data from the U.S. Geological Survey and the U.S. Department of the Interior's "Mineral Commodity Summaries 2023." U.S. Geological Survey: Reston, VA, January 2023.

[31] Based on analysis of data from the U.S. Geological Survey and the U.S. Department of the Interior's "Mineral Commodity Summaries 2023." U.S. Geological Survey: Reston, VA, January 2023.

[32] Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine. "Ukraine Investment Opportunities in Exploration and Production." https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf, 2023.

[33] Based on analysis of data from the U.S. Geological Survey and the U.S. Department of the Interior's "Mineral Commodity Summaries 2023." U.S. Geological Survey: Reston, VA, January 2023, pp. 184-187.

[34] Barich, Anthony. "Metals and the invasion: Ukraine aims for critical minerals after the war." *S&P Global Market Intelligence,* February 21, 2023.

[35] Based on analysis of data from the U.S. Geological Survey and the U.S. Department of the Interior's "Mineral Commodity Summaries 2023." U.S. Geological Survey: Reston, VA, January 2023, pp. 184-187.

[36] Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine. "Ukraine Investment Opportunities in Exploration and Production." https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf, 2023; Faiola, Anthony, and Dalton Bennett. "In the Ukraine war, a battle for the nation's mineral and energy wealth." *Washington Post*, August 10, 2022; Kadam, Tanmay. "Critically Dependent on Russia and China, US-Led West Look to Secure 'Rare' Metal in Ukraine Vital for Fighter Jets, Air Planes." *Eurasian Times*, January 30, 2023.

[37] "Ukrainian mining company Velta will build a $1.5B factory to produce titanium powder in the US and Ukraine." *Ukraine Business News*, May 16, 2023; Brennan, David. "The Battle for Ukraine's Titanium." *Newsweek,* January 28, 2023; Kadam, Tanmay. "Critically Dependent on Russia and China, US-Led West Look to Secure 'Rare' Metal in Ukraine Vital for Fighter Jets, Air Planes." *Eurasian Times,* January 30, 2023.

[38] Based on analysis of data from the U.S. Geological Survey and the U.S. Department of the Interior's "Mineral Commodity Summaries 2023." U.S. Geological Survey: Reston, VA, January 2023, pp. 184-187.

[39] Theise, Eugen. "Russia plundering Ukraine's natural resources." *DW,* August 28, 2023; Barich, Anthony. "Metals and the invasion: Ukraine aims for critical minerals after the war." *S&P Global Market Intelligence,* February 21, 2023.

[40] Barich, Anthony. "Metals and the invasion: Ukraine aims for critical minerals after the war." *S&P Global Market Intelligence*, February 21, 2023; Based on analysis of data and text from the U.S. Geological Survey and the U.S. Department of the Interior's "Mineral Commodity Summaries 2023." U.S. Geological Survey: Reston, VA, January 2023, pp. 82-83; Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine, "Ukraine Investment Opportunities in Exploration and Production." https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf, 2023; Theise, Eugen. "Russia plundering Ukraine's natural resources." *DW,* August 28, 2023.

[41] Tabuchi, Hiroko. "Before Invasion, Ukraine's Lithium Wealth Was Drawing Global Attention." *New York Times*, March 2, 2022; Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine. "Ukraine Investment Opportunities in Exploration and Production." https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf, 2023; Coakley, Amanda. "Ukraine was poised to become an important rare earths exporter. Then came the invasion." *Coda*, March 20, 2023; Theise, Eugen. "Russia plundering Ukraine's natural resources." *DW*, August 28, 2023.

[42] Theise, Eugen. "Russia plundering Ukraine's natural resources." *DW*, August 28, 2023; Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine, "Ukraine Investment Opportunities in Exploration and Production." 2023. https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf.

[43] Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine, "Ukraine Investment Opportunities in Exploration and Production." 2023. https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf.

[44] Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine, "Ukraine Investment Opportunities in Exploration and Production." 2023. https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf; Barich, Anthony. "Metals and the invasion: Ukraine aims for critical minerals after the war." *S&P Global Market Intelligence*, February 21, 2023.

[45] Coakley, Amanda. "Ukraine was poised to become an important rare earths exporter. Then came the invasion." *Coda*, March 20, 2023; Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine, "Ukraine Investment Opportunities in Exploration and Production." 2023. https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf; Tabuchi, Hiroko. "Before Invasion, Ukraine's Lithium Wealth Was Drawing Global Attention." *New York Times*, March 2, 2022; Brennan, David. "'Russia Threatens 'Dozens of Billions' in Ukraine Gas, Minerals: Minister." *Newsweek*, February 6, 2023.

[46] Energy Information Agency. "Ukraine Report." August 2021; Muggah, Robert. "Russia's Resource Grab in Ukraine." *Foreign Policy*, April 28, 2022.

[47] Data from the Energy Institute's *2023 Statistical Review of World Energy*; Brennan, David. "Russia Threatens 'Dozens of Billions' in Ukraine Gas, Minerals: Minister," *Newsweek*, February 6, 2023.

[48] Energy Information Agency." Ukraine Report." August 2021.

[49] Energy Information Agency. "Ukraine Report." August 2021; Data from the Energy Institute's *2023 Statistical Review of World Energy.*

[50] Stern, David. "Despite War, Ukraine Allows Russian Oil and Gas to Cross Its Territory." *Washington Post*, May 24, 2023; Energy Information Agency. "Ukraine Report." August 2021; Wikipedia. "Trans-Balkan Pipeline." Accessed October, 31, 2023.

[51] Losz, Akos. "Q&A | Russian Gas Transit Through Ukraine." Center on Global Energy Policy, Columbia University, October 3, 2023.

[52] Corbeau, Anne-Sophie, and Tatiana Mitrova. "Will the Ukrainian Gas Transit Contract Continue Beyond 2024?" Center on Global Energy Policy, Columbia University, June 8, 2023; Stern, David. "Despite War, Ukraine Allows Russian Oil and Gas to Cross Its Territory." *Washington Post*, May 24, 2023; Losz, Akos. "Q&A | Russian Gas Transit Through Ukraine." Center on Global Energy Policy, Columbia University, October 3, 2023.

[53] Losz, Akos. "Q&A | Russian Gas Transit Through Ukraine." Center on Global Energy Policy, Columbia University, October 3, 2023.

[54] Losz, Akos. "Q&A | Russian Gas Transit Through Ukraine." Center on Global Energy Policy, Columbia University, October 3, 2023.

[55] Losz, Akos. "Q&A | Russian Gas Transit Through Ukraine." Center on Global Energy Policy, Columbia University, October 3, 2023; Corbeau, Anne-Sophie, and Tatiana Mitrova. "Will the Ukrainian Gas Transit Contract Continue Beyond 2024?" Center on Global Energy Policy, Columbia University, June 8, 2023.

[56] Corbeau, Anne-Sophie, and Tatiana Mitrova. "Will the Ukrainian Gas Transit Contract Continue Beyond 2024?" Center on Global Energy Policy, Columbia University, June 8, 2023; Naftogaz Group, "Ukraine plans to end Russian gas transit contract in 2024—interview for Deutsche Welle." October 24, 2023. https://www.naftogaz.com/en/interviews/ukraine-will-not-extend-gas-transit-contract-with-russia-interview-deutsche-welle.

[57] Corbeau, Anne-Sophie, and Tatiana Mitrova. "Will the Ukrainian Gas Transit Contract Continue Beyond 2024?" Center on Global Energy Policy, Columbia University, June 8, 2023; Losz, Akos. "Q&A | Russian Gas Transit Through Ukraine." Center on Global Energy Policy, Columbia University, October 3, 2023.

[58] Energy Information Agency. "Ukraine Report." August 2021.

[59] Data from the Energy Institute's *2023 Statistical Review of World Energy*.

[60] Energy Information Agency. "Ukraine Report." August 2021; Stern, David. "Despite War, Ukraine Allows Russian Oil and Gas to Cross Its Territory." *Washington Post*. May 24, 2023; International Energy Agency. "Ukraine Energy Profile." September 20, 2021, p. 23.

[61] Muggah, Robert. "Russia's Resource Grab in Ukraine." *Foreign Policy*, April 28, 2022; Faiola, Anthony, and Dalton Bennett. "In the Ukraine war, a battle for the nation's mineral and energy wealth." *Washington Post*, August 10, 2022; Energy Information Agency. "Ukraine Report." August 2021; Data from the Energy Institute's *2023 Statistical Review of World Energy*.

[62] Energy Information Agency. "Ukraine Report." August 2021; Faiola, Anthony, and Dalton Bennett. "In the Ukraine war, a battle for the nation's mineral and energy wealth." *Washington Post*, August 10, 2022; Theise, Eugen. "Russia plundering Ukraine's natural resources." *DW,* August 28, 2023.

[63] Ukraine Geological Survey and Ministry of Environmental Protection and Natural Resources of Ukraine, "Ukraine Investment Opportunities in Exploration and Production." 2023. https://www.geo.gov.ua/wp-content/uploads/presentations/en/investment-opportunities-in-exploration-production-strategic-and-critical-minerals.pdf; Brennan, David. "Russia Threatens 'Dozens of Billions' in Ukraine Gas, Minerals: Minister." *Newsweek*, February 6, 2023.

A Gray Zone Option for Integrated Deterrence

Special Operations Forces (SOF)

By Kevin D. Stringer

In a speech delivered on April 30, 2020, U.S. Secretary of Defense Lloyd Austin reaffirmed that deterrence is still the foundation of American defense, but that with the current operating environment, deterrence must incorporate all elements of national power. His concept of integrated deterrence goes far beyond the traditional nuclear and conventional military deterrence, encompassing a wider range of capabilities and stakeholders.[1] An understudied and under-researched element of this integrated deterrence idea is the role of special operations forces (SOF) as an essential component of a multi-layer set of deterrence options for a nation-state. The inclusion of SOF in deterrence derives from its utility operating in the gray zone, defined as the region of "…competitive interactions among and within state and non-state actors that fall between the traditional war and peace

Special Operations Forces train together at exercise Night Hawk 21. Operators from the Royal Danish Army's special forces, the Jaeger Corps, settle in to a German Army CH-53 helicopter during exercise Night Hawk 21 on 5 October 2021.

Colonel Kevin D. Stringer, USA (Ret.), Ph.D., is adjunct faculty at the Baltic Defence College and a Lecturer at the University of Northwestern Switzerland.

duality. They are characterized by ambiguity about the nature of the conflict, opacity of the parties involved, or uncertainty about the relevant policy and legal frameworks."[2] This gray zone setting frequently occurs prior to actual war and is a natural area for creating deterrent effects in the mind of an adversary. The inclusion of SOF in deterrence efforts is counterintuitive given that most SOF activities are clandestine by nature and purposefully hidden from public view to preserve secrecy and safeguard specialized tactics, techniques, and procedures. However, an appropriate and calculated level of visibility on SOF activities can supplement other types of measures in enhancing deterrent effects. Additionally, since special operations formations conduct tactical and operational level actions that typically have strategic outcomes, they would logically be valuable contributors to national level deterrence efforts.

This article provides a brief theoretical foundation and working definition for deterrence before delving into the practical use of SOF for deterrence using North Atlantic Treaty Organization (NATO) SOF doctrine as a framing mechanism. The examination offers examples of SOF deterrence activities carried out within the three NATO SOF missions of military assistance (MA), special reconnaissance (SR), and direct action (DA). It then considers the risks and opportunities of using SOF for deterrence efforts. The objective of the article is to deliver a contribution to national security policymakers and military leadership that stimulates their practical thinking on the application of SOF in a field with sparse literature and minimal research.

DETERRENCE

Deterrence is an important mechanism in international relations, and its theories, both nuclear and conventional, played a significant role in shaping interstate conflict during the Cold War. The changed security environment of the 21st century calls for a re-examination of this concept, with the goal of adjusting both theory and practice.[3] For example, the French understanding of deterrence only applies to nuclear activities, which is limiting in the more ambiguous, 21st century multipolar world of great power conflict characterized by competition between China, Russia, and the United States and its Allies.

The classic definition of deterrence offered by Alexander George and Richard Smoke "…is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits."[4] This characterization emphasizes the strong cognitive and perceptual element of deterrence as a psychological effect and serves as the foundational operating definition for this article. In fact, having sufficient strategic empathy to understand the opponent's psychological cost-benefit calculation for an aggressive action is a critical element for successful deterrence. With this starting point, the challenge is then to deftly shape and adjust the adversary's perception of the cost-benefit calculation, and the intended action is not taken.[5] This shaping action occurs by demonstrating the three elements of successful deterrence: capability, credibility, and communication. In other words, the actor "has the technical means to perform the operation, demonstrates the willingness to employ said capabilities, and ensures that the opponent clearly understands the parameters of behavior and the costs of violating those limitations."[6] Concerning the last point, deterrence theory holds that if the communicated costs are severe enough, the threatening activity will be discouraged.[7]

RAND scholar Michael Mazarr goes further and divides deterrence strategies into two categories: deterrence by denial and deterrence by punishment. The former seeks "to deter an action by making it infeasible or unlikely to succeed, thus denying a potential aggressor confidence in attaining its objectives, while the latter "threatens severe penalties…

if an attack occurs."[8] In this second case, clear communication of the tripwire mechanism that would trigger the punishment is critical. This step communicates the unbearable costs of crossing this red line. Recently, the United States and NATO posited deterrence by resilience as a subset of deterrence by denial, the premise being that building societal resilience endeavors to persuade "…an adversary not to attack by convincing it that an attack will not achieve its intended objectives" because the population is able "to withstand, fight through, and recover quickly from disruption."[9] For the examination of SOF in deterrence activities, this article will apply these categorizations supplemented by a distilled and synthesized definition of deterrence formulated as the prevention of an action by instilling a fear of consequences, supported by the tripartite model of capability, credibility, and will.[10]

SOF AS AN ELEMENT OF INTEGRATED DETERRENCE

There is little literature on SOF as an element of integrated deterrence.[11] The 2021 RAND study *Countering Russia: The Role of Special Operations Forces in Strategic Competition* noted this deficiency, highlighting that while some sources offer ways for SOF to enhance conventional deterrence, the recommendations are often vague and there is a need for more specificity and conceptual thinking on the employment of SOF in this role.[12] This article will propose the utilization of SOF for deterrence efforts using the NATO SOF doctrine as its guiding framework. For NATO, *Allied Joint Publication (AJP)-3.5 (B), Allied Joint Doctrine for Special Operations* is the foundational document for NATO SOF and defines the SOF core missions as military assistance (MA), special reconnaissance (SR), and direct action

NATO enhanced Forward Presence troops road march through Poland in support of NATO's defence and deterrence measures. US soldier onboard Stryker vehicle.

(DA).[13] While acknowledging that special operations are frequently classified and challenging to observe, there is still a need for pragmatic, unclassified, and thoughtful discussion on the employment of SOF as a deterrent. The following sections will elaborate on the use of SOF for deterrence in each of these distinct mission areas to illustrate potential SOF contributions to a multi-layer deterrence campaign.

MILITARY ASSISTANCE (MA): SOF DETERRENCE BY DENIAL AND PUNISHMENT

Military assistance encompasses the broad task of training, advising, mentoring, and partnering to support and enable friendly assets.[14] Within this mission, SOF can contribute to deterrence by denial and punishment through the development of partner SOF, national territorial defense forces (TDF), conventional forces, and other volunteer organizations for comprehensive defense, specifically in the establishment of national resilience and resistance capabilities. Comprehensive defense is understood as an official government strategy which encompasses a whole-of-society approach to protecting the nation against potential threats.[15]

While all populations have the potential to resist, this population capability must be developed in peacetime for effectiveness. If a pre-crisis developed resistance organization does not exist, it cannot deter an aggressor.[16] In many countries, volunteer territorial defense forces, also known as national guards or home guards, have a central role in this process. In peacetime, these forces contribute to societal resilience through crisis response work and civil population engagement, while during an occupation, TDF are cross-cutting and core contributors to all the classic resistance components—underground, auxiliary, and guerrillas.[17] In the pre-crisis phase, national or allied SOF can train and advise territorial defense forces in core resistance activities such as subversion, sabotage, and guerrilla warfare. This MA helps to build "a whole-of-nation, government-led resistance capability which provides ways to coerce, disrupt, and potentially defeat an occupier in wartime."[18] These resistance capabilities, both overt and clandestine, can make an occupation untenable and thereby affect adversary cost calculations to deter aggression. Such a resistance organization is not only a viable response to an incursion, but it should be considered a gray zone deterrence option, complementary and amplifying to conventional and nuclear deterrents.

Metaphorically, SOF feed and care for the "national resistance porcupine" to make it appear larger and more indigestible, thereby deterring aggressors. Credible and strategic communication is essential to ensuring the adversary views it as a porcupine and not a smaller hedgehog. This utilization of SOF in its MA role appears to be the most effective use of its unconventional warfare expertise, while also providing the greatest deterrent value against revisionist powers within a comprehensive defense national framework. This model is currently being used with encouraging results in the Baltics, Poland, Georgia, and other Eastern European countries, where national or allied SOF develop territorial forces and their resistance capabilities to augment overall deterrence measures and provide national defense options.

SPECIAL RECONNAISSANCE: SOF DETERRENCE BY DENIAL VIA AMBIGUITY OR PUNISHMENT

The second SOF mission for deterrence consideration is special reconnaissance. NATO doctrine describes it as "reconnaissance and surveillance activities conducted as a special operation in, but not limited to, hostile, denied, or diplomatically and/or politically sensitive environments to collect or verify information of strategic or operational significance, led by SOF using distinct techniques and modes

of employment."[19] These activities, carried out in sensitive regions or on the periphery of strategic nodes and made partially visible to the adversary, can contribute to instilling perceptions of deterrence by denial. The objective is not to compromise the core SR mission but to provide enough of a "visible SOF iceberg" to create anxiety or uncertainty in the minds of adversarial decisionmakers that they may lack the capabilities to address or suppress an opaque special operations threat, thereby increasing the costs of their aggressive intent. The use of SOF in the SR mode for deterrence also plays upon the mystique of special forces, justified or not, that they can conduct successful, high-risk operations that result in strategic effects.

Considering strategic empathy and adversary military culture, Russia is likely highly sensitive to such unknown or ambiguous special operations activities occurring on its borders, maritime or terrestrial, given its own military culture of indirect action that often uses SOF. In fact, using allied SOF in this SR role would actually mirror aspects of the Russian concept of strategic deterrence which relies heavily on proactive gray zone measures that include special operations units.[20] This Russian approach brought success in the Second Chechen War (1999-2009) and in Crimea in 2014, and hence the Kremlin would be wary of similar allied SOF activities occurring under the banner of SR near its strategic nodes or borders.

Concretely in SR mission mode, allied SOF units would operate in such maritime locations as the Baltic, Black, Caspian, Barents, and White seas to create ambiguity of intent and send deterrence signals to the Russian military and political leadership as part of their preparation of the environment, which includes information gathering, pre-targeting groundwork, and the mapping of enemy assets, decision-making processes, and infrastructure. These activities are holding the adversary's assets at risk by conducting pre-targeting tasks to find and fix objectives for rapid finish operations. Similar SR actions could occur on land near the Kaliningrad enclave, Transnistria, Abkhazia, South Ossetia, or along the long Central Asian border. As the article "Jomini and Naval Special Operations Forces—An Applied-Competition Approach to Russia" noted, such "overt activities, amplified by appropriate and supporting information operations, …create uncertainty in the minds of adversary leadership, leading them to question what…special operations forces actually are doing in these sensitive regions."[21] These doubts are intended to create anxieties that will influence the Russian decision-making calculus and enhance an overall multilayer approach to deterrence. Because such operations are part of the Russian cultural and historical playbook, this particular application of SOF serves as a limited demonstration of force to communicate seriousness and play upon Russian psychology.

DIRECT ACTION: SOF DETERRENCE BY PUNISHMENT VIA PRE-EMPTIVE STRIKES

According to NATO SOF doctrine, direct action (DA) involves "a short duration strike or other small-scale offensive action by SOF to seize, destroy, capture, recover, or inflict damage to achieve specific, well-defined and often time-sensitive results."[22] This SOF mission has strongly characterized the Middle Eastern counterterrorist campaigns over the last two decades and is the most popularized special operations task in public media and even films. Several governments have used special operations direct action as a deterrence by punishment tool against non-state actors, often insurgent or terrorist groups, to exact revenge and to send warning signals to discourage future actions. This usage usually takes the form of pre-emptive strikes against significant terrorist actors or installations. A key element for this use of SOF in DA deterrence is the clear communication of "red lines" and the applicable punishment

Nahal's Special Forces conducted a firing drill in southern Israel with a range of different weapons. The firing course was part of their advanced training where they learn to specialize in a certain firearm.

principles prior to the action in order to achieve deterrent effect. Two examples, one purportedly Israeli and the other American, demonstrate the use of SOF DA as a deterrence by punishment measure.

On January 19, 2010, an alleged Israeli special operations team eliminated the Hamas functionary Mahmoud al-Mabhouh in a Dubai luxury hotel for his killing of two Israeli soldiers in 1989 and his role in procuring sophisticated weaponry for Hamas activities in Gaza.[23] Purportedly, a specialized Mossad task unit called "Kidon" (or "bayonet") made up of former Israeli Defence Force special operators conducted the strike.[24] Although this strike was a covert action conducted by a specialized intelligence unit, its example illustrates potential SOF utilization in the direct action deterrence role. Apparently, Mahmoud al-Mabhouh was the beneficiary of a Mossad "Red Page" order, authorized by the Israeli prime minister and defense minister, for enemies of the state. These orders do not have an expiration date.[25] In this vignette, a direct action strike by covert SOF is used as a strategic signaling device designed to dissuade terrorist group elements from future action. This SOF case fits into the broader Israeli concept of deterrence exemplified by the 2007 conventional Israeli airstrike on a suspected Syrian nuclear reactor, which was considered a "...strategic signal...about deterrence more than creating damage."[26]

Similarly, the January 3, 2020, U.S. drone strike that killed Qasem Soleimani, head of the terrorist-designated Iranian Islamic Revolutionary Guard Corps–Quds Force in Baghdad, displayed elements of special operations direct action used as a deterrent. According to news sources, U.S. SOF sniper teams were emplaced at the Baghdad International Airport in a direct action backup role in case the Hellfire missiles did not destroy their target.[27] Already during the Bush administration in 2007, U.S. special operations forces planned a mission to capture Soleimani, but senior U.S. leaders declined to approve it.[28] As the official Department of Defense press release stated concerning Soleimani, "This strike was aimed at deterring future Iranian attack plans."[29]

Naturally, there are significant concerns about the effectiveness, risks, escalation, and legality of using SOF in such direct action roles for deterrence. These themes will be discussed in the following section. For great power conflict, discrete and selective SOF direct action missions remain an option for deterrence signaling after an appropriate risk assessment. In light of the current conflict in Eastern Europe, possible uses of SOF could include the elimination or capture of pro-Russian separatist leaders and politicians in contested areas. Such actions, while risking escalation, would potentially deter other collaborators from supporting Russian subversive elements in disputed regions such as Abkhazia, South Ossetia, and Transnistria or those in Ukraine's eastern regions while avoiding strikes on actual Russian personnel. There are historical precedents for such direct action SOF deterrence activities in occupation scenarios. During World War II, both the Norwegian and Polish governments-in-exile authorized targeted elimination of turncoats by either special operations forces or national resistance cells to deter traitors. The Norwegian government-in-exile published a prioritized list of collaborators for elimination, while the Polish state established an entire underground judiciary for authorizing tasked units to mete out justice to betrayers.[30]

RISKS AND OPPORTUNITIES

According to the definition of deterrence offered above, SOF have both the capability and credibility to contribute to deterrence efforts. The open variable is the political will to commit SOF to such actions. A political decision to use SOF in deterrence must carefully balance risks and opportunities. For risks, three significant ones emerge: escalation; exposing clandestine tactics, techniques, and procedures (TTPs); and violating international law. Considering these three major risks and mapping them against the SOF deterrence missions, military assistance seems to be the least problematic while providing good deterrent value in raising adversarial cost calculations through heightened societal resistance and resilience capabilities. This application would mirror the emerging deterrence by resilience concept. Special reconnaissance, through its generation of ambiguity near sensitive objects or regions, runs a medium risk of escalation and the potential exposure of TTPs. SOF direct action deterrence in the form of pre-emptive strikes appears to possess the highest risk level since it exposes the initiator to escalation and retribution, potentially bares TTPs to scrutiny, and provides the grounds for accusations of human rights and international law violations.

That said, the use of SOF in deterrence also provides opportunities. First, because of their small size and low cost, SOF are a cost-effective deterrent. Second, the high level of special operator training, coupled with organizational capabilities, enables a precision and nuanced application of deterrence activities in regions and areas sensitive to the adversary. Third, SOF deterrent actions can be easily combined with conventional deterrence activities such as exercises, shows of force, and rapid deployments, while also serving as a multiplier or amplifier of national deterrence efforts in other domains.

CONCLUSION

In the pre-crisis or competition phase, SOF can contribute to a multilayer deterrence campaign through the conduct of tailored military assistance, special reconnaissance, and direct action missions. All three SOF tasks have the potential to influence the conflict environment and the opponent's behavior and calculus. Military assistance to national volunteer or territorial defense forces is most likely the least risky deterrence option that can contribute to improved comprehensive defense, force readiness, and credible resilience and resistance capabilities. These abilities warn an aggressor that a military occupation will be

both costly and unwinnable. Special reconnaissance, which is slightly riskier, increases situational awareness by gathering intelligence and understanding in sensitive locations, while transmitting ambiguous yet potentially threatening signals to the adversary as a limited demonstration of force. Finally, direct action through pre-emptive strikes, with pre-communicated "red lines," sends a sharp deterrent message that can either influence adversarial decisionmaking to change course or engender increasing levels of escalation and retribution. Regardless of mission employment and risk levels, SOF offer viable gray zone deterrence options that can blend readily with conventional and even nuclear deterrence efforts. In the deterrence role, SOF provide policymakers with a precise, nuanced instrument for creating deterrent effects which "are strategic or political rather than tactical in nature."[31] The examples derived from the application of the NATO SOF doctrinal framework underpin a perspective that SOF can be an integral element of a thoughtful and layered national or Allied deterrence effort. This application demonstrates the versatility of SOF in this era of great power conflict. PRISM

Notes

[1] Secretary of Defense Lloyd J. Austin III, Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command, Honolulu, HI, April 30, 2021, Secretary of Defense Remarks for the U.S. INDOPACOM Change of Command > U.S. Department of Defense > Transcript, accessed, June 16, 2022.

[2] Philip Kapusta. *US SOCOM White Paper: The Gray Zone* (MacDill AFB: USSOCOM, 2015).

[3] Patrick M. Morgan, "The State of Deterrence in International Politics Today," *Contemporary Security Policy*, 33:1 (2012), 85-107.

[4] Alexander L. George and Richard Smoke. *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974), 11.

[5] Robert Jervis, "Deterrence and Perception," *International Security*, Vol. 7, No. 3 (Winter, 1982-1983), 3-30; H.R. McMaster. *Battlegrounds: The Fight to Defend the Free World* (New York, Harper, 2020), 16-17; and Michael Mazarr, "Understanding Deterrence" *Perspectives* (Santa Monica, CA: RAND, 2020), at Understanding Deterrence | RAND, accessed July 15, 2022.

[6] Richard D. Newton, JSOU, "Two Air Forces," unpublished paper, May 2022.

[7] Daniel S. Nagin, "Deterrence in the Twenty-First Century," Crime and Justice, Vol. 42, No. 1, *Crime and Justice in America 1975–2025,* August 2013, 199-263, specifically 206.

[8] Michael Mazarr, "Understanding Deterrence" *Perspectives* (Santa Monica, CA: RAND, 2020), at Understanding Deterrence | RAND, accessed July 15, 2022.

[9] North Atlantic Treaty Organization, *Deterrence and defence*, July 19, 2023, at https://www.nato.int/cps/en/natohq/topics_133127.htm, accessed October 2, 2023; and U.S. Department of Defense. *U.S. National Defense Strategy* (Washington, DC: Department of Defense, 2022), 8.

[10] Baltic Defence College's Higher Command Study Course 2022 consensus definition. This multinational class consisted of 23 senior military and civilian defense leaders.

[11] The extant literature that touches on this specific subject includes: Robert Haddocks, *How Do SOF Contribute to Comprehensive Deterrence? JSOU Report 17-11* (MacDill Air Force Base, FL: Joint Special Operations University, 2017); Tom Hammerle and Mike Pultusker, "Special Operations are Deterrence Operations," *Small Wars Journal*, May 2022; Katie Crombe, Steve Ferenzi, and Robert Jones, "Integrating deterrence across the gray—making it more than words," *Military Times*, December 9, 2021, at Integrating deterrence across the gray — making it more than words (militarytimes.com), accessed July 22, 2022; Michal Strzelecki, *Special Operations Forces' role in the deterrence of Russian aggression*, M.A. thesis, U.S. Army War College, Carlisle, PA, April 2022; Kevin D. Stringer, "Jomini and Naval Special Operations Forces—An Applied-Competition Approach to Russia," *Naval War College Review*, Vol. 74 : No. 4 (2021); and Kevin D. Stringer, "Special Operations Forces (SOF): The Integrators for Total Defense and Resistance," *Journal on Baltic Security*, Vol. 8 : No. 1 (2022).

[12] Stephen Watts, Sean M. Zeigler, Kimberly Jackson, Caitlin McCulloch, Joe Cheravitch, and Marta Keep, *Countering Russia: The Role of Special Operations Forces in Strategic Competition* (Santa Monica, CA: RAND Corporation, 2021) at https://www.rand.org/pubs/research_reports/RRA412-1.html, accessed July 15, 2022.

[13] NATO Standardization Office. *Allied Joint Publication (AJP)-3.5 (B), Allied Joint Doctrine for Special Operations (Edition B, Version 1)* (Brussels, Belgium: North Atlantic Treaty Organization, 2019).

[14] NATO Standardization Office. *Allied Joint Publication (AJP)-3.5 (B), Allied Joint Doctrine for Special Operations (Edition B, Version 1)* (Brussels, Belgium: North Atlantic Treaty Organization, 2019), 7-8.

[15] *NATO Special Operations Headquarters Comprehensive Defence Handbook,* Volume 1, Edition A, Version 1 (Mons: NATO Special Operations Headquarters, December 2020), 15.

[16] *NATO Special Operations Headquarters Comprehensive Defence Handbook,* Volume 1, Edition A, Version 1 (Mons: NATO Special Operations Headquarters, December 2020), 45.

[17] Kevin D. Stringer, "Special Operations Forces (SOF): The Integrators for Total Defense and Resistance," *Journal on Baltic Security* 8:1 (2022).

[18] Derek Jones and J. Bryant Love, "Resilience and Resistance 2.0: initial lessons of Ukraine and the implication of resilience and resistance efforts to deter and respond to invasion and occupation by revisionist powers," *Security Theory and Practice*, No. 1 (XLVI), 2022.

[19] NATO Standardization Office. *Allied Joint Publication (AJP)-3.5 (B), Allied Joint Doctrine for Special Operations (Edition B, Version 1)* (Brussels, Belgium: North Atlantic Treaty Organization, 2019), 8.

[20] *Russian National Security Strategy, December 2015—Full-text Translation*, at Russian-National-Security-Strategy-31Dec2015.pdf (ieee.es), accessed July 21, 2022.

[21] Kevin D. Stringer, "Jomini and Naval Special Operations Forces—An Applied-Competition Approach to Russia," *Naval War College Review*, Vol. 74: No. 4 (2021), 79-93 specifically 90.

[22] NATO Standardization Office. *Allied Joint Publication (AJP)-3.5 (B), Allied Joint Doctrine for Special Operations (Edition B, Version 1)* (Brussels, Belgium: North Atlantic Treaty Organization, 2019), 9.

[23] Ronen Bergman, "The Dubai Job," *GQ* (January 4, 2011), The Dubai Job | GQ, accessed July 20, 2022.

[24] D. Bednarz, E. Follath, C. Schult, A. Smoltczyk, H. Stark, B. Zand, "Targeted Killing in Dubai: A Mossad Operation Gone Awry?" *Der Speigel* (23 Feb. 2010), at Targeted Killing in Dubai: A Mossad Operation Gone Awry? - DER SPIEGEL, accessed July 20, 2022.

[25] Ronen Bergman, Christoph Schult, Alexander Smoltczyk, Holger Stark, and Bernhard Zand, "The Anatomy of Mossad's Dubai Operation," *Der Spiegel* (17 Jan. 2011), at An Eye for an Eye: The Anatomy of Mossad's Dubai Operation - DER SPIEGEL, accessed July 20, 2022.

[26] Headquarters, U.S. Marine Corps. *MCDP 1-4 Competing* (Washington, DC: Department of the Navy, 2020), 2-5.

[27] Jack Murphy and Zach Dorfman, "'Conspiracy is hard': Inside the Trump administration's secret plan to kill Qassem Soleimani," *Yahoo News*, May 8, 2021, at 'Conspiracy is hard': Inside the Trump administration's secret plan to kill Qassem Soleimani (yahoo.com), accessed July 22, 2022.

[28] This statement was made by retired U.S. Army Colonel Frank Sobchak, a Middle Eastern expert, in a conversation with *Politifact*. See Tom Kertscher, "Fact-checking Trump's claim that Obama designated Iran's Soleimani a terrorist but did nothing," *Politifact*, January 16, 2020, at PolitiFact | Fact-checking Trump's claim that Obama designated Iran's Soleimani a terrorist but did nothing, accessed July 20, 2022.

[29] *Statement by the Department of Defense*, January 3, 2020, at Statement by the Department of Defense > U.S. Department of Defense > Release, accessed July 20, 2022.

[30] Tony Insall, *Secret Alliances: Special Operations and Intelligence in Norway 1940-1945* (London: Biteback Publishing, 2019), 211, 304, and Katarzyna Utracka, "The Phenomenon of the Polish Undergound," *The Warsaw Institute Review*, 4 Dec 2019, The Phenomenon of the Polish Underground State | Warsaw Institute, accessed October 2, 2023.

[31] Rob de Wijk, Frank Bekkers, Tim Sweijs, Stephan de Spiegeleire, Dorith Kool, *The Future of NLD SOF: Towards an All-Domain Force* (The Hague: The Hague Centre for Strategic Studies, July 2021), 13.

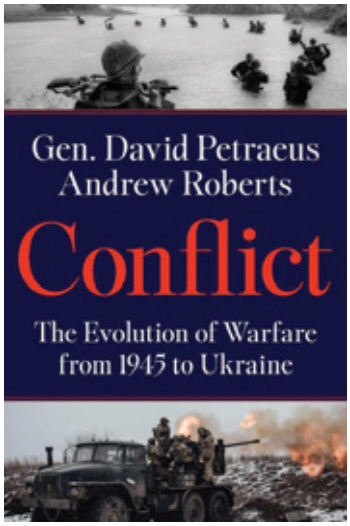
WWW.WARSAWSECURITYFORUM.ORG

#WSF2024

Conflict: The Evolution of Warfare from 1945 to Ukraine

By David Petraeus and Andrew Roberts
Harper Collins Publishers, 2023
544 pp. $32.00
ISBN: 9780063293137

Reviewed by Robert B. Zoellick



David Petraeus is perhaps the leading American general of his generation. Andrew Roberts is an illustrious biographer of wartime leaders, including Churchill, Napoleon, George III, Lord Salisbury, and the allied Masters and Commanders of World War II. Students of military history—whether general readers, rising officers, senior NCO's, or teachers at staff colleges—will no doubt want to see what their teamwork produced.

PRISM readers appreciate that military histories have taken many forms. Russell Weigley related stirring episodes in his *The Age of Battles*; Petraeus and Roberts reference momentous battles—such as Dien Bien Phu, Ia Drang Valley, the Sinai, Shahi Kot Valley, and Fallujah—but are not preoccupied by individual engagements. Michael Howard's *The Franco-Prussian War* offers the classic story of a campaign; *Conflict*'s account of the Falklands presents a stirring tale, but the authors' priority is to show how campaigns evolved. Margaret MacMillan's *War: How Conflict Shaped Us* explains how violent conflicts have shaped societies; Petraeus and Roberts focus instead on the challenging learning process of militaries since 1945. In sum, *Conflict* is a modern military history that reflects the authors' warning that warfare must be understood as a continuous expedition of learning and adaptation, as well as a contest of arms and strategies.

One can almost hear Petraeus's voice arguing to more traditional colleagues that most of the 150 to 300 armed conflicts since 1945 have not been state-on-state wars. Therefore, leaders had better prepare for messy fights that blur war and peace. Consider how Iran's strategy today relies on wounding attacks just short of provoking a direct U.S. military response. The Korean War of 1950–1953 rang the warning bell: a brutal conflict short of mutually assured destruction, forcing recognition that countries would need to wage conventional combat under

Robert B. Zoellick served as President of the World Bank, U.S. Trade Representative, and Deputy Secretary of State and was involved with the diplomacy of many conflicts. He is the author of America in the World: A History of U.S. Diplomacy and Foreign Policy.

the shadow of possible nuclear escalation—a risk that still hangs over Ukraine.

The authors deploy the Malayan and Borneo counterinsurgencies as forewarnings of the Vietnam War, a lesson not learned in the 1960s, but recalled by Petraeus in his Counterinsurgency Field Manual of 2006. Vietnam serves as an example of how generals mistook the type of war they were waging; fading stars of World War II wanted to wage an older campaign of firepower and attrition, but their enemy combined conventional assaults and guerrilla insurgency to defeat the South Vietnamese and erode American will.

The chapter on Iraq presents the backbone of the authors' thesis. They emphasize how the pieces of the war-fighting puzzle must fit together. Leaders must grasp the nature of their conflict and strategize appropriately. Yet commanders must also communicate their plans effectively at various levels—to units, national publics, coalitions, and even the wider world. Plans will be useless without execution and continuous assessment and adaptation. Learning will often flow up the chain of command from innovative leaders in the field. For a counterinsurgency contest, military leaders need to know the "human terrain" of tribes, religions, regions, and local histories and societies. The book includes a copy of General Petraeus's Commander's Guidance so that readers can see how he communicated strategy in basic terms all the way to platoon and squad leaders.

The account of Afghanistan feels less certain, perhaps because of Petraeus's shorter experience, but also because the authors recognize the difficult decisions. Carter Malkasian's deeply researched *The American War in Afghanistan* suggests that the United States and coalition effort always faced long odds because of the Taliban's advantages of Islam and resistance to "occupation," plus Pakistan's protection of insurgents. Defense Secretary Donald Rumsfeld wanted to get out after overthrowing the Taliban, but President George W. Bush felt an obligation of "nation building." U.S. leaders faced difficult choices about backing local leaders, centralized and decentralized authority, elections, Pakistan, logistics, and the size of the American footprint. Regardless, the authors point out that Bush's government never properly analyzed the implications or devoted the resources to build a self-sustaining Afghanistan. Then it took Washington nine years to develop a coherent strategy backed by resources. But after almost a decade of war, President Barack Obama signaled he wanted out, too. The heart of the matter seemed to be that if the United States could or would not strike an agreement with the Taliban after initial battlefield success, America would have to build an Afghan force that could hold its own, with appropriate equipment and logistics. President Joe Biden decided to terminate that 20-year experiment.

Petraeus and Roberts recognize that modern wars have also quickened the pace and destructive power of combat between massed forces. The Israeli-Arab Six Day and Yom Kippur wars highlighted the superiority of speed, advanced technology, and professional experience and training, as well as the growing lethality of air power. The U.S.-led coalition in the Gulf War of 1990–1991 epitomized the lessons learned with sheer intensity, and added an advanced course in Coalition Diplomacy, use of overwhelming force, intelligence, night-fighting, and peerless logistics. Yet the other side learns, too: after 1990, potential enemies did not want to go head-to-head with United States conventional forces in the desert.

Vladimir Putin's assault on Ukraine returned aggressive war to Europe, ending its "holiday from history" after 1989. The authors caution that Russia's lunge to conquer its neighbor offers a glimpse of war between big powers and a reminder that major wars need not be short and decisive. This war of attrition requires economic as well as military strategies. The warfare tests information systems, industrial bases, and shell stockpiles. For now, defense seems

dominant. Low-cost surveillance and targeting technologies require military dispersion—of command and control, aircraft, ammunition, maintenance, and supply stocks. The Russia–Ukraine war is now a contest of wills, with Western resolve in too short supply.

Beijing will scrutinize Putin's mistakes carefully. No one should take the course of large scale, complex operations for granted. War and uncertainty are twinned. The authors hope that the Taiwanese also learn lessons from Ukraine about air and ballistic missile defenses, sea and shore denial fire, information warfare and civil defense, mine warfare, and resilient critical civilian infrastructure. Yet for all the weaponry and technology, Petraeus and Roberts continually stress the exponential power of leadership, resolve, and morale.

Surveying the land, air, and seascapes of 75 years of modern war, *Conflict* highlights a few other practical admonitions. Surprise can be a powerful force multiplier, yet leaders continue to be astonished by the unexpected. Money spent on deterrence is rarely wasted. Air dominance is vital, but not sufficient, as witnessed in the Balkan wars; invest in the best planes, pilots, and algorithmically-guided systems. To be prepared for the next counterinsurgency mission, the new U.S. Security Forces Assistance Brigade (the British nomenclature of a Ranger Regiment seems more historically appealing) should be capable of helping Special Forces to advise, assist, and enable local allies. Joint command structures need to be streamlined and empowered to quicken the adaptation and OODA (observe, orient, decide, and act) loops. Military strategy, especially in democracies, needs public support at home, posing a special challenge for civilian leaders and civil-military relations.

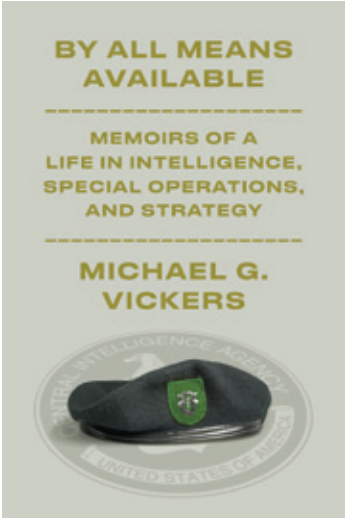
The closing chapter anticipates warfare on the horizon. The authors observe that in the past militaries pioneered new technologies, whereas today innovations in the private sector will outpace those in the fighting forces. Cyber and space now accompany the traditional domains of land, sea, and air. Drones and swarms will be matched by sensors, electronic jamming, and other countermeasures. Robots will be fighting robots, waging algorithmic combat. Petraeus and Roberts soberly report that 30 countries already have robotic, automated weapons with which the speed of engagement is too fast for the human mind. Military history has transformed from tales of champions in single combat to asking where humans will fit within the doom loop. As this book was released, war flared again in Israel, Gaza, and the Middle East. Hamas shocked and surprised the technically superior, respected, and victorious Israeli Defense Force. Violence and terror have erased lines between combatants and civilians. Risks of escalation loom. Israel, the United States, and other friends of Israel are struggling to integrate military and political strategy. The events reinforce the authors' call for adaptive warfare.

Of course, any review needs to suggest missing passages for the next edition. The book briefly references conflict with organized criminal networks, including in Mexico and Central America. Given the importance of this violence to U.S. security—and the U.S. border and immigration—tomorrow's military leaders might benefit from the authors' analogies to counterinsurgency. Similarly, Petraeus's experience with the CIA remains cloaked, probably for understandable reasons of clearance. When the General assumed the post of CIA Director, some watchers of the Agency guessed that he would guide the development of a new combat command from Langley. Given the fusion of intelligence with the modern military arts, we should urge the authors to offer insight on that challenge next!

By All Means Available: Memoirs of a Life in Intelligence, Special Operations, and Strategy

By Michael G. Vickers
Penguin Random House, 2023
544 pp. $35.00
ISBN: 9781101947708

Reviewed by Sandor Fabian and Kevin Stringer



In the 2007 movie "Charlie Wilson's War" Michael G. Vickers is depicted as CIA`s in-house weapons expert and a master chess player. Although he stated multiple times that in real life he does not play chess, his more than four decades of service in U.S. special operations, intelligence, and the Department of Defense demonstrated his genius at "playing the strategy game" against multiple adversaries across time and space. In his recently published memoir *By All Means Available: Memoirs of a Life in Intelligence, Special Operations, and Strategy*, Vickers masterfully assesses the most important intelligence and special operations missions over recent decades including his own roles and impacts.

Beyond Vickers` impressive career as a special operator, a CIA clandestine operator, an academic, and a high-ranking policymaker (including President George W. Bush`s Assistant Secretary of Defense for Special Operations, Low Intensity Conflict and Interdependent Capabilities and President Barack Obama`s Under Secretary of Defense for Intelligence) and the timeliness of his topic, what also makes his book an intriguing subject for review is the early praise it has received from many key figures across the defense enterprise. For example, Robert M. Gates, former Director of Central Intelligence and Secretary of Defense, said: "Vickers saw it all, experienced it all. Readers of his memoir are in for a rare treat and a gripping story." General Jim Mattis, U.S. Marines (Retired) and 26th Secretary of Defense, stated that Vickers`s "unique eyewitness insights reveal the passion and wisdom that gained him trust across all ranks and throughout Washington." And General Stanley McChrystal, U.S. Army (Retired), Former Commander of U.S. and Coalition Forces in Afghanistan, described the book as a "monumental memoir and thoughtful account of a uniquely tumultuous period in history. In a compelling narrative, Mike Vickers shares his front-row seat to the complex wars of our age." Such praise sets the bar very high for this book and motivated us to give it a particularly meticulous and critical read.

Sandor Fabian (Ph.D) is Chair of Engagements and Kevin Stringer (Ph.D) is Chair of Education at the Irregular Warfare Center.

To describe the purpose of his memoir and set the direction of the book, Vickers lists three reasons why he crafted this book in his prologue. All three reasons carry the common theme of duty. First, Vickers suggests that he had a duty to history since he played a central role in "world-changing" events. Second, he argues that crafting this memoir was also his duty to the American people to inform them about the critically important work our intelligence professionals, special operators, and defense and national security strategists have done and are doing today. Finally, Vickers states that it was also his duty to current and future special operators, intelligence professionals, and national security strategists to pass on to them what he learned over his decades long career.

To meet his purposes and present an engaging argument Vickers builds a simple but effective structure. He organizes the book into five parts (preparation, war with the Red Army, war with al-Qaeda, fighting on multiple fronts, and reflections); the first half follows a chronological path while the second half follows a thematic path.

In the first four parts of the memoir Vickers specifically focuses on his service spanning more than four decades. He dedicates just the right amount of attention to his personal career and spends more time on expanded discussion of events. He starts his journey down memory lane by describing early memories from his years with U.S. Special Forces (SF) starting in December 1973 when he reported to the Special Forces Qualification Course. After graduation from the course, he rose quite quickly through the enlisted ranks and was selected for Officer Candidate School (OCS). Vickers graduated from OCS in 1978 as an infantry officer, then in 1980 from SF Officers Course as the distinguished honor graduate. After his graduation he was deployed to Latin America several times where he commanded a classified counterterrorism unit.

Seeking more individual autonomy and responsibility and believing that the CIA was the best suited for fighting and winning the Cold War, Vickers decided to switch his career to CIA clandestine service in 1982. During his 3-year tenure with CIA Vickers served as the CIA's program officer and chief strategist for the Afghanistan Covert Action Program to force the Soviet army out of the country. Vickers provides substantial details about the program he led in Afghanistan, including the background on the decision he made to transform the program. In the chapters about the program Vickers presents a frank discussion about what went right and a bit surprisingly, what could have been done better. An especially interesting part of the book is his assessment of how the United States made a significant error when it assumed that Afghanistan lost strategic significance after the Soviet Army was repelled and defeated.

Next, Vickers devotes two chapters to an outstanding overview of the planning, preparation, and execution of Operation Neptune's Spear (the operation to capture or kill Osama bin Laden). Serving as the Assistant Secretary of Defense for Special Operations, Low Intensity Conflict and Interdependent Capabilities during most of the planning phase and then as Undersecretary of Defense for Intelligence during the preparation and execution phases, he has exceptional details on the various aspects of this mission and adds immensely to a reader's understanding of this operation. His discussion includes details about the numerous cabinet meetings conducted throughout the different phases, the assessment of bin Laden`s conjectured location, details of the raid planning and preparation, and the ultimate decision to execute the mission.

The analysis of *Operation Neptune's Spear* concludes the chronological part of the memoir, and Vickers shifts to a thematic approach in part four. He provides his personal high-ranking government official perspectives on topics like

counter-proliferation and counter-narco-insurgency; U.S. activities in Iran, Iraq, Syria, Yemen, and Libya (calling this part the "Battle for the Middle East); and crisis and change in the defense intelligence community. And this is where (quite surprisingly) the memoir nature of the book pretty much ends. Vickers departs from focusing on his career and the events of the past and offers an analysis of the present and future U.S. national security challenges in a chapter entitled "Winning the New Cold War." In this chapter Vickers specifically points to China and Russia as the primary adversaries of the United States in the New Cold War. Standing on realist theoretical grounds, Vickers argues that this conflict was generated by significant changes in the global balance of power, the West`s failure to fully integrate China and Russia into the U.S.-led rules-based international order, and China`s and Russia`s perception that the United States is a declining power. He shares his blueprint for a successful grand strategy with the readers and argues that it is based on five essential elements: the United States must restore national unity and resilience to the levels of the Cold War, position itself to prevail in the competition for technological and economic supremacy, execute and win intelligence and covert action wars, improve regional and global deterrence (if needed, defeat aggression), and transform the U.S. institutions and the alliance frameworks to meet the requirements of the New Cold War. Vickers posits the intriguing concept of escalation dominance throughout the book as the cornerstone of any successful strategy. Policymakers and military leaders would do well to examine the examples he offers of when the United States achieved it and when it did not.

The final part of the book focuses on emphasizing the lessons Vickers learned (and relearned) during his service in intelligence and covert action, special operations, and strategy. This part very effectively brings together the key points of the memoir and delivers more supporting analysis to emphasize their importance. Arguably the most interesting part of this section is the two sub-chapters in which Vickers warns the readers to remember that success is never final and offers his list of ten strategic leadership principles. Although some of Vickers principles might not relate to everyone, as a group they add value to the content of the book.

Vickers` memoir has many strengths that make it a must-have for many readers` bookshelves. First, his personal involvement in shaping critical world events and his willingness to discuss it in great detail are quite remarkable. His candid analysis of what worked and what did not is very refreshing, especially because his points do not come with any sense of bias. He does not shy away from critiquing himself. Second, Vickers` account is written in an engaging, conversational tone, making the reader feel like he is sitting next to the author and listening to his stories. Such tone makes the book easily readable for many readers. Third, the book is written in a way that carries significant value for special operators, intelligence professionals, and senior government officials, while it is also an interesting and informative volume for general readers who want to gain better understanding of world-changing events and how the world of today came to be. The final strength of the memoir worth mentioning is the nearly fifty pages long superb, annotated notes section adding extra details and helping to better understand Vickers`s key concepts. It adds a lot of value to the experience if readers indeed refer to these notes when prompted in the main text.

No book is without any weakness and Vickers` book is not an exception. Three areas stand out for constructive critique. First, memoirs are by nature self-congratulatory, yet Vickers would have strengthened his manuscript by greater reflection on the second and third order effects of his Afghanistan operations against the Soviet Union. The blowback in regards to al-Qaeda and Pakistan is huge,

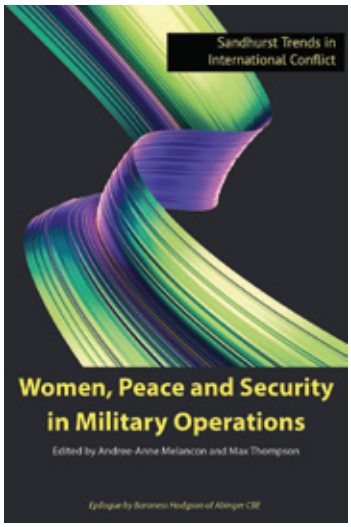
as documented in books like *Ghost Wars* by Steve Coll. Second, the analysis of the present and future U.S. national security challenges section feels quite detached from the previous parts of the memoir and creates an odd shift for the reader. Third, the author makes superficial evaluations of both Trump and Biden policy decisions, but the reader is not clear on why the actions receive a negative assessment. For example, Vickers criticizes Trump's decision to redeploy operators out of Somalia, labeling it unwise, but his substantiation is missing.

Overall, Vickers offers a masterful and engaging account of his remarkable career in *By All Means Available*. He delivered on all three of the objectives he described in the prologue. This account is much more than a traditional memoir. While it carries the usual characteristics of a memoir by re-living the past, it also offers a critical analysis of the present, and provides a blueprint for achieving success in the future. This book is a mandatory read for those who are in the business of special operations, intelligence, and strategy development. The movie "Charlie Wilson's War" is no longer the primary reference for understanding this patriot and his remarkable career. *By All Means Available* is.

Women, Peace and Security in Military Operations

Edited by Andree-Anne Melancon and Max Thompson
Howgate Publishing, 2023
247 pp. $75.99
ISBN 9781912440436

Reviewed by Cornelia Weiss



The Commandant of the Royal Military Academy Sandhurst, Major General Z.R. Stenning, OBE, in the foreword to *Women, Peace and Security in Military Operations*, writes, this book "should be required reading for security professionals." When I was the sole female military student in my war college class (2010-2011), I would have appreciated a book like this as required reading. I did have the great fortune to be taught peace operations by Brent Beardsley, General Romeo Dallaire's personal staff officer in Rwanda during the Rwanda genocide. He told me women are important. It was the first and only time in my military career I heard these words.

In June 2020, the U.S. Department of Defense issued its Women, Peace, and Security Strategic Framework and Implementation Plan (DOD SSFIP) to ensure "principles are appropriately reflected in relevant DOD policies, plans, doctrines, training, education, operations, resource planning, and exercises" (Intermediate Objective 1.2). In 2023, according to Tahina Montoya and Joan Johnson-Freese, the U.S. Air Force, through its Department of the Air Force Women, Peace, & Security Strategic Action Plan (DAF WPS), "became the military department to establish *how* its services—the Air Force and the Space Force—would implement WPS."[1] The DAF WPS addresses proposed DAF metrics through DAF WPS Objective 2: "Employ WPS on Operations and Exercises."[2] For operations, the DAF WPS has one metric: "breakdown of metrics for operations . . . by rank and gender."[3] The strength of *Women, Peace & Security in Military Operations* is that it goes beyond counting. An edited volume, it addresses military operations, while also exploring needed analysis, education, and training.

Military operations include the withdrawal from Afghanistan in 2021, as well as actions taken (and not taken) during the twenty years of international military presence in Afghanistan. Evacuating hundreds of Afghan cats and dogs while abandoning Afghans, "especially women," is an issue Sanam

Cornelia Weiss is a former U.S. Air Force Colonel.)

Naraghi Anderlini raises in this book's introduction. Anderlini appears to argue that the failure to uphold the WPS agenda enabled the Taliban. For example, she highlights the connection between the arguably "deliberate" failure of Zalmay Khalizad (the U.S. negotiator of the agreement with the Taliban) to include women in the negotiations and the Taliban's increased targeted killings of women during negotiations. Khalizad is married to the author of *Veiled Courage: Inside Afghan Women's Resistance*.[4] Thus, it is unclear why Khalizad appeared to ignore the U.S. Women Peace and Security Act of 2017 (WPS Act), an Act "[t]o ensure that the United States promotes the meaningful participation of women in mediation and negotiation processes seeking to prevent, mitigate, or resolve violent conflict."[5] The WPS Act highlights research suggesting "peace negotiations are more likely to succeed and to result in durable peace agreements when women participate in the peace process."[6] Whether, and to what extent, the failure to include women affected and affects military operations, as well as the lives of U.S. and other military members, is needed research.

Military operations include peace operations. An Jacobs and Katerina Krulisova address failures of gender mainstreaming in peace operations, to include the practices of simply resorting to "box-ticking." Steve Maguire uses Judith Steihn's three "I" framework (inertia as well as the failure to implement and institutionalize) to address absences of operationalized WPS in both UN peace operations and the British Army. Examining the work of Irish Major General Maureen O'Brien, a veteran of numerous peace operations and most recently the Deputy Military Advisor to the UN Secretary-General, opens a treasure chest of solutions. Here are two. In response to the "culture" excuse by a troop contributing country (TCC) for excluding women in military police units, General O'Brien informed the TCC that including women was the UN culture, and if the TCC did not change, the UN would replace it; the TCC then determined that including women was their culture.[7] When observing that women were being "corralled" into "engagement" platoons simply because they were women (not because of their particular qualifications), General O'Brien mandated engagement teams were to be composed fifty-fifty of trained men and women.[8]

Military operations, under WPS, should prevent rape and other forms of sexual violence, to include in civil conflicts. Korean Marine Corps veteran Changwook Ju, using a data set of the years 1980-2009, finds that in civil conflicts "women's combat participation in state forces leads to the groups' higher level of wartime rape" and the "presence of women combatants decreases the prevalence of wartime rape by rebel forces." Curious about which state forces did not exclude women as combatants in the 1980s, 1990s, and the 2000s, I obtained the data set from its creator, Meredith Loken. The data set reveals only four state forces not excluding women as combatants: Israel, Liberia, Rwanda, and Democratic Republic of Congo/Zaire; less than 10 percent of the total number of state forces included in the data set. The value of the data set is that it makes visible state forces not committing rape in civil conflicts during this time period: Azerbaijan, China, Croatia, Georgia, Indonesia (OPM), Lebanon, Liberia, Mali, Morocco, Mozambique, South Africa, and the UK. I recommend investigating why these state forces did not rape. Factors might include leadership, discipline, professionalism, morality, and/or fear of punishment. Such research might also help to end rape by state forces outside of civil conflicts—for example, the UK in Kenya.[9] At minimum, preventing rape, to include by state forces in civil conflicts, is a subject that should be taught in professional military education (PME). Yet regarding a paper of mine about creating counter-strategies to prevent rape as a weapon of war, one U.S. PME peer reviewer admitted: "If the problem resides among the militaries of

other nations and the policies they pursue toward legitimizing rape, what is it that the U.S. PME institutions and leadership are expected to do to counter such matters? Those listed in the examples . . . are rarely, if ever, trained in U.S. PME schools, and there is no indication given that this is a similarly systematic problem within the U.S. military or its policies."

Military operations include military and governance missions. Given his personal involvement as a governance advisor and course curriculum developer, Spencer Meredith addresses the long history of the United States using military forces to govern and states the U.S. Army Special Warfare Center and School "revised its governance curriculum in 2019, focusing on governance as a battlefield for influence" and legitimacy. I urge military schools to include General Douglas MacArthur's first demand for reform to the Government of Japan in post-World War II Occupied Japan; that is, the "emancipation of women."[10] Preceding UNSCR 1325 by over a half-century, General MacArthur's women's emancipation policy provides a blueprint for implementing WPS. However, to the best of my knowledge, paid PME educators fail to teach it, to include in U.S. Army PME. Yet General MacArthur's women's emancipation policy is part of U.S. Army heritage. The failure to teach it harms military operations. One only needs to read, for example, Nadje al-Ali and Nicola Pratt's *What Kind of Liberation: Women and the Occupation of Iraq* to understand how.[11]

Military operations include countering insurgencies and terrorism. U.S. Air Force Major Kelly Atkinson argues the U.S. "hearts and minds" approach is transactional, whereas WPS is transformational. If we examine the 2006 U.S. Counterinsurgency manual (FM 3-24/MCWP 3-33.5), we find a section titled "Engage the Women, Beware the Children," with the arguably transactional language of "co-opting . . . women."[12] In contrast, the drafters of the 2021 validated U.S. Counterinsurgency manual (JP 3-24) have excised the "co-opting women" language. Instead, JP 3-24 has a section titled "Females as Insurgents,"[13] as well as sprinkled language regarding the reintegration of women[14] and political reform.[15] To get to transformational, I recommend the U.S. military include Major Atkinson as a drafter of the next iterations of the U.S. Counterinsurgency manual.

Military operations include the cyber domain. Alexis Henshaw, whose work on Colombia has influenced me, addresses the cyber domain through the WPS pillars of participation, protection, prevention, relief and recovery, and institutionalization. Henshaw raises numerous concerns. They include the biometric data the U.S. military collected on millions of Afghan citizens falling into the hands of the Taliban, online radicalization and armed attacks, and the harassment and discrimination by men against women working in cybersecurity and the resulting attrition of women. The cyber domain also offers positive possibilities. Sola Mahfouz (now a quantum computing researcher at Tufts University Quantum Information Group), when prevented from attending school in-person in Afghanistan, completed her education without a bricks-and-mortar school; she learned online through the Khan Academy.[16] Mahouz also enhanced her English through "an online language-learning platform that matches language learners with native speakers."[17] She needed to learn English for an exam to prove English proficiency to attend a U.S. university. The stumbling block to her education was a male interviewer at the U.S. embassy in Kabul. He rejected her application for a visa to study in the United States because "he didn't believe I was really going to America to study."[18] Through the online tools of email and Skype, a reporter from *The New York Times* was able to interview her and then publish a story about Mahfouz's plight. Eventually the U.S. embassy did issue her a visa. The experiences

of individuals like Mahfouz are a first step in demonstrating how the cyber domain can also help actualize the WPS pillars.

The book also provides frameworks for enhancing operational effectiveness through WPS analysis. Whitney Grespin uses the PMEII-PT (Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time) tool as a gender analysis for Djibouti, while also examining Cori Flesher's gender analysis for Ukrainian security assistance. Colonel (ret.) Jody Prescott and Robin Lovell urge using a socio-ecological system (SES) approach "to better identify geographical areas at the highest risk of any compounding effects of armed conflict, climate change, and gender inequality." Prescott and Lovell compare the SES approach with NATO's military gender analysis method and argue that the "standard NATO gender analysis is not well-suited to analyzing the complex relationships between social and environmental factors that characterize the intersections between armed conflict, gender inequality, and climate change and environmental degradation."

The book further explores WPS in PME and training. In their chapter on education, Max Thompson and Andree-Ann Melancon address their experiences in integrating WPS in PME at the Royal Military Academy Sandhurst. As part of their approach, they utilize an academic exercise they call "Ex Complex Terrain" to assess conflicts. It involves a group Conflict Analysis Report (CAR) and a timed, open book individual Human Security Individual Assessment (HSIA). According to them, the best CARs also "consider CRSV, child soldiers, disruptions to health and education services," and human trafficking. The HSIA list of ten metrics includes "women and children." To avoid appearing to fall into the "womenandchildren" nomenclature, it might be an interesting experiment to instead permit students to choose one of the following categories: women, men, girls, boys, non-binary, trans, and intersex. The chapter's authors also use an exercise they call "Ex TEMPLER'S TRIUMPH" in which they insert the WPS agenda. My favorite part of the chapter is their caution to "don't get too academic about it – WPS education does not require a comprehensive course on feminist and critical approaches to IR." I agree. Using terms that belong in the glossary of a WPS book creates cognitive overload, to include the words "gender mainstreaming" and "hegemonic masculinities." Given that one misconception about WPS is that WPS imposes "Western beliefs on another country,"[19] WPS educators must know, and be able to explain, the history of the creation of UNSCR 1325. Namibia, not "Western" states, used its position on the UN Security Council to create UNSCR 1325.[20]

This fourth book in the Sandhurst Trends in International Conflict series concludes with an Epilogue by Baroness (Fiona) Hodgson of Abinger CBE, Co-chair of All Party Parliamentary Group on Women, Peace & Security and Hon Col 77th Brigade Outreach Group. In 2022, the Baroness introduced the Women, Peace and Security Bill in the House of the Lords.[21] As of 6 September 2023, it still is not law.[22] This book, as the Baroness writes, "serves as a reminder of how far we have come, but also how much work is still to be done."

Notes

[1] Tahina Montoya and Joan Johnson-Freese, "From Exception to Norm: Closing the Women, Peace and Security Implementation Gap Through Joint Professional Military Education," Modern War Institute, 12 July 2023, https://mwi.westpoint.edu/from-exception-to-norm-closing-the-women-peace-and-security-implementation-gap-through-joint-professional-military-education/.

[2] Department of the Air Force (DAF) Women, Peace, & Security (WPS) Strategic Action Plan (CAO: April 2023), https://www.af.mil/Portals/documents/2023SAF/DAF_WPS_Strategic_Action_Plan.pdf [hereinafter DAF WPS]: 15-16.

[3] DAF WPS, 15.

[4] Cheryl Bernard (in cooperation with Edith Schaffer), *Veiled Courage: Inside Afghan Women's Resistance* (New York: Broadway Books, 2002). Cheryl Bernard, "Afghan Women are in charge of their own fate," *National Interest*, February 27, 2017, https://nationalinterest.org/feature/afghan-women-are-charge-their-own-fate-45777.

[5] Women, Peace, and Security Act of 2017, Pub. L. No. 115-68 (2017), https://www.gov/app/details/PLAW-115pub168 [hereinafter WPS Act].

[6] WPS Act, Sec 2(3).

[7] "Advancing the Women, Peace and Security Agenda," IIEA, June 16, 2023, at 26:50 – 27:07, https://www.youtube.com/watch?v=qTOPdAU42NE [hereinafter "Advancing WPS"].

[8] "Advancing WPS," at 13:00 – 14:06.

[9] Rebecca Cook and Cornelia Weiss, "Gender Stereotyping in the Military. Insights from Court Cases," in Eva Brems and Alexandra Timmer (eds), *Stereotypes and Human Rights Law* (Cambridge: Intersentia, 2016): 194.

[10] Cornelia Weiss, "The Nineteenth Amendment and the U.S. 'Women's Emancipation Policy' in Post-World War II Occupied Japan: Going Beyond Suffrage," *Akron Law Review*, Vol. 53, No. 2 (2019), https://ideaexchange.uakron.edu/akronlawreview/vol53/iss2/4/.

[11] Nadje al-Ali and Nicola Pratt, *What Kind of Liberation: Women and the Occupation of Iraq* (Berkeley: University of California Press, 2009).

[12] Headquarters Department of the Army, FM 3-24, MCWP 3-33.5, Counterinsurgency, December 2006, 192.

[13] Joint Chiefs of Staff, JP 3-24, *Counterinsurgency*, 25 April 2018, Validated 30 April 2021 [hereinafter JP 3-24], II-9, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3-24.pdf.

[14] JP 3-24, III-34.

[15] JP 3-24, V-12.

[16] Sola Mahfouz and Malaina Kapoor, *Defiant dreams: the journey of an Afghan girl who risked everything for education* (New York: Ballantine Books, 2023).

[17] Mahfouz, *Defiant dreams*, 197.

[18] Mahfouz, *Defiant dreams*, 221.

[19] Barbara Salera Lopez, "An Ancillary Duty? The Department of Defense Approach to Women, Peace, and Security in Security Cooperation Programs," forthcoming in *Prism*.

[20] Cornelia Weiss, "Creating UNSCR 1325: Women who served as initiators, drafters, and strategists," in Rebecca Adami and Dan Plesch (eds.), *Women and the UN: A New History of Women's International Human Rights* (New York: Routledge, 2022).

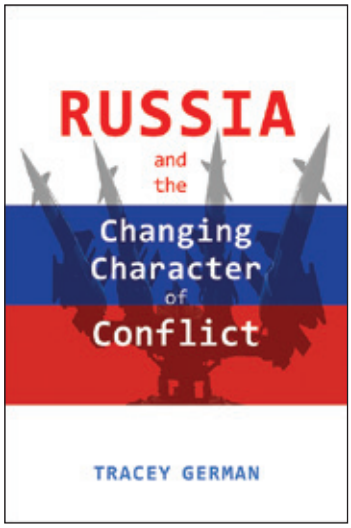
[21] UK Parliament, House of Lords Business, "Women, Peace and Security Bill [HL] Baroness Hodgson of Abinger presented a bill to support women in UK sponsored and supported conflict prevention, peace processes, mediation and diplomatic delegations; to ensure systematic gender consideration and responsiveness in UK foreign and defence policy; and for connected purposes," 8 June 2020 at 15:50, https://lordsbusiness.parliament.uk/

[22] Women, Peace and Security Bill [HL], last updated 6 September 2023, https://bills.parliament.uk/bills/3178.

Russia and the Changing Character of Conflict

By Tracy German
Cambria Press, Amherst, NY, 2023
280 pp. $109.00
ISBN: 9781621966753

Reviewed by Jeffrey Mankoff



The failure of Russia's initial foray into Ukraine in the spring of 2022 and the ensuing war of attrition between Russian and Ukrainian forces is already forcing military analysts to rethink long-standing assumptions about the character of 21st century warfare—a task perhaps more urgent in Russia than anywhere else. As Tracy German shows in her new book on the development of Russian military thought, Russia's early failures in Ukraine stemmed not only from an underestimation of the Ukrainians' will to resist and the scale and scope of Western support, but also from how Russian military thinkers had come to think about the character of modern war. As German shows, the Russian military has remained wedded to a particular way of fighting that failed to account for the ways in which a smaller, more nimble enemy could blunt Russian firepower and force Russia into a long attritional fight that will stress its economic and political order as well as its military.

German's *Russia and the Changing Character of Conflict* was already in the works when Russian forces invaded Ukraine *en masse* in February 2022. The book is not, therefore, primarily a postmortem on the Russian invasion, though it does provide some analysis of what went wrong with the initial stages. Rather, the primary task German sets herself is to analyze and explain how Russia has prepared to fight over the past few decades. Her book is less about the reorganization of the Russian military itself than about the ideas of the military thinkers who have provided the intellectual framework for organizational and operational decisionmaking in both peacetime and wartime. The first section addresses thematic topics, including the Soviet legacy, the role of the West as a template, and integrating operational experience from Russia's own wars in Chechnya, Georgia, Syria, and Ukraine. The longer second section looks at doctrinal and operational debates around such issues as the impact

Dr. Jeffrey Mankoff is a Distinguished Research Fellow, Russia and Eurasia at the Institute for National Strategic Studies, National Defense University.

of technology, information operations, and the role of proxy forces like the infamous Wagner Group. A final chapter raises the question of whether Russia learned the wrong lessons, leading it to fight a war in Ukraine for which it had not prepared.

A great virtue of German's book is that it surveys the entire landscape of Russian military thought. Perhaps surprisingly to Western audiences, what Russian thinkers term "military science (*voennaya mysl'*)" remains characterized by very public debates between proponents of different ideas about the character of war and how Russia should adapt to it. In each of her chapters, German shows how dominant ideas (for instance, about the importance of precision munitions in modern war), emerged despite challenges from within the military science community. This debate and others like it played out in the pages of the publicly available military journals that German mined for her research. The picture they paint is of an analytic community willing to challenge one another, but blind to some larger cognitive and conceptual biases afflicting that community as a whole.

Among the most enduring forces shaping Russian military thought is the legacy of the Second World War (which Russians call the Great Patriotic War). Even though the USSR was eventually on the winning side, the war was disastrous for the Soviet Union and its people: much of the war on the Eastern Front took place on Soviet territory, and around 27 million Soviet citizens lost their lives as a result of the war. The war produced a strong "never again" ethos among Soviet and, later, Russian thinkers. Postwar analysts pointed to the Germans' ability to achieve the element of surprise in June 1941 as instrumental to their initial success. They consequently emphasized surprise, the need to maintain the operational initiative (the "cult of the offensive") and the importance of the initial stages of conflict. Soviet/Russian military thinking about defensive operations, and about the factors that might allow an enemy to resist or parry such an overwhelming thrust, were comparatively ignored.

If World War II remains the reference point for much of Russian "military science," the template and the mirror against which the Russian military tends to compare itself is the United States. The centrality of the United States as a reference point is a result not just of the Cold War, but also of the more recent history of U.S. military interventions, notably those against Iraq (1990 and 2003-2017), Yugoslavia (1999), Afghanistan (2001-2021), and Libya (2011). Russian observers have been impressed by the U.S. military's ability to devastate enemy forces and, at times, topple enemy governments while incurring minimal casualties among its own forces (though they seemingly paid less attention to the struggles the United States subsequently faced confronting insurgents).

Washington's ability to dismantle the Iraqi military from the air (as it had done a few years earlier in Yugoslavia) and march nearly unopposed into Baghdad appeared to many Russian thinkers a watershed in the history of warfare, inaugurating what the influential military theorist Vladimir Slipchenko termed "sixth generation" warfare. According to Slipchenko, sixth generation warfare was characterized by its "contactless" nature, with an emphasis on airpower, precision munitions, cyber tools, and other capabilities to target enemy forces without having to engage in bloody infantry or armor battles. Meanwhile, Russian forces in Chechnya remained engaged in what Slipchenko characterized as "fourth generation" mechanized warfare similar to World War II. Other Russian theorists used different terminology (e.g., "non-contact warfare"), but they were largely in agreement by the early 2000s that the fundamental character of war had changed, that the United States was at the forefront of these changes, and that Russia had to quickly adapt.

Among Slipchenko's backers were some of the key figures in translating the ideas of Russian

military theorists into doctrinal and organizational reality. They include retired General Makhmut Gareev, longtime head of the Academy of Military Sciences and Slipchenko's sometime co-author, as well as General Valery Gerasimov, chair of the Russian General Staff and overall commander of the war effort in Ukraine. Gerasimov became notorious in the West for his 2013 article "The Value of Science is in the Foresight," which applied many of the ideas developed by Slipchenko, Gareev, and others to thinking about how Russia should adapt for a world of competition with the United States in which information and other non-kinetic tools would be employed alongside traditional weapons.

For Gerasimov and his intellectual forebears, the focus on information operations and other dark arts was less a specifically Russian way of war (there is no Gerasimov Doctrine, in other words), but rather a diagnosis of the character of 21st century war and a prescription for Russia on how to fight it. One of Gerasimov's major theses was that "the role of non-military means of achieving strategic and political goals has grown, and in many cases, they have exceeded the power of force of weapons in their effectiveness." Recognizing that it was not just the military that determined how and for how long a war would continue, Gerasimov prioritized measures that would undermine social cohesion and the will to fight among members of the government and society at large.

Here too, Gerasimov (and his intellectual progenitors) was drawing on a Soviet legacy. What had changed, however, was the increasing informatization of modern societies. Gerasimov noted that the United States had been able to paralyze Iraqi decisionmaking through information and cyber measures even before it started carrying out airstrikes against Saddam Hussein's troops. For Gerasimov and other leading Russian thinkers the combination of precision weapons and information operations offered a package that could be deployed in tandem to quickly paralyze the ability of an enemy to continue the fight. Russian military planning came in the 2010s to emphasize this combination, on the assumption that achieving the element of surprise and sustaining the strategic initiative would allow Russia to avoid being drawn into a long, grinding conflict like World War II or the first Russian war in Chechnya.

Another characteristic of Russian military thinking that German emphasizes is the fluid boundary between peace and war—and, consequently, the importance that Russia places on non- kinetic or grey zone activities as part of its toolkit for strategic competition away from the battlefield. As German shows, the emphasis on information and cyber tools at once harkens back to the Soviet notion of "reflexive control (*refleksivnyi kontrol'*)"—shaping an adversary's decisionmaking calculus such that he willingly behaves in the way you desire—and stems from a more recent perception that the United States and other democracies are uniquely vulnerable in the information space.

In taking their inspiration from the United States, Russian military thinkers looked back not only to U.S. military deployments, but also to what they saw as U.S.-led or U.S.-inspired efforts at regime change using non-kinetic means—specifically the "color revolutions" that sparked regime change in Georgia (2003) and Ukraine (2004), as well as the later Arab Spring uprisings. Most mainstream Russian thinkers viewed the color revolutions not as spontaneous uprisings against corruption and misrule, but as deliberately engineered campaigns by Washington to transform Georgia and Ukraine into outposts of the Euro-Atlantic West. Russian fury about the color revolutions produced a whole genre of writing about what the military theorists A.N. Belsky and O.V. Klimchenko describe as "color revolution engineering." Along with other prominent military thinkers, Belsky and Klimchenko assert that the United States

deliberately provoked the color revolutions because Washington remains engaged in a struggle with Moscow over control of post-Soviet Eurasia, with the United States seeking to isolate and surround Russia to prevent its re-emergence as a strategic rival.

Taken aback by not just the color revolutions themselves, but what they saw as Russia's defeat in the information space during the 2008 invasion of Georgia, Russian military thinkers subsequently set out to develop new doctrinal and technical capabilities to ensure Russia would remain at the forefront of the "information war (*informatsionnaya voina*)" with the West. Russia's embrace of information and cyber operations is therefore part of a larger strategy of confrontation that aims to destabilize adversarial states from within and stir up unrest in the way that Russian analysts believe the United States did during the color revolutions in Georgia and Ukraine.

In the last chapter of her book, German digs into the question of how "military science" led the Russian military astray in Ukraine. She particularly emphasizes how Russia's top-down military culture and emphasis on firepower led Moscow to systematically underestimate the importance of intangible factors like morale. Ukrainian forces may have been outmanned and outgunned, but they had the advantage of knowing what it was they were fighting for. Ukraine was also able to disaggregate its forces and push initiative down to lower levels of command in ways that vitiated the Russian emphasis on paralyzing decisionmaking in the initial phase of the war. Unlike how Russia's own military was structured, the Ukrainians did not have a single point of failure that Russian artillery, drones, or information operations could target. And while precision weapons may have been instrumental in U.S. combat operations against second-rate armies like those of Iraq or Yugoslavia, the efficacy of such weapons dropped substantially when confronted with robust Ukrainian air defense capabilities (nor did Russia have precision munitions in anywhere near the quantity that the United States did, limiting their use in a protracted conflict).

The intellectual culture that German describes has made the Russian military a formidable force. Yet the emphasis on seizing the initiative and applying overwhelming force created blind spots that led commanders and decisionmakers to underestimate the difficulties they would face in Ukraine, and could prove even more problematic in a conflict against a peer force. Despite these failures, German is in the camp of analysts who see the Russian military as an adaptable organization. Battlefield developments in the year-plus since German's book was published seem to support that thesis. The war that Russia prepared to fight was not the war it ended up fighting in Ukraine. That it has nonetheless adapted in the face of high casualties and unprecedented sanctions suggests that it would be a mistake to underestimate Russia as an adversary. Western analysts will also need to continue paying attention to debates among Russian military thinkers now that they have new experience and new information from two years of high-intensity combat. It is not just the West that is learning (and re-learning) lessons in Ukraine.

SUBSCRIPTIONS

Keep up to date with global and national security affairs, including sources, effects, and responses to international insecurity, global policy and development, nation-building and reconstruction, counterinsurgency, and lessons learned. To request your journal of complex operations, contact the *PRISM* editorial staff at <prism@ndu.edu>. Please include your preferred mailing address and desired number of copies in your message.


NATIONAL DEFENSE UNIVERSITY


PRISM
SCIRE QUOD SCIENDUM


IRREGULAR
WARFARE CENTER