PRISM

VOL. 9, NO. 3 | 2021

THE JOURNAL OF COMPLEX OPERATIONS

PRISM
VOL. 9, NO. 3, 2021

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."

PRISM is published with support from NDU's Institute for National Strategic Studies (INSS). In 1984, Secretary of Defense Casper Weinberger established INSS within NDU as a focal point for analysis of critical national security policy and defense strategy issues. Today INSS conducts research in support of academic and leadership programs at NDU; provides strategic support to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, combatant commands, and armed services; and engages with the broader national and international security communities.

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 We also welcome Letters to the Editor that are exclusive to PRISM—we do not publish open letters.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 Editor260 Fifth Avenue, S.W. Building 62, Suite 212 Fort Lesley J. McNair Washington DC 20319

DISCLAIMER

FEATURES

INTERVIEWS

BOOK REVIEWS

PRISM VOL. 9, NO. 3

2021 www.ndu.edu

Zurab Tsereteli's monument to Peter the Great. Памятник Петру Первому / Monument to Peter the Great (AlphaTangoBravo / Adam Baker is licensed with CC BY 2.0.)

The Origins of Russian Conduct

By Clint Reach

In 1947 George Kennan argued for a policy of U.S. containment of the Soviet Union based on his assessment of the origins of Soviet conduct. Because the Kremlin was ideologically bent on global domination through a zero-sum competition with the West, political accommodation was not an appropriate strategy. Fifty years after the "X" article appeared, Kennan saw in the Russian Federation a wholly different animal than its Soviet predecessor. Russia was in the early stages of democracy, and its development should be shepherded by a magnanimous West. Based on this updated view of Russia, Kennan asserted that the enlargement of NATO would be "the most fateful error of American policy in the entire post-cold-war era."[1] Implicit in Kennan's argument was that the nature of the new Russian regime was not inherently antagonistic toward the United States and the West. There was not an underlying ideology or feature of the new political and economic system that led him to conclude that confrontation with Russia was unavoidable or that cooperation was impossible. This assumption turned out to be one of the critical dividing lines in the debate on how to deal with the Russians after the Cold War, and it is implicitly found in discourse on Russia policy that continues to this day.[2]

What are the origins of Russian conduct? Has Russian domestic and foreign policy predominantly been the result of misguided U.S. and European actions? Would the Kremlin have behaved differently if these policies had been more accommodating to Russia as a separate but equal partner in European integration? As in 1947, the answers to these questions are directly tied to current and future U.S. policy toward Russia. Those who believe Russian conduct is largely a reaction to Western actions that threaten Russia's core strategic interests are likely to promote policies guided by a sense of compromise.[3] Those who believe Russia would have acted similarly even if NATO had been disbanded or if the West had been more sensitive to Russian interests likely support a tougher military and diplomatic line with Russia and will be less interested in engagement. Yet there is rarely a full examination of the underlying reasons for promoting a particular approach.[4] It is often taken as a given that we can do business with Russia or we cannot. To develop an optimal strategy toward Russia, it is important to clearly articulate a reasoning for coming to one conclusion or the other.

Kennan's reasoning was that Russia in the 1990s was on a path toward becoming a member of the European project. Russian embrace of Western political norms would mitigate the potential for the

Clint Reach is a policy analyst at the nonpartisan, nonprofit RAND Corporation. Reach served in the U.S. Navy from 2005 to 2014 as a Russian linguist.

reemergence of dividing lines and the need for American security guarantees in areas of historical Russian influence. The United States, however, was considering actions that would derail this process by fomenting nationalist and militaristic sentiments within Russia that might otherwise be marginalized due to the lack of a legitimate Western threat. The extent to which this turned out to be the case is difficult to determine. Since the late 1990s, there have been a number of U.S. and Russian actions outside the NATO enlargement dispute that have muddied the analytical waters. But, as Kennan said, "The attempt must be made if [Russian] conduct is to be understood and effectively countered."[5]

Historical Background

The Soviet Union was neither militarily defeated nor forced to succumb to the political preferences of its opponent. Leaders in the Kremlin instead allowed the entire system to fall without much resistance. The Cold War ended with more of a truce than a peace. The Russian Federation under Yeltsin nevertheless behaved as a relatively willing participant in the political and economic integration processes of the West. There was genuine interest among Yeltsin's reformist team in charting a new domestic and foreign policy course for Russia.[6] Yeltsin himself stated that "Russia had to rid itself of its imperial mission."[7] Russian strategy documents from the early 1990s envisioned that at some point in the future Russia would pursue an alliance with the United States, perhaps even within NATO.[8]

As Russia was in the throes of young democracy and the transition to market capitalism, discussions began in the West on the enlargement of NATO into former Warsaw Pact countries. Then NATO intervened in the former Yugoslavia. Russia to some extent vacillated on the NATO enlargement threat, with the military most fervently against, and it was almost unanimously opposed to the military action in the Balkans.[9] But in the early 2000s, Russian President Vladimir Putin—who succeeded Yeltsin in 2000—was not prepared to write off a strategic orientation toward the West, a policy even his Chief of the General Staff endorsed in 2004.[10] Putin's speech to the German Bundestag in 2001 and his immediate offer to assist the United States in the aftermath of 9/11 affirmed this position. In May 2004, after the accession of six countries to NATO, including Estonia, Latvia, and Lithuania, Putin's speech to the Federal Assembly welcomed the expansion of the European Union and "new possibilities for the future of Greater Europe."[11]

There were no immediate overt signals in the early 2000s that Russian political leadership saw NATO enlargement as a grave threat to its security or Western-leaning foreign policy objectives, although there were clearly misgivings in some circles. Russia did strongly object to the U.S. withdrawal from the Antiballistic Missile (ABM) Treaty in 2002 and the U.S.-led invasion of Iraq in 2003, and Russian frustration with U.S. foreign policy writ large famously boiled over in Putin's 2007 speech to the Munich Security Conference.[12] But Russian military reforms begun a year later in 2008 led to a large reduction in the armed forces based on the premise that local military conflicts along the periphery were most likely and that the probability of large-scale war was low (an assessment that remained true even after the 2014 crises in Ukraine).[13] The Russian war with Georgia in 2008 was followed by a "reset" in U.S.-Russia relations, and the last U.S. tanks departed Europe in 2013.[14] There were, though, sufficient indications during the time period up to 2014 that Russia's problem with the United States and its allies was more fundamental than a military threat from NATO.

Of greater consequence was what was happening within Russia, where the Kremlin by 2003 had taken a number of steps to establish greater control over the domestic political situation.[15] Putin, often described as a statist deeply affected by the calamitous political

and economic times of the 1990s, believed that for the state apparatus to function effectively it must not be challenged by independent actors with the means to potentially supplant his authority.[16] The information environment—e.g., large television broadcast companies—was quickly shored up under direct or indirect state control. The "commanding heights" of the economy suffered a similar fate, as Putin delivered an unequivocal message to the Russian captains of industry to maintain their loyalty to the Kremlin above all else.[17] The remainder of Putin's second term focused on the consolidation of "sovereign democracy," which outside observers have described as a euphemism for authoritarianism.[18]

NATO intervention in Libya and the 2011-2012 street protests throughout Russia essentially spelled the end of the "reset" and any potential constructive U.S.-Russia relationship in the near term. Dmitri Trenin described the events that followed Putin's return to the presidency in 2012 as Russia's "breakout from the post-Cold War system."[19] According to Trenin, Putin during his tenure as Prime Minister had explored the possible religious underpinnings of a new national idea for the Russian Federation, one that was distinct from the greater West. Although political usage became more common in the early 2000s, Russian leadership increasingly began to embrace the idea of Russia as a Eurasian power that would project and protect so-called traditional values and conservative culture.[20] In 2011, Putin promoted not the path of Austria, Sweden, or Finland, who have chosen to remain outside of NATO but acceptant of the overall political and economic vision of the continent, but the creation of a Eurasian Union.[21] It was in fact this new union, which Putin later described as a distinct political and economic counterpart to the EU, that collided with the West and sparked the Maidan protests that have been disastrous for Ukraine and to some extent for Russia as well.[22] The centrality of this initiative to Russia's vision for the region cannot be overstated, and it is arguable that a Eurasian Union that includes Ukraine, Georgia, and Moldova remains a long-term objective for the Kremlin.[23]

U.S. – Russian security cooperation of the 1990s seems a remote possibility today. (BalkanPhotos is licensed with CC BY-NC 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc/2.0/) November 7, 2016

Need It Have Been So?

Post-Cold War history has shown that there is a deeper problem in U.S.-Russia relations that transcends NATO enlargement or Western policies that threaten Russian security. The Western interventions in Yugoslavia, Iraq, and Libya were perceived by the Kremlin as a pattern that could be repeated in Russia, although this is highly improbable. These actions were the United States and allies simply conducting foreign policy as they saw fit in pursuit, however clumsily, of a generally agreed upon vision and set of guiding principles. The actions did not paint Russia into a corner from which its only escape was to engage in full-blown confrontation to sow discord within European and American societies. Had Russia remained on a path toward political reform along the Western model and sought to integrate more closely with the European Union, would it have seen U.S. action in Libya as a national security challenge? States that generally are pursuing the same regional and global vision are theoretically much less likely to resort to the means Russia has as a way to express displeasure with a counterpart's behavior. China did not harangue Russia at a security conference after Moscow violated Georgian and Ukrainian sovereignty and territorial integrity, nor did German or French displeasure with the U.S. decision to invade Iraq result in an irreparable fallout in relations.

In fact, most consequential is the incompatibility of the U.S. and Russian political systems (and great power mentalities), which are an outgrowth of geographic, historical, and cultural influences on the formation of a governance model, national interests, and foreign policy. Russia likely could not have "fit" in Europe regardless of what the West plausibly might have done.[24] Russia finds itself once again at odds with the United States less because of individual foreign policy actions on either side, but because Russia's chosen domestic course, and the resultant regional vision, is difficult to reconcile with the Western development project that majorities in nearly every other country in Europe accepts as the best available option.[25] Friction is created by alternative development models seeking to expand their respective influence, which turns what might otherwise be resolvable disputes among like-minded states into more intractable challenges.

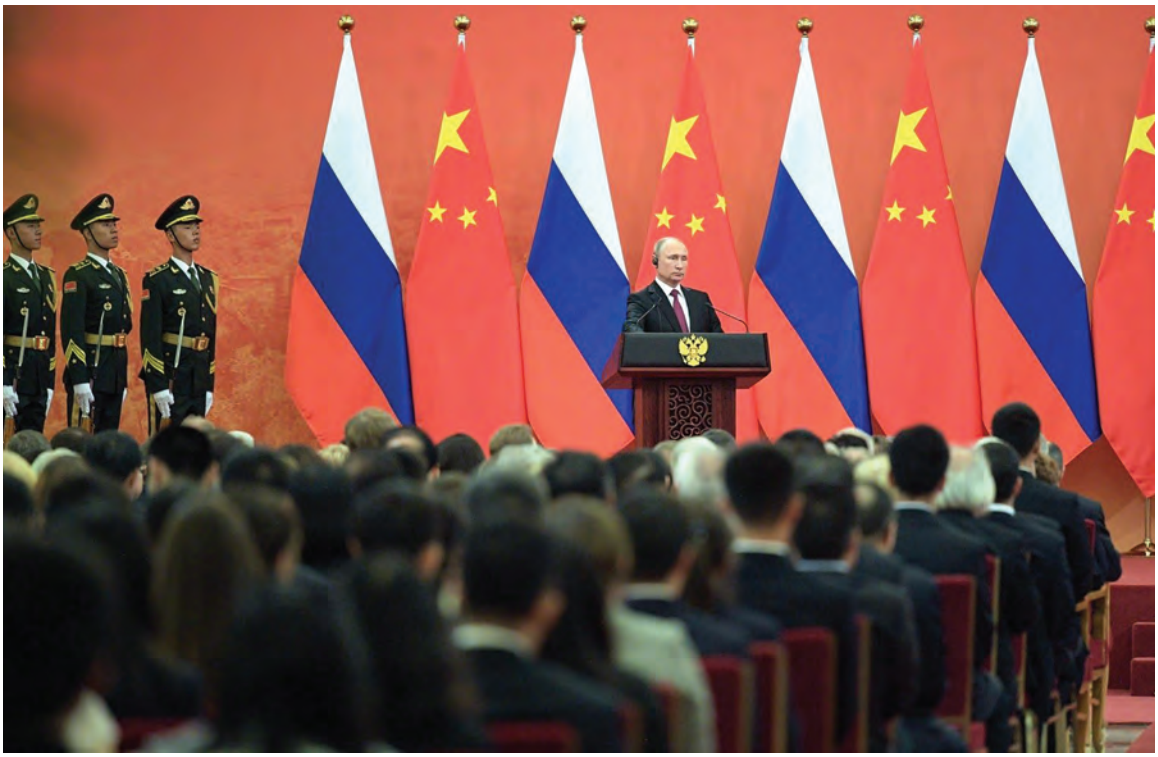
The Russian decision to adopt "sovereign democracy" in 2002-2003 was the most pivotal moment in the relationship, and it was not connected to NATO or EU enlargement or the U.S. withdrawal from the ABM Treaty. Russia in fact was not on the sustainable path to liberal democracy that Kennan foresaw in 1997. Russia's choice of a governance model was rather the latest incidence of a history of conservative triumph over liberal reformist forces in Russia, a lopsided battle that has been under way for at least two centuries.[26] It was not a result of marginal Russian political figures empowered by U.S. recklessness. And because of Russia's geographic location on the eastern edge of Europe, the clash of governance models is more consequential than if Russia's neighborhood were on another continent. In Europe as it is today, virtually united on questions of governance, economics, and security, an alternative development model requires an alternative alliance or strategic partnership for Russia, the isolation of which would be "unenviable," as General Yurii Baluevskii and military futurist Musa Khamzatov euphemistically described it in mid-2014.[27]

Critics of U.S. foreign policy in Europe have argued that as a great power Russia should be entitled to a sphere of influence that presumably would consist of the former Soviet republics with the exception of Estonia, Latvia, and Lithuania.[28] But the creation of a sphere of influence can only occur in two ways. It can either evolve out of shared interests of countries that have a similar regional political vision or it can be created by force. Historically, the Kremlin has found allies and partners in Europe that were willing to collectively ensure regional

stability and security, or it occupied areas by force and established political regimes that superficially gave the appearance of shared interests and regional vision. The connective tissue of the post-Cold War order in Europe has been the agreement across the continent on a single governance and development model. Russia's rejection of that critical binding element makes it difficult for Moscow to establish a sphere of influence in Europe based on shared interest as it has done in the past.

This problem for Russia is at the foundation of the current competition with the United States. When Putin early in his third term was soliciting input for a Russian idea, what he was after was an ideology that not only could drive Russian domestic and foreign policy, but one that could attract partners in rejection of the U.S.-led order in Europe and beyond.[29] Hence the notion of Russia as a protector of so-called traditional values, which was a conscious policy choice by the Kremlin to appeal to those in Europe and perhaps the United States dissatisfied with socio-cultural trends supported in many Western capitals.[30] Post-Soviet Russia is searching for ways to avoid isolation and rebuild lost influence. This is the result of the choice, early in Putin's first term, to go a different direction from a solid majority of those in the West.

In sum, it is unlikely that the United States would be facing a different Russia today if it had not participated in NATO enlargement, withdrawn from the ABM Treaty, or intervened in Iraq or Libya. Such policies became agitants to a deeper problem. The underlying political contradictions compounded by geographic realities and great power mentalities virtually assured confrontation at some point.



President of China Xi Jinping awarded the Order of Friendship of the People's Republic of China to Vladimir Putin. The President of Russia is the first foreign leader to be awarded this high national order of China. (Presidential Press and Information Office is licensed with CC BY 4.0.)

Russia's Vision for the Future

Having chosen to go its own way, Russia is now faced with the challenge of carving out its unique place in the world among the great powers. Lacking the soft power of the West or the economic clout of China, Russia has fewer options to pursue its national interests, although it is far from impotent. One of the most consequential moves the Kremlin has made since the total fallout with the West has been to seek a closer relationship with China in the hope of forging a "non-Western" coalition of the unwilling to push back against U.S. policies seen as destabilizing to global stability. Yevgenii Primakov, who apparently never believed that Russia's Western orientation would bear much fruit, in the mid-1990s spoke of the development of a multipolar (polycentric) world in which U.S. hegemony would be replaced by disparate power centers and a greater role for non-Western countries such as Russia, China, and India who would form the center of a non-Western international order.[31]

While the eventual rise of the polycentric world has remained an article of faith in Russia's official rhetoric, it has largely not come to pass.[32] Russia's strategic forecast to 2036 leaves open the possibility of a wider dispersion of power over the next fifteen years, but "bipolarity 2.0" is more likely to materialize according to other Russian long-term forecasts.[33] In this scenario, China replaces the USSR in a new era of superpower competition that relegates all other participants to a secondary role in shaping international relations. Nevertheless, a sphere of privileged influence in the former Soviet space with the exception of the Baltic countries would remain a guiding light for Russian foreign policy even in this case.

Because of the dynamics discussed above, Russian strategy has not and will not be limited to influencing the political situation in its immediate neighborhood. In fact, the primary targets for Russia to realize its regional vision are Western European countries and the United States. Both Western populations and the political elite will come under pressure through all means available below direct conflict to either change their view on policy toward Russia or to simply be driven toward a state in which conducting a sustained foreign policy of any kind will be increasingly difficult given domestic turmoil. The extent to which Russia is able to play much of a role in this outcome is a subject of much debate, but there is little question that inflicting "damage" on target societies is part of Moscow's strategy. Until the matter of the regional order in eastern Europe is resolved, there should be little expectation of letup in Russian activity that Kennan described as "a fluid stream which moves constantly, wherever it is permitted to move, toward a given goal."[34]

If the establishment of unchallenged authority in its near abroad is a minimum foreign policy objective for Russia, the maximum objective is to reduce the role of the United States in Europe. A more isolationist United States and a more independent Europe would from the Russian perspective certainly constitute a polycentric world. The United States would lead the western hemisphere, while Russia would at the very least face a much less powerful opposition in Europe in the near and medium term. The overall power of the United States together with the leading economies of Europe is overwhelming compared with that of Russia.[35] It will be very difficult for the foreseeable future for Russia to coerce a cohesive alliance of that magnitude. A Russian Ministry of Defense (MOD) assessment in 2015 clearly explained the relationship between power dynamics and Russia's ability to advantageously affect international relations:

> *Assurance of the realization of such a combination of scenarios (such as the polycentric world) could . . . strengthen and develop the socio-political potential of the state on the basis of effective socially oriented domestic policy and the preservation*

and development of fundamental moral values of the nation. This will ensure the important and growing role of Russia in the formation and strengthening of trade, economic, and military coalitions and alliances with the leading states of the world that conduct independent policies (i.e. non-Western countries) and pursue their national interests within the bounds of international law. If Russia does not manage to create the above conditions, it will not be able to play any substantive role in the formation of new power centers and influence the international situation.[36]

Put another way, Russia needs to create the domestic and international conditions such that it does not get left behind and become internationally irrelevant. Maximally speaking, even a partial collapse of the Western alliance would go some way in creating such conditions from Russia's perspective.

Russian foreign policy outside of the Western world is driven today not by the expansion of ideology, but by the expansion of influence, which perhaps is an easier problem to manage given the absence of quasi-messianism. As Dmitry Medvedev explained Russian interest in moving back into Africa: "Let's be frank, there is a lot of interest in Africa today. The primary players are actively established here. The (People's Republic of China) is doing a lot of things, the United States and European Union are actively engaged. Are we worse? We should also be engaged."[37] If Soviet behavior was a "fluid stream which moves constantly, wherever it is permitted to move, [to fill] every nook and cranny available to it in the basin of world power," Russian behavior is directed toward what basins are left available in a much more crowded map of powerful river systems. These river systems include not only the United States, leading EU countries, and China, but also India, Japan, Brazil, and Turkey, who each have economic interests and a considerable amount of military potential, particularly if allied with other powers that are willing to challenge Russia.[38]

The Indirect Approach to Strategy

As it pursues its vision of a lesser but still meaningful role around the world, in cases where Russian military power can be matched by an opposing side, the "indirect approach" is the preferred means to the desired end for the Kremlin and the MOD.[39] The indirect approach is one of battle avoidance that seeks to frustrate or exhaust the stronger opponent without actually engaging in open conflict unless faced with an existential threat.[40] Russia almost surely would like to turn the tables on the Western political and security system and see it collapse under the weight of its own contradictions without firing a shot. If it can opportunistically put its finger on the scale it will certainly do so, at least until a regime comes to power

Radio Free Europe (bB killingtime2 is licensed with CC BY-NC-ND 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/2.0/) May 31, 2012

in Moscow that is no longer diametrically opposed to the Western vision and believes it has more to gain than lose from cooperation. As before, the means to execute such a strategy will almost always take the form of what Kennan called "political warfare," which is a nonviolent approach to affect political division within a target country with the ultimate aim of a sharp change in policy toward Russia.

U.S. Strategy Toward Russia

The origins of Russian conduct have evolved from 1947 but not significantly so. Russia still remains fully and willingly outside the Western orbit. It seeks its own unique place in international affairs and to find or create spheres of influence based on an alternative development model. The Kremlin may not directly say so, but its behavior sends a strong signal that it would not be disappointed if the U.S. and Western-led military, political, and economic alliances were replaced with something smaller and more manageable and manipulable. At a minimum, it desires that Western capitals quite substantially alter what heretofore have been guiding principles of their foreign policies. If existing Western political parties or elites can be replaced by those who have different principles and different views toward Russia, Moscow will support those groups through existing nonmilitary means. What is different is that Russia is no longer the most vexing long-term challenge to the United States. This is due to the confluence of Russia's geopolitical and military decline (relative to the Soviet Union and the Warsaw Pact) and China's precipitous rise.[41] These factors mean that Russia for much of this century will play a role of a "swing state," and as a result U.S. strategy toward Russia cannot be a reprise of containment of the USSR.

Over the long-term, U.S. strategy should not be oriented toward countering Russia at all points around the globe. As attention and resources increasingly shift to China, this would be difficult to execute in any case, but it also leads to policies guided by a less rigorous assessment of U.S. strategic interests and more by a desire to oppose an adversary wherever they happen to be gaining influence at a given time. For example, assertions that Russia gaining a "foothold" in the Middle East would *ipso facto* be detrimental to U.S. interests should be met with a healthy dose of skepticism based on the American experience of the past three decades. In fact, it could turn out to be quite the opposite. Managing disparate interests and populations that are suspicious of foreign presence can be quite costly in myriad ways for the fleeting prize of international leadership. Broadly speaking, Kennan's view that Europe and Asia should be the anchor of American foreign policy is as true today as it was then. U.S. alliances in both regions should be managed with the greatest care, not subject to "microaggressions" toward allies at the expense of the much greater strategic benefit of these relationships. Russian forays elsewhere into areas with unstable regimes and security environments should cause the opposite of alarm so long as they do not lead to expanded opportunity to threaten the U.S. homeland.

One of the ways to resolve the current standoff in eastern Europe is to find a compromise solution to the regional order.[42] Such ideas are based in part on the aforementioned conclusion that had the U.S. pursued different policies in the preceding decades, an improved modus vivendi between Russia, Europe, and the United States could have been achieved. It deserves consideration, but, given the origins of Russian conduct, this approach is highly unlikely to produce anything more than a tactical reduction of U.S.-Russia tensions at some cost to U.S. credibility. Moreover, because Russia alone has chosen an alternative course that rejects what nearly all other European countries have accepted, should the whole project be overturned?

It is more appropriate at this juncture to pursue a strategy based on resilience and military deterrence with the long-term aim that Russia will see

cooperation with the West as most beneficial to its interests. Accommodation of the Kremlin on questions of European security and the political order will not produce the desired result because of the contradictions discussed above. Better to let Russia's relationship with China fizzle over time as the two great powers find it difficult to manage each other, and allow Russian policy to shift the other direction when it has a clear interest in doing so. Actively seeking various agreements with Russia under the current regime would send the opposite signal than should be sent in the very early stages of a renewed competition that in hindsight appears not so much to have ended as to have hibernated.[43]

One of the key tactics of Russia's indirect approach is to identify weak links in a stronger adversary and exploit them using inexpensive tools. Building resilience implies understanding what these weak links are and working to shore them up. By now it has become abundantly clear that societal cleavages resulting from a host of natural—in particular, economic—and manufactured forces are a key point of emphasis in Russian strategy. Political leaders and elites in the United States and Europe must recognize that domestic sentiment in the current information environment must be managed responsibly or it will continue to be a low-hanging fruit for the indirect approach.[44] They must also ensure that a considerable majority of the participants in the liberal democratic experiment believe they have something to gain by the continuation of an approach to governance and economic policy that on the whole has served their societies well since 1945, particularly in comparison to the alternative. In short, an emphasis on domestic political compromise as opposed to fundamentalism and zero-sum thinking must become a central tenet of the overarching national security strategy.

Extreme societal divisions can clearly become a national security problem over time. As the Soviet strategist Aleksandr Svechin wrote in 1927, "a significant superiority in forces and a hostile state whose political structure resembles a giant with feet of clay are conditions which favor a destructive strike and make it possible to end a war very quickly."[45] Updating this remark to modern times, a superiority in information dominance and an opponent whose socio-political structure resembles a clay giant are apt for a "destructive" strike that could end a confrontation without having to wage war. Resilience requires bipartisan political leadership and elites to accept responsibility to shape an information environment that is less susceptible to foreign or domestic disruption. Kennan's advice in this respect has stood the test of time:

> *In the light of these circumstances, the thoughtful observer of Russian-American relations will find no cause for complaint in the Kremlin's challenge to American society. [She] will rather experience a certain gratitude to a Providence which, by providing the American people with this implacable challenge, has made their entire security as a nation dependent on their pulling themselves together and accepting the responsibilities of moral and political leadership that history plainly intended them to bear.*[46]

If the Russia challenge can serve as a catalyst for more responsible political and elite leadership to adjust the "profit model" toward unity as opposed to division, fear, and anger, we would all be safer and more prosperous in the end.

The U.S. military can and should assist in this effort to build resilience to political warfare in Europe and it should develop ways to threaten Russia in kind. Indeed, senior Russian military officers and the Minister of Defense have stated explicitly that they believe the West is waging a war in the information domain to weaken or even unseat the current regime.[47] If the Russian military thinks it

Saber Strike 17 was a U.S. Army Europe-led multinational combined forces exercise conducted annually to enhance the NATO Alliance throughout the Baltic Region and Poland. (Staff Sgt. Brian Kohl (U.S. Army Europe is marked under CC PDM 1.0.) June 16, 2017

is at "war," this could expand the boundaries of their activities up to—but not including—military force to a considerable degree.[48] But on the whole building resilience to political warfare is not primarily a military problem; it is a political and societal problem that entails a whole-of-government approach that should emanate from the top, down. The primary role of the U.S. military is to maintain credible deterrence for as long as the confrontation lasts, in the confidence that our system of governance is better than any other on offer.

Deterrence of Russian military aggression provides the time and space needed for the more sustainable Western political and economic system to prevail again over an adversary whose alternative regional vision thus far has generated little appeal in Europe. The devil is in the details, but at a broad level Russia understands military deterrence as the ability to inflict damage on critical political, military-economic, and military infrastructure with both nuclear and long-range conventional weapons (and perhaps cyber weapons). If the United States and NATO allies are able to sustain the ability to credibly threaten Russia with those capabilities, they will have achieved deterrence as Russia defines it. Some Russian deterrence theorists have argued that the damage thresholds have lowered over time as a result of greater recognition on both sides of the unacceptability of the consequences of nuclear and conventional strikes.[49] If one accepts this proposition, this actually reduces the resource requirements due to fewer munitions needed to inflict the required damage.

At an operational level, in light of the worsening confrontation with China that is expected to last decades, the United States should be guided

by the principle of sufficiency in Europe. Given the overall military potential imbalance between the two sides in favor of NATO, perhaps the most important capability to develop will be a robust logistics system that allows for the flow of superior forces right up to Russia's border to assure defense of NATO allies in the event of an unexpected military conflict. Forward deployed forces are not irrelevant, but necessary in perhaps far fewer numbers than in the previous era of confrontation based on Russian concerns of air and sea-based aerospace potential and limited Russian inventories of long-range conventional munitions.[50] A minimum threshold might be holding Kaliningrad at risk in the initial period of war with a combination of U.S., Polish, and other allied ground forces while simultaneously threatening critical military and military-economic infrastructure across Russia's western border through both kinetic and nonkinetic means.

An important outstanding question is U.S. strategy toward the non-aligned countries in eastern Europe. Regardless of the intent, Russian actions in Ukraine and Georgia improved the attraction of the argument for further NATO enlargement. At the same time, Russian interests in the former Soviet space are clearly strategic. Andrei Kokoshin, the former Secretary of the Russian Security Council, wrote in the late 1990s, "Russia attaches particular importance to the quality of its relations with the territories of the former Soviet Union, particularly with Ukraine, Belarus, and Kazakhstan. Admittedly, the prominence of the Russian-Ukrainian relationship transcends the boundaries of the Commonwealth of Independent States (CIS) and even Europe as a whole. World politics to a large extent depends on the status of that relationship."[51] This dynamic suggests a strategy of patient constraint on the part of the United States that is oriented toward resilience through democratic and economic development assistance as opposed to a leading role for military deterrence. To be sure, this line of effort toward building resilience has been ongoing for some time. The idea that the professed neutrality of these countries could produce a lasting peace is dubious both because of the populations' desire for political and economic integration with the West and because Russia's rejection of the underlying political norms lays the groundwork for creating an alternative sphere of influence by force. The ultimate end state would be one in which a future Russian regime does not feel the need to resist a Western orientation of its neighbors because it has concluded the most beneficial course of action is to embrace the political norms that could legitimately create a Europe whole and free. *Nadezhda umiraet poslednei* (Hope springs eternal).

Despite Kennan's assertions to the contrary, his analysis and conclusions on the Soviet regime remain relevant today with the leadership of the Russian Federation. The rejection of a governance model that would have assured security on its western flank was Russia's sovereign choice. And that choice was the perhaps inevitable result of the pull of conservative political forces throughout Russian history. Russia simply could not be "another Poland," and it is not clear what plausible arrangement could have satisfied Russian desires given political realities throughout Europe and the United States.[52] As it is, an alternative Russian model requires a separate sphere of influence. A separate sphere of influence automatically brings Russia into conflict with the United States and much of Europe who are pursuing a different vision for the continent. Russia could change its vision, or the West could change, but neither is likely to do so in the near term despite concerted efforts on each side to facilitate that outcome. Thus, "it is clear that the United States cannot expect in the foreseeable future to enjoy political intimacy with the (Russian) regime."[53]

Given this reality, the United States must settle in for another round of confrontation and competition with the Kremlin. In this iteration, however, the Kremlin will not be the primary object of U.S. focus.

That critical difference has a number of implications for U.S. strategy. It simply may not be possible over the course of decades to put up strong resistance to Russian attempts to expand its global influence while also confronting and containing China. But it also will not be necessary. Russia has limited means at its disposal, and there is not yet any indication that Putin is willing to commit anywhere near the resources on the military that likely would be required to do so.[54] In light of renewed competition with two great powers, the U.S. will need to prioritize. It will need to pursue less costly approaches to dealing with Russia than in the past. It will need to rely more on resilience and deterrence than on forward deployed forces. But this is appropriately suited to counter a Russian strategy centered on the indirect approach and battle avoidance with a stronger power. The origins of Russian conduct are inherently confrontational with the West, but they are not suicidal. PRISM

Notes

[1] George Kennan, "A Fateful Error," *The New York Times*, February 5, 1997. https://www.nytimes.com/1997/02/05/opinion/a-fateful-error.html.

[2] Rose Gottemoeller, Thomas Graham, Fiona Hill, Jon Huntsman Jr., Robert Legvold and Thomas R. Pickering, "It's Time to Rethink our Russia Policy," *Politico*, August 5, 2020, https://www.politico.com/news/magazine/2020/08/05/open-letter-russia-policy-391434; David J. Kramer, "No, Now is Not the Time for Another Russia Reset," *Politico*, August 5, 2020, https://www.politico.com/news/magazine/2020/08/11/russia-reset-response-open-letter-393176; Sławomir Dębski, James Sherr, and Jakub Janda, "Take It From Eastern Europe: Now Is Not the Time to Go Soft on Russia," *Politico*, August 31, 2020, https://www.politico.com/news/magazine/2020/08/31/open-letter-not-time-to-go-soft-on-russia-405266; Ariana Gic, Hanna Hopko, and Roman Sohn, "Appeasing Vladimir Putin's Russia Will Only Embolden It," *Politico*, September 25, 2020, https://www.politico.com/news/magazine/2020/09/25/open-letter-russia-ukraine-421519.

[3] As Graham Allison and Dimitri Simes wrote for *National Interest*, "As seen during Obama's second term, when treated primarily as a 'foe,' Russia can undermine important American objectives. If it can be persuaded to act more as a partner, within the framework of a sustainable, if difficult, working relationship, Moscow can help advance U.S. foreign-policy objectives in a number of ways." See, Graham Allison and Dimitri K. Simes, "A Blueprint for Donald Trump to Fix Relations with Russia," *National Interest*, December 18, 2016. https://nationalinterest.org/feature/blueprint-donald-trump-fix-relations-russia-18776.

[4] Celeste Wallander and Anne Wildermuth, *The Sources of Russian Foreign Policy After the Cold War*, (Routledge, 1996).

[5] Kennan, 1997.

[6] Yegor Gaidar, *Collapse of an Empire: Lessons for Modern Russia*. 1st Edition. (Washington, DC: Brookings Institution Press, 2007).

[7] Timothy Colton, *Yeltsin* (Basic Books, 2008), 266.

[8] President of Russia, Kontseptsiia vneshnei politiki Rossiiskoi Federatsii, April 23, 1993; Colton, p. 269.

[9] The Russian Foreign Minister at the time, Yevgenii Primakov, was traveling to Washington. Upon receiving the news of the NATO intervention, ordered the plane back to Moscow in protest. For a brief chronology of Russian reactions to NATO enlargement, see, Radin, Andrew and Clint Reach, Russian Views of the International Order. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_resports/RR1826.html.

[10] Yurii Baluevskii (ed.), et al., *Voennaia bezopasnost' Rossiiskoi Federatsii v XXI veke*, Center for Military-Strategic Studies of the General Staff, Moscow, 2004, pp. 10-25.

[11] Vladimir Putin, speech, "Annual Address to the Federal Assembly of the Russian Federation." 26 May 2004. http://archive.kremlin.ru/eng/speeches/2004/05/26/1309_type70029type82912_71650.shtml.

[12] Thomas Ambrosio, "The Russo-American Dispute over the Invasion of Iraq: International Status and the Role of Positional Goods," *Europe-Asia Studies*, Vol. 57, No. 8, December 2005, pp. 1189-1210, DOI: 10.1080/09668130500351357.

[13] Clint Reach, Vikram Kilambi, Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means*, Santa Monica, CA: RAND Corporation, RR-4235, 2020, pp. 115-122. https://www.rand.org/pubs/research_reports/RR4235.html.

[14] U.S. armor returned to Europe only after Russian annexation of Crimea and intervention in eastern Ukraine.

[15] Andrew Radin and Clinton Bruce Reach, *Russian Views of the International Order*, Santa Monica, CA: RAND Corporation, RR-1826, 2017, p. 71. https://www.rand.org/pubs/research_resports/RR1826.html.

[16] Fiona Hill and Clifford Gaddy, *Mr. Putin: Operative in the Kremlin*, (Washington, DC: Brookings Institution Press, 2015).

[17] Putin assembled the leaders of the leading Russian industries in 2000 and "passed the puck" to them, which essentially meant that it was their choice to keep their distance from politics and enjoy the fruits of privatization, or not. Khodorkovsky chose the latter. See, "Kak Putin vstrechalsia s krupnym biznesom," *Kommersant*, December 24, 2015.

[18] Vladislav Surkov, "Natsionalizatsiia budushchego (polnaia versiia), surkov.info, December 6, 2006. As of October 26, 2020: http://surkov.info/nacionalizaciya-budushhego-polnaya-versiya/; Steven Rosefielde & Romana Hlouskova, "Why Russia is Not Democracy," *Comparative Strategy*, 26:3, 2007, p. 216, DOI: 10.1080/01495930701454454.; Michael McFaul and Kathryn Stoner-Weiss, "The Myth of the Authoritarian Model," *Foreign Affairs*, January/February 2008, pp. 68-84. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/Myth_of_the_Authoritarian_Model.pdf.

[19] Dmitri Trenin, "Russia's Breakout from the Post-Cold War System: Drivers of Putin's Course," Carnegie Moscow Center, December 22, 2014. https://carnegie.ru/2014/12/22/russia-s-breakout-from-post-cold-war-system-drivers-of-putin-s-course-pub-57589.

[20] Marlene Laruelle, *Russian Eurasianism: An Ideology of Empire*, (Woodrow Wilson Center Press with Johns Hopkins University, 2008); Brian Taylor, *The Code of Putinism*, (Maryland: Oxford University Press, 2018).

[21] Vladimir Putin, "Novyi integratsionnyi proekt dlia Evrazii – budushchee nachinaetsia segodnia," *Izvestiia*, October 4, 2011.

[22] Vladimir Putin, Interview, "Miroporyadok," *Rossiya* HD. December 20, 2015.

[23] The 2015 National Security Strategy and 2016 Foreign Policy Concept each emphasized the prioritization of Eurasian integration processes. There is little public indication that senior Russian leadership exclude Ukraine, Georgia, and Moldova from this long-term integration project.

[24] Aleksei Miller and Fedor Lukyanov, "Otstranennost' vmesto konfrontatsii: postevpopeiskaia Rossiia v poiskakh samodostatochnosti," Sovet po vneshnei i oboronnoi politike, 2016, pp. 1-2.

[25] Stephen Watts, Nathan Beauchamp-Mustafaga, Benjamin Harris, and Clint Reach, *Alternative Worldviews: Understanding Potential Trajectories of Great-Power Ideological Competition*, Santa Monica, CA: RAND Corporation, RR-2982, 2020, Appendixes, pp. 21-32. https://www.rand.org/pubs/research_reports/RR2982.html.

[26] Richard Pipes, *Russian Conservatism and its Critics: A Study in Political Culture*, (UK: Yale University Press, 2007).

[27] Yurii Balaluevskii and Musa Khamzatov, "Globalizatsiia i voennoe delo," *Nezavisimoe voennoe obozrenie*, August 8, 2014.

[28] John J. Mearsheimer, "Why the Ukraine Crisis is the West's Fault: The Liberal Delusions that Provoked Putin," *Foreign Affairs*, September/October, 2014. https://www.foreignaffairs.com/articles/russia-fsu/2014-08-18/why-ukraine-crisis-west-s-fault.

[29] Stephen Watts, Nathan Beauchamp-Mustafaga, Benjamin Harris, and Clint Reach, *Alternative Worldviews: Understanding Potential Trajectories of Great-Power Ideological Competition*, Santa Monica, CA: RAND Corporation, RR-2982, 2020, Appendixes, pp. 21-32. https://www.rand.org/pubs/research_reports/RR2982.html.

[30] Mark Galeotti, "Putin's Hydra: Inside Russia's Intelligence Services," European Council on Foreign Relations, ECFR/169, May 2016, p. 13.

[31] "Lavrov rasskazal ob idee Primakova sozdat' 'treugol'nik' Rossiia-Indiia-Kitai," *RIA Novosti*, October 29, 2019.

[32] Andrei Kortunov, "Pochemu mir ne stanovitsia mnogopoliarnym?" *Rossiia v global'noi politike*, June 26, 2018.

[33] Nikolai Patrushev, Videt' tsel', Rossiiskaia gazeta, November 11, 2019; V. M. Burenok (ed.), *Kontseptsiia obosnovaniia perspektivnogo oblika silovykh komponentov voennoi organizatsii Rossiiskoi Federatsii*, Rossiiskaia Akademiia raketnykh i artilleriiskikh nauk, 2018, pp. 339-370.

[34] Kennan, 1997.

[35] Burenok (ed.), 2018, pp. 300-310.

[36] S. R. Tsyrendorzhiev, "Prognoz voennykh opasnostei i ugroz Rossii," *Zashchita i bezopasnost'*, Vol. 4, 2015, pp. 10-14.

[37] Aleksandr Kolesnichenko, "Kak president Medvedev chut ne 'zazheg' v Namibii," *Argumenty i fakty*, June 26, 2009.

[38] V. M. Burenok (ed.), *Kontseptiia obosnovaniia perspektivnogo oblika silovykh komponentov voennoi organizatsii Rossiiskoi Federatsii*, Granitsa Publishing House, 2018, pp. 300-310.

[39] B. H. Liddell Hart, *Strategy*, BN Publishing, 2008.

[40] Andrei Kartapolov, "Uroki voennykh konfliktov, perspektivy razvitiia sredstv i sposobov ikh vedeniia. Priamye i nepriamye deistviya v sovremennykh mezhdunarodnyh konfliktakh," *Vestnik Akademii voennykh nauk*, Vol. 2, Issue 51, 2015; Rod Thornton, "The Russian Military's New 'Main Emphasis'," *The RUSI Journal*, Vol. 162, Issue 4, August/September 2017, p. 20.

[41] Ben Connable, Abby Doll, Alyssa Demus, Dara Massicot, Clint Reach, Anthony Atler, William Mackenzie, Matthew Povlock, Lauren Skrabala, *Russia's Limit of Advance: Analysis of Russian Ground Force Deployment Capabilities and Limitations*, Santa Monica, CA: RAND Corporation, 2020, RR2563. https://www.rand.org/pubs/research_reports/RR2563/html.

[42] Kissinger, for example, has proposed that Ukraine should be a "bridge" between Russia and NATO, a view that he concedes is in the minority in American foreign policy thought. See, Jeffrey Goldberg, World Chaos and World Order: Conversations with Henry Kissinger, *The Atlantic,* November 10. 2016. https://www.theatlantic.com/international/archive/2016/11/kissinger-order-and-chaos/506876/.

[43] New Start Treaty excepted.

[44] It would also be the right thing to do for the country, regardless of Russia's actual ability to manipulate public opinion in the United States.

[45] Kent Lee (ed.), translation of Aleksandr A. Svechin, *Strategy*, 2nd Edition, (Minneapolis: East View Publications, 1991), 98.

[46] Kennan, 1997.

[47] M.A. Gareev, et al., "Metodologiia i praktika sovershenstvovaniia strategicheskogo rukovodstva oboronoi strany s uchetom kharaktera buduschikh voin i vooruzhennykh konfliktov," *Vestnik Akademii voennykh nauk*, No. 1(66), 2019; "Shoigu nazval tsel' informatsionnoi voiny Zapada protiv Rossii," TASS, June 26, 2019; Oleg Falichev, "Pravo pervym podnyat'sya v ataku," *Voenno-promyshlennyi kur'er*, September 11, 2018.

[48] Modestov in 2009 discussed the idea of strategic deterrence in the information sphere, which included operations to inflict "damage" both psychologically and to critical information infrastructure on which modern socities and economies rely. See, S. A. Modestov, "Strategicheskoe sderzhivanie na teatre informatsionnogo protivoborstva," *Vestnik Akademii voennykh nauk*, Vol. 1, Issue 26, 2009, pp. 33-36.

[49] A. A. Kokoshin (ed.), *Vliianie tekhnologicheskikh faktorov na parametry urgroz natsionaloi i mezhdunarodnoi bezopasnosti, voennykh konfliktov i strategicheskoi stabil'nosti*, Izdatel'stvo Moskovskogo Universiteta, 2017, pp. 205-225.

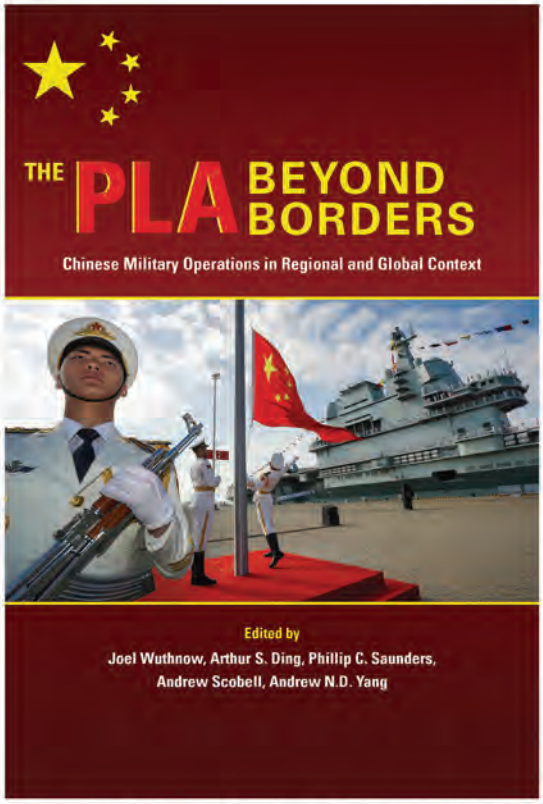
[50] Clint Reach, Vikram Kilambi, Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means*, Santa Monica, CA: RAND Corporation, RR-4235, 2020. https://www.rand.org/pubs/research_reports/RR4235.html.

[51] Andrei Kokoshin, *Soviet Strategic Thought, 1917-1991*, (Massachussets: MIT Press, 1998), 194.

[52] Fyodor Lukyanov, "The Lost Twenty-Five Years," *Russia in Global Affairs*, February 28, 2016. https://eng.globalaffairs.ru/articles/the-lost-twenty-five-years/.

[53] Kennan, 1997.

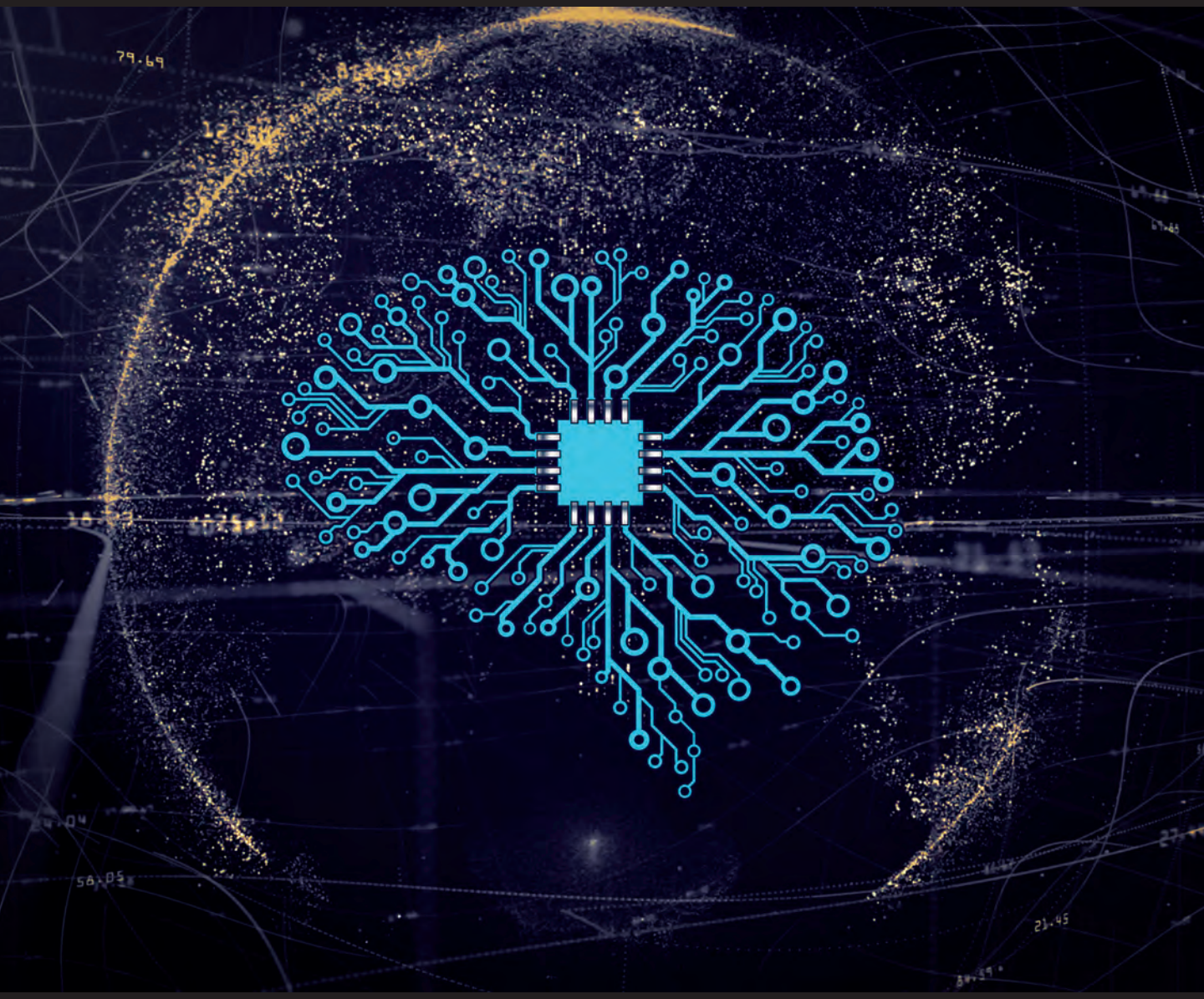
[54] Henry Foy, "Russia to cut defence spending in bid to prop up ailing economy," *Financial Times*, September 21, 2020. https://www.ft.com/content/763b1345-b703-40db-8065-167cbfe7f.



https://ndupress.ndu.edu/Publications/Books/PLA-Beyond-Borders/

No longer confined to China's land territory or its near abroad, the People's Liberation Army (PLA) is conducting increasingly complex operations farther and farther from China's continental borders. Within Asia, the PLA now regularly operates into the far reaches of the South China Sea and deep into the Western Pacific, enforcing China's territorial claims and preparing to counter U.S. intervention in a regional conflict. Beyond Asia, the PLA is present on the ground, at sea, or in military exercises with foreign partners across the Indian Ocean and into the Middle East, Africa, and Europe. Foreign militaries now regularly encounter the PLA, whether in tense incidents or friendly contacts, on their home turf and in the global commons.

Drawn from a 2019 conference jointly organized by NDU, the RAND Corporation, and Taiwan's Council on Advanced Policy Studies, *The PLA Beyond Borders* surveys the dimensions of Chinese operations within the Indo-Pacific region and globally. The international contributors look both at the underlying enablers of these activities, including expeditionary capabilities and logistics, command and control, and ISR systems, as well as new and evolving operational concepts and operational patterns. Employing different analytic lenses, they portray a reformed PLA accelerating the pace of its overseas operations and increasing its modernization not only in the traditional domains, but also in space and cyber.



China is pursuing what its leaders call a "first-mover advantage" in artificial intelligence (AI), facilitated by a state-backed plan to achieve breakthroughs by modeling human cognition. (www.vpnsrus.com)

China's "New Generation" AI-Brain Project

By Wm. C. Hannas and Huey-Meei Chang

China is pursuing what its leaders call a "first-mover advantage" in artificial intelligence (AI), facilitated by a state-backed plan to achieve breakthroughs by modeling human cognition. While not unique to China, the research warrants concern since it raises the bar on AI safety, leverages ongoing U.S. research, and exposes U.S. deficiencies in tracking foreign technological threats.

The article begins with a review of the statutory basis for China's AI-brain program, examines related scholarship, and analyzes the supporting science. China's advantages are discussed along with the implications of this brain-inspired research. Recommendations to address our concerns are offered in conclusion. All claims are based on primary Chinese data.[1]

China's Plan to "Merge" Human and Artificial Intelligence

Analysts familiar with China's technical development programs understand that in China things happen by plan, and that China is not reticent about announcing these plans. On July 8, 2017 China's State Council released its "New Generation AI Development Plan"[2] to advance Chinese artificial intelligence in three stages, at the end of which, in 2030, China would lead the world in AI theory, technology, and applications.[3] The announcement piqued the interest of the world's techno-literati[4] in light of the plan's unabashed goal of world hegemony, its state backing, and a well-founded belief that China is already a major AI player.[5] Although China still lags in semi-conductor design and basic AI research, it is moving to address —or circumvent— these problems, lending credence to its long-term aspirations.

Buried in this plan, and absent entirely from the Western dialog on China AI, is what we see as that country's most interesting and potentially significant research, namely, a top-down program to effect a "merger" (混合) of human and artificial intelligence. These efforts to use neuroscience to inform AI, and vice-versa, date to at least 1999[6] and precede China's focus on AI as a standalone discipline. Whereas the earliest appearance of AI in a ministry notification was in July 2015,[7] China's "National Medium- and Long-term S&T Development Plan"[8] issued in 2006 had already identified brain science and cognition among its top research priorities. The 2016 "Notification on National S&T Innovation Programs for the 13th

William Hannas is Lead Analyst at Georgetown's Center for Security and Emerging Technology (CSET).
Huey-Meei Chang is a Research Analyst at Georgetown's Center for Security and Emerging Technology (CSET).

Five-Year Plan" mentioned AI but did not count it among its major projects.[9] What appeared instead was "brain science and brain-inspired research" defined as "brain-inspired computing" and "brain-computer intelligence."

This timeline establishes "AI-brain research" as a line of inquiry in China before AI became a household word and a focus of state interest. In March 2016, the "China Brain Project" (中国脑计划) was approved, a 15-year effort that "prioritized brain-inspired AI over other approaches."[10] In May of the same year, Chinese president Xi Jinping publicly endorsed one of its key pillars:

> "Connectomics is at the scientific forefront for understanding brain function and further exploring the nature of consciousness. Exploration in this area not only has important scientific significance, but also has a guiding role in the prevention and treatment of brain disease *and the development of intelligent technology*." (our emphasis)[11]

Taking these circumstances into account, it is not surprising that the 2017 New Generation AI Development Plan[12] uses the word "brain" 27 times and "brain-inspired/neuromorphic" (类脑) some 20 times. The plan's "strategic goals" include "major breakthroughs in brain-inspired intelligence, autonomous intelligence, mixed [human-artificial] intelligence, swarm intelligence, and other areas so as to have an important impact in the area of international AI research, and occupy the commanding heights of AI technology." The document goes on to explain:

> "Brain-like intelligent computing theory focuses on breakthroughs in brain-like information coding, processing, memory, learning, and reasoning theories; on forming brain-like complex systems, brain-like control, and other theories and methods; and on establishing new models of large-scale brain-like intelligent computing and brain-inspired cognitive computing models."

In terms of priorities, "AI-brain" occupies two of the plan's eight "basic theory" categories: "(3) hybrid enhanced intelligent theory" and "(7) brain intelligent computing theory," defined as:

> "Research on 'human-in-the-loop' hybrid enhanced intelligence, human-computer intelligence symbiosis behavior enhancement and brain-computer collaboration, machine intuitive reasoning and causal models, associative memory models and knowledge evolution methods, hybrid enhanced intelligent learning methods for complex data and tasks, cloud robot collaborative computing methods, situational understanding in real-world environments, and human-machine group collaboration."

and,

> "Research theories and methods of brain-like perception, brain-like learning, brain-like memory mechanisms and computational fusion, brain-like complex systems, and brain-like control."

In sum, China's New Generation AI plan aims to "build for China a *first-mover advantage* in artificial intelligence development,"[13] which to us invokes the self-bootstrapping scenario—a mainstay of the AI safety literature—of a country with an early AI advantage leveraging its lead past the point where others are able to compete.

China's AI-Brain Academic Research

2016 was a watershed year in terms of China's AI-brain scholarship. We identified a core group of six papers published that year by leading Chinese

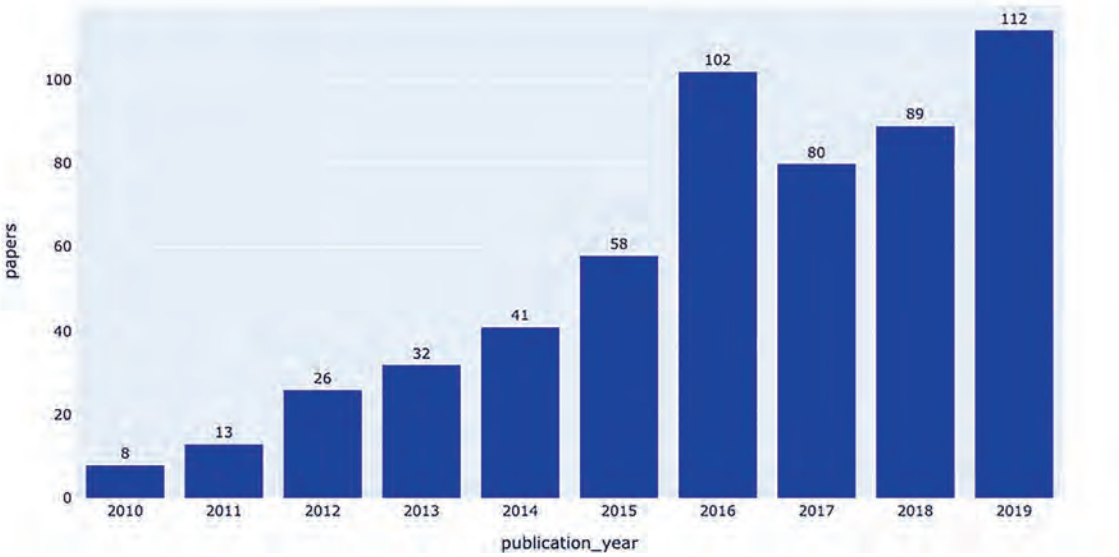
researchers that define China's approach to this hybrid area and signal acceptance of the paradigm:

- "Retrospect and Outlook of Brain-inspired Intelligence Research" (类脑智能研究的回顾与展望).[14]
- "Brain Science and Brain-inspired Intelligence Technology-an Overview" (脑科学与类脑研究概述).[15]
- "Progress and Prospect on the Strategic Priority Research Program of 'Mapping Brain Functional Connections and Intelligence Technology'." ("脑功能联结图谱与类脑智能研究"先导专项研究进展和展望).[16]
- "The Human Brainnetome Atlas: A New Brain Atlas Based on Connectional Architecture."[17]
- "Neuroscience and Brain-inspired Artificial Intelligence: Challenges and Opportunities" (神经科学和类脑人工智能发展: 机遇与挑战).[18]
- "China Brain Project: Basic Neuroscience, Brain Diseases, and Brain-inspired Computing" (全面解读中国脑计划: 从基础神经科学到脑启发计算).[19]

The content of these and other key studies is described in our technical review of China's AI-brain program;[20] these samples give a sense of the topics and players. That same year—2016—saw the start of an upward trend in the number of papers by Chinese scientists on brain-inspired AI specifically, one of the discipline's three defining elements.[21]

Meanwhile, China's National Natural Science Foundation (NNSF), the main sponsor of state grants to individual scholars, in August 2017 solicited proposals for 25 AI projects, most of which are brain-related, within the following ten approved research areas:[22]

1. Multi-modal, efficient cross domain perception and augmented intelligence
2. Machine understanding of perception and behavior under uncertain conditions
3. New methods for complex task planning and reasoning
4. Machine learning theory and methods based on new mechanisms (deep reinforcement learning, adversarial learning, brain-like / natural learning)



Brain-inspired AI papers in China's CNKI database
(reprinted with permission from GU/CSET "China AI-brain Research")

5. New brain-inspired computing architectures and methods
6. New methods of human-machine hybrid intelligence
7. Chinese semantic computing and deep understanding (machine reading comprehension and Chinese text creation, human-computer dialogue, etc.)
8. New computing devices and chips for artificial intelligence
9. Heterogeneous multi-core parallel processing methods and intelligent computing platforms
10. Machine intelligence test models and evaluation methods

In January 2018, NNSF funding guidelines recognized AI for the first time as an independent category, but also listed *nine specific subcategories* for "cognitive and neuroscience-inspired AI." Here are the topics and their respective funding codes:[23]

China NNSF cognitive-neuroscience-inspired AI funding subcategories

F060701 computational modeling of cognitive mechanisms (基于认知机理的计算模型)

F060702 modeling attention, learning, and memory (脑认知的注意、学习 与记忆机制的建模)

F060703 audiovisual perception modeling (视听觉感知模型)

F060704 neural information encoding and decoding (神经信息编码与解码)

F060705 neural system modeling and analysis (神经系统建模与分析)

F060706 neuromorphic engineering (神经形态工程)

F060707 neuromorphic chips (类脑芯片)

F060708 brain-like computing (类脑计算)

F060709 BCI and neural engineering (脑机接口与神经工程)

Besides NNSF support, China's Ministry of Science and Technology, the Chinese Academy of Sciences (CAS), and local municipalities also announced grants for AI-brain research.[24] In terms of scholarship and support, it is clear that China has committed to this alternative paradigm.

What Constitutes "AI-Brain" Science in China?

As confirmed by a survey of its practitioners, three areas of research contribute to China's AI-brain program: brain-inspired artificial intelligence (BI-AI, 类脑智能), connectomics ("brain mapping"人脑连接组), and brain-computer interfaces (BCI, 脑机接口).[25]

- BI-AI seeks mathematical descriptions of brain processes that contribute to behavior. This is understood literally, not as metaphor—the models match the actual "computation performed by biological wetware."[26]
- Connectomics involves empirical and computational efforts to replicate brain structure and functioning. The link with AI derives from a need to invoke AI to test simulations, and from AI's role in interpreting (aligning) images of brain sections.
- BCIs acquire electrical signals from the brain, interpret them, and optionally transform the signals into actions. Their link with AI is twofold: AI is used to process brain signals and, potentially, support direct access to computing resources.

Although some goals of this research mirror mainstream AI, the difference is while the latter may seek to replicate brain behavior, the new approach emulates the actual neuronal functioning that gives rise to behavior. The motivation for BI-AI (and its companion discipline connectomics) is the empirical

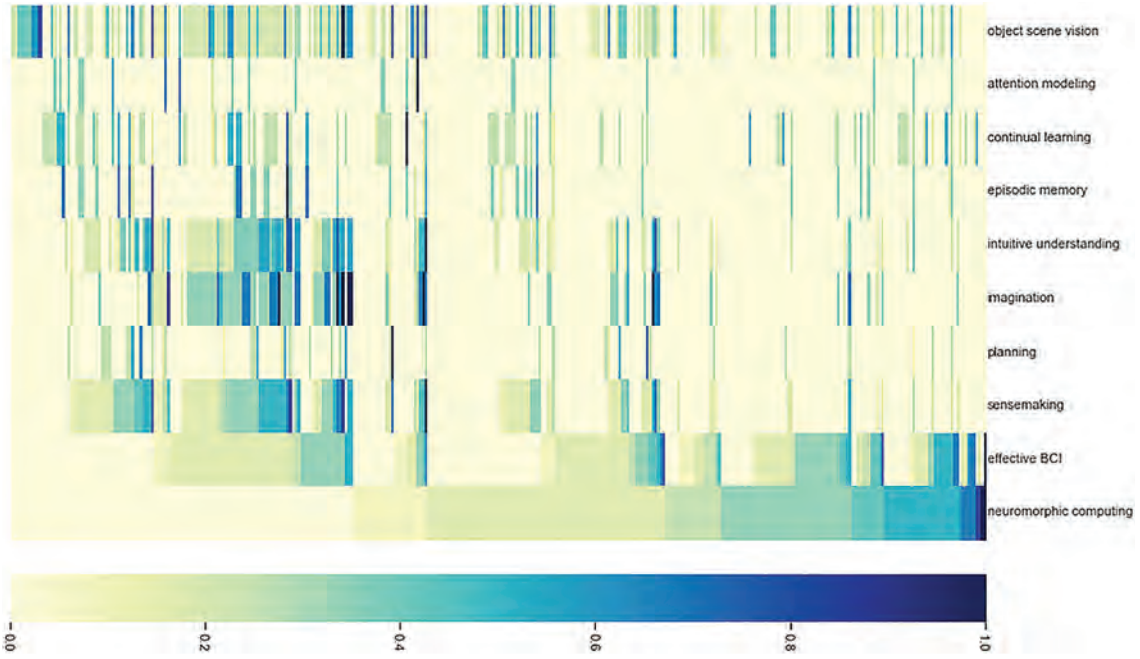
observation that the human brain, with minimal resources, effortlessly performs many high-order tasks beyond the reach of today's machine learning (ML).

A short list of these tasks, culled from standard references,[27] includes object/scene vision, attention modeling, continual learning, episodic memory, intuitive understanding, imagination, planning, and sensemaking. Two other goals are effective BCI (minimally invasive interfaces with useful throughput) and neuromorphic computing (hybrid digital-analog chips that mimic brain structure). In this context, we examined 561 Chinese papers and found 352 of them binning into one or more of the aforementioned categories, indicating that Chinese BI-AI research aligns with worldwide scientific aspirations.

Further testimony to China's commitment comes from the number of institutes, state and university affiliated, engaged in BI-AI, connectomics, or BCI as their primary research area. We identified 30 such institutes, including concentrations in Beijing and Shanghai, and in provincial locations such as Chengdu, Guangzhou, Hangzhou, Harbin, Hefei, Nanjing, Qingdao, Shenzhen, Suzhou, Tianjin, Wuhan, Xiamen, and Zhengzhou, exclusive of facilities working the disciplines peripherally.

We are struck by the caliber of personnel, collaborative networks, and research directions at three of these "outlying" institutes: the Fujian Key Laboratory for Brain-like Intelligent Systems (福建省仿脑智能系统重点实验) operating since 2009 in Xiamen;[28] the HUST-Suzhou Institute for Brainsmatics (华中科技大学苏州脑空间信息研究院) established 2016 at Wuhan's Huazhong University of S&T; and Hefei's National Engineering Laboratory for Brain-inspired Intelligence Technology and Application (NEL-BITA) (类脑智能技术及应用国家工程实验室), a government-sponsored lab set up in 2017 with China's major AI companies and Microsoft Research Asia.

NEL-BITA researches brain cognition and neural computing, brain-inspired multimodal sensing and information processing, brain-inspired



"Heat map" of 352 Chinese BI-AI technical journal articles. The color spectrum of each segment is the paper's category affinity. (reprinted with permission from "China AI-brain Research")

chips and systems, "quantum artificial intelligence," and brain-inspired intelligent robots.[29] The HUST-Suzhou "Brainsmatics" facility, whose work has been praised by the Allen Institute's chief scientist,[30] has pioneered research in micro-optical sectioning tomography on its way to creating a high-resolution mammalian brain atlas.[31] Bear in mind that these are institutes *outside* the main research nexus.

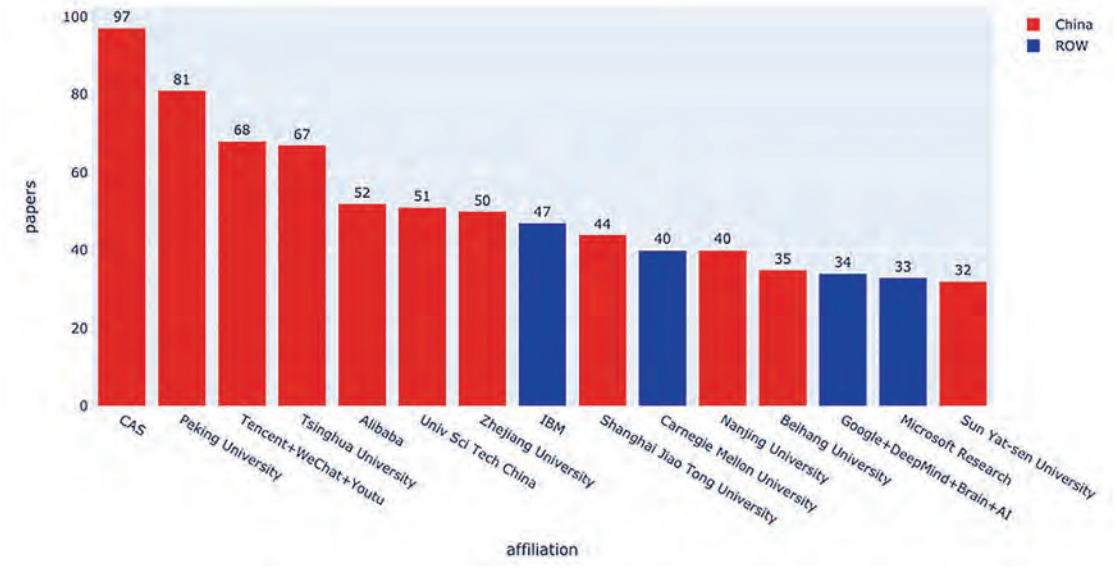
Meanwhile, Pu Muming's Center for Excellence in Brain Science and Intelligence Technology (中国科学院脑科学与智能技术卓越创新中心), one of three major complexes in Shanghai, is host to a "G60 Brain Intelligence Innovation Park" established in 2018 with a U.S. $1.5 billion budget for BI-AI research and $2.85 billion more promised in 2020.[32] The facility uses cloned monkeys.[33] A final example, from Beijing, is Tsinghua University's Center for Brain-inspired Computing Research (清华大学类脑计算研究中心), established in 2014 to study neural coding, ML algorithms, and chip architecture.[34]

The China-ROW Balance Sheet

China enjoys several advantages over other nations in AI-brain research. We lay this out for consideration without judgment on how these advantages may play out. Similar research is being conducted worldwide and we have no crystal ball to foretell what nation will prevail in the global AI competition (if "prevail" is the right way to frame the matter). For China, seven such factors come to mind, the first three being the usual staples about *China's more permissive experimental ethos, abundance of data, fewer privacy concerns on data collection and use*, and the fourth being *national commitment*, which we have been at pains to demonstrate. The other advantages require elaboration.

Fifth, and most obvious, is China's *AI talent*, as shown in a breakdown of papers accepted at the Association for the Advancement of Artificial Intelligence's (AAAI) 2020 conference, a central event for the world's AI community.[35]

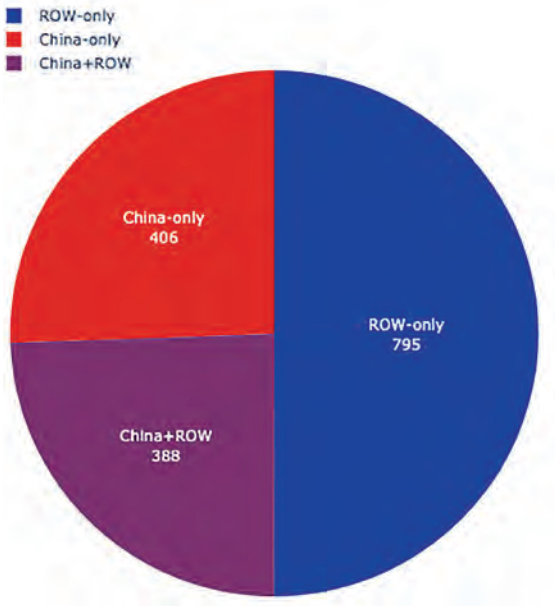
The key takeaway is that ownership of the event has slipped from U.S. institutions, which dominated previous years.[36] A China-ROW comparison of papers at the NeurIPS 2019 conference, a more focused gathering where China is a relative newcomer, had scholars from Tsinghua University placing 13th in number of accepted papers.[37] In



AAAI 2020 Accepted Papers - Top Affiliations

2020, Tsinghua papers ranked 7th behind AI giants Google, Stanford University, MIT, Microsoft, UC Berkeley, and Carnegie Mellon, all of which are targets of PRC "talent" co-option programs, if not actively cooperating with China already (see technology transfer discussion below).[38]

Both the AAAI and NeurIPS conferences had roughly the same paper acceptance rate (20.6 percent and 21.2 percent), so it is clear China is playing with the best. Chinese participation at these two key events would be skewed more in China's favor if we account for co-authorship and the national origins of authors with non-China affiliations. Here is another breakdown of the AAAI 2020 event that accommodates co-authorship:



AAAI 2020 Accepted Papers - China and ROW

Papers by authors with China-only affiliations are 26 percent of the total. Papers by authors with China affiliations collaborating with authors claiming other (rest-of-world) affiliations constitute another 24 percent. Together they account for half of the papers.[39] Statistics for the NeurIPS 2019 gathering show 42 percent of accepted papers having "Chinese authorship" (华人作者).[40] The importance of Chinese AI talent can also be measured by the stream of arguments from our own Georgetown center for measures to retain Chinese students and other diaspora talent to keep the U.S. competitive, a position we wholly support.[41]

A sixth advantage is China's *near monopoly on non-human primates* (NHP) regarded by most AI-brain researchers as essential.[42] By 2016, when China's AI-brain project had come into its own, high-tech primate facilities already existed in Guangzhou, Hangzhou, Shenzhen, Suzhou, and elsewhere in Guangxi, Hainan, and Yunnan. While other countries were scaling back NHP production, China was raising laboratory grade monkeys in volume at a fraction of the cost for export and as a lure to foreign scientists, inhibited by domestic restrictions, to conduct their research in China.[43]

Nikos Logothesis, director of the Max Planck Institute for Biological Cybernetics, one of several brain scientists who migrated some or all of their research to China, announced plans to co-direct with Shanghai neuroscientist Pu Muming (Mu-ming Poo) an International Center for Primate Brain Research[44] built at a cost of U.S. $106 million.[45] Pu's success in cloning monkeys, which speeds breeding and eliminates genetic variation, is another draw.[46]

Finally, we consider *foreign technology transfer*, generally seen as a sign of weakness but which we regard—from China's perspective—as a stunning advantage. For more than six decades China has operated a comprehensive program of foreign technology appropriation to remedy shortcomings in indigenous science and technology without the cost, risk, and political challenges incurred by the world's liberal democracies. The phenomenon has been documented in scholarly and government studies both in general[47] and for AI.[48] It has been briefed to U.S. and allied elected and counterintelligence officials, who are well-informed on the matter, and is a mainstay of media reporting, so that the discussion turns

Neural Net Accelerator Board for China's Artificial Brain (brewbooks, licensed with CC BY-SA 2.0.)

not on whether these illegal and extralegal transactions take place but rather on what to do about it.

We raise the matter to emphasize that whatever else one thinks of it, China's hybrid system of indigenous innovation and foreign "borrowing" has been extraordinarily effective. China through its outreach efforts, talent programs, diaspora exploitation, cooperative ventures, open source tracking, overseas support guilds, indigenization enclaves, "two-bases" and "short-term return" schemas, and other hidden or barely disguised practices has mastered the skill of adapting useful technologies created abroad into its own (under-rated) indigenous enterprises.[49]

If these are China's advantages, what are its disadvantages? Two deficits are commonly cited: chip design and fabrication, and foundational research. We defer judgment on the former, which is outside our fields of expertise. As for the latter, China is seen as weak in basic research, specifically in AI theory, by the country's top practitioners. Sinovation founder and best-selling AI author Kai-Fu Lee argues that China's forte is its ability to create practical AI products, not revolutionize the field.[50] His point is supported by top Chinese scientists. Here is a sample:[51]

- Sun Maosong (孙茂松), Tsinghua University professor of computer science, argues that China lacks leaders in world-class scientific research and falls behind other countries in training "top talent in the basic sciences."[52]
- Tan Tieniu (谭铁牛), deputy director of CAS (see below), claims "At present, China is still in the 'follow-up' position in terms of frontier theoretical innovation of artificial intelligence. Most of the innovations are focused on technology applications."[53]

- Xu Kuangdi (徐匡迪) former head of the Chinese Academy of Engineering (CAE) said, "The cornerstone of artificial intelligence is mathematics, and the key element is algorithms. But China's investment in this field is far behind the United States."[54]
- Yau Shing-Tung (丘成桐), Harvard professor and Fields Medal winner, concludes that China "is still some distance from the United States and Britain in terms of basic theory and algorithm innovation."[55]
- Zheng Nanning (郑南宁), another CAE academician, believes it will take China another 5 to 10 years to reach world levels in basic theoretical and algorithmic research. Hardware design is also an issue.[56]

We regard these complaints as valid but vacuous: theory cannot be embargoed and there is no will to do so either by governments or by scientists,[57] who embrace collaboration as part of their enterprise. Accordingly, to the extent this is a problem at all, China is addressing it as it always has, by a robust program of foreign interaction, cooperation, co-option, licit and illicit transfers, and—like everyone else—by monitoring publicly available information.[58]

The Chimera of AGI

China's decision to focus on AI-brain research leads to speculation that the effort may be aimed at the "holy grail" of artificial general (human level) intelligence (AGI), or will end up there as an unintended consequence of this brain-centric pursuit. Indeed, as will be shown, that view is held by many Chinese researchers. The issue in a nutshell is this: in contrast to AI, which focuses on narrow problems of "creating programs that demonstrate intelligence in one or another specialized area,"[59] AGI aims at,

> "the construction of a software program that can solve a variety of complex problems in a variety of different domains, and that controls itself autonomously, with its own thoughts, worries, feelings, strengths, weaknesses and predispositions."[60]

In other words, the elements of human cognition—with instant access to the sum of the world's knowledge and ability to process that information at lightning speed. Since BI-AI models brain function to enhance AI programs, there is a tendency among scientists working in brain-inspired AI to equate their research with this outcome. A survey of China's AI scientists revealed 74 percent believe BI-AI will lead to general AI. The number rises to 83 percent among China's BI specialists.[61] These figures are buttressed by statements from BI-AI principals of standing:

Xu Bo (徐波), director of the CAS Institute of Automation—host to Beijing's Research Center for Brain-inspired Intelligence (home of the "Brainnetome" connectomics project), Associate Director of Shanghai's Center for Excellence in Brain Science and Intelligence Technology (中国科学院脑科学与智能技术卓越创新中心, CEBSIT), and chair of the "Next Generation Artificial Intelligence Strategic Advisory Committee" is cited in the Ministry of Science and Technology's official newspaper *S&T Daily*:

> "As General Secretary Xi Jinping pointed out in the collective study of the Politburo, artificial intelligence research must explore 'unmanned areas.' In the areas of swarm intelligence, human-machine hybrid intelligence and autonomous intelligence, there are large unmanned areas to be explored… We believe that autonomous evolution is a bridge from weak artificial intelligence to general artificial intelligence."[62]

Shi Luping (施路平), director of the Center for Brain-inspired Computing Research, Tsinghua University and leader of the research group that

created the Tianjic neuromorphic chip, has a novel epistemological take on the emergence of AGI:

> "Our human intelligence is built on carbon, and we have built the current digital universe on silicon. The structure of carbon and silicon is very similar, so we believe what can be realized on carbon, must be possible on silicon… Moreover, nanodevices have enabled us to develop electronic devices such as neurons and synapses at the level of human brain energy consumption, so now is the best time to develop artificial general intelligence."[63]

Tan Tieniu (谭铁牛), deputy director of the Chinese Academy of Sciences, deputy chief of the PRC's liaison office in Hong Kong, and a leading AI figure, explained in *Qiushi*, the Communist Party's main theoretical journal:

> "How to make the leap from narrow artificial intelligence to general artificial intelligence is the inevitable trend in the development of the next generation of artificial intelligence. It is also a major challenge in the field of research and application."[64]

Zeng Yi (曾毅), deputy director of CAS's Research Center for Brain-inspired Intelligence, 2019 member of the New Generation Artificial Intelligence Governance Expert Committee, and keynote speaker at "AGI-19," the 12th annual international conference on AGI:

> "Whether to develop general artificial intelligence, or limit it to specific AI is a major point of divergence among many proposals for artificial intelligence guidelines… In fact, the development of dedicated [专用, 'narrow'] AI does not completely avoid risk, because the system is likely to encounter unexpected scenarios in its application. Having a certain general ability may improve the robustness and adaptiveness of an intelligent system."[65]

Huang Tiejun (黄铁军), chair of Peking University's Department of Computer Science, dean of the Beijing Academy of Artificial Intelligence, and also a 2019 member of the New Generation Artificial Intelligence Governance Expert Committee:

> "My point is different from that of the other colleagues. Absolutely we should [build superintelligence]. Our human race is only at one stage. Why stop? Humans evolve too slowly. It's impossible for humans to compare to machine-based superintelligence. It will happen sooner or later, so why wait? Even from the perspective of human centrism or human exceptionalism, superintelligence is needed to face big challenges that we can't figure out. That's why I support the idea." (Future of Life conference)[66]

Other such prognostications are commonplace.[67] As part of the trajectory, China's Ministry of Science and Technology and the Beijing city government in 2020 stood up a "Beijing Institute for General Artificial Intelligence" (北京通用人工智能研究院, BIGAI)[68] headed by returned UCLA professor and renowned AI scientist Zhu Songchun (朱松纯),[69] in concert with Peking University's Institute for Artificial Intelligence and Tsinghua University's own (planned) AGI institute.[70] The facility is in Beijing's Haidian districts and will be staffed by some 1,000 researchers drawn from China and, as usual, "all over the world."[71]

The move will lead to clones, first in Shanghai then the other major cities and provinces. Our concerns are two-fold. Firstly, AI hype tends to outpace its accomplishments, and the former should not become the basis for fear and countermeasures. In our view, a *move toward* AGI is a natural feature of AI research, in China or anywhere, as AIs become more capable. While the research warrants scrutiny,

we believe AGI, understood literally, is not imminent (five years out) but possible in some form by the end of the decade.

Beijing Institute of General Artificial Intelligence

Inviting talents from all over the world

Secondly—and more ominously—AGI may not be the best way to envision the result of brain-inspired or other lines of AI research. One need not subscribe to an AGI scenario to appreciate that *all AI research* entails risks. Nor is AGI a necessary condition for "superintelligence." Here is one scenario, for example, which is plausible over a shorter term and comes directly from a credible Chinese source:

> "Speaking of the brain-computer interaction of tomorrow, we will move from intelligence [of one type] to intelligence [of another] (从智能而来，到智能而去). The future is not about replacing human beings with artificial intelligence, but making AI a part of human beings through interconnection and interoperability. A blend of human and computer without barriers is the inevitable end of the future."[72]

This potential outcome, a way station on the path to AGI, portends fundamental changes in the human condition, indeed, in the nature of humanity and is cause for concern by itself.

Policy recommendations

The authors are daunted by the expectation that we propose policies addressing the issues we write about—something not encouraged in our former lives. Here are three, offered in good faith.

1. Pay greater attention to AI safety

We assess the likelihood of China achieving artificial general intelligence (AGI) through BI-AI within the next five years as improbable. Chinese scientists agree. The project is in its infancy and there is nothing in the open literature to suggest China has made breakthroughs in key areas. We are less confident other troublesome aspects of this research will not emerge sooner rather than later. We encourage the U.S. government, allied nations, and scientists worldwide to draw China and its AI cadre into a strong safeguards regime to manage these common dangers.

2. Mitigate greyzone technology transfers

China's appetite for foreign technology, obtained with or without permission, is insatiable and we see no indication that China's status as an emerging S&T power will impact this behavior. Absent a concerted effort to control technology transfers, the rest of the world is disadvantaged as it invests resources in technologies that China acquires gratis. We propose the creation of dedicated centers, nationally and internationally, to monitor "informal" technology transfers and refer them to cognizant

authorities. The framework should also encompass legal transfers of sensitive technology where national security is at risk.[73]

3. Build a "National S&T Analysis Center"

China's AI-brain project blossomed in 2016, yet there has been no significant reporting about it outside China. As we describe elsewhere,[74] U.S. intelligence agencies, unlike China's, are ill-equipped to detect emerging technologies because their secrets-based platforms, a Cold War relic, are not tuned to capture worldwide scientific trends. Open source intelligence, by contrast, is well poised to provide the "indications and warnings" to reduce technology surprise. Realizing its full value will happen under the auspices of an organization established *outside the IC* to provide assessments and forecasts of S&T developments without institutional biases. PRISM

Notes

[1] This study expands on research done at Georgetown University, reported in the authors' "China AI-Brain Research: brain-inspired AI, connectomics, brain-computer interfaces."https://cset.georgetown.edu/research/china-ai-brain-research/. We thank CSET's Lynne Weil for connecting us with PRISM, Daniel Chou for data and graphics support, and Founding Director Jason Matheny for his counsel on AI policy.

[2] 国务院关于印发新一代人工智能发展规划的通知. State Council (35).

[3] Hannas and Chang, "China's 'artificial' intelligence," in Wm. C. Hannas and Didi Kirsten Tatlow, eds. *China's Quest for Foreign Technology: Beyond Espionage*, Routledge, 2021.

[4] Roberts, H., Cowls, J., Morley, J. *et al*. "The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation," *AI & Soc* (2020). https://doi.org/10.1007/s00146-020-00992-2. Sarah O'Meara, "Will China lead the world in AI by 2030?," *Nature*, August 21, 2019. https://www.nature.com/articles/d41586-019-02360-7.

[5] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, 2018.

[6] Pu Muming' Shanghai-based "International Mesoscopic Connectome Project," a part of the Chinese Academy of Sciences' Institute of Neuroscience, was founded in November 1999. A "Beijing Key Laboratory of Human-Computer Interaction" was stood up the same year.

[7] PRC State Council, "国务院关于积极推进"互联网+"行动的指导意见 (State Council Guiding Opinions on Positively Promoting 'Internet +' Activity)," No. 40, July 1, 2015. The notification promoted "AI and other technologies" as catalysts for commercial products, not as a self-contained discipline.

[8] PRC State Council, "国家中长期科学和技术发展规划纲要(2006-2020年) (National Medium- and Long-term S&T Development Plan (2006-2020))," February 9, 2006.

[9] PRC State Council, "国务院关于印发"十三五"国家科技创新规划的通知 (State Council Notification on National Science and Technology Innovation Programs for the 13th Five-Year Plan)," No. 43, July 28, 2016.

[10] Mu-ming Poo (Pu Muming), "Towards brain-inspired artificial intelligence," in *National Science Review* 5: 785 (October 25, 2018).

[11] Xi Jinping, "Striving to Build a World S&T Superpower," May 2016. http://www.xinhuanet.com/politics/2016-05/31/c_1118965169.htm.

[12] PRC State Council, "New Generation AI Development Plan." Translation by the Foundation for Law and International Affairs, verified by the present authors.

[13] Ibid.

[14] Zeng Yi (曾毅), Liu Chenglin (刘成林), Tan Tieniu (谭铁牛) in *Chinese Journal of Computers* (计算机学报), 39(1), January 2016, 212-222.

[15] Pu Muming (蒲慕明), Xu Bo (徐波), Tan Tieniu (谭铁牛) in *Bulletin of Chinese Academy of Sciences* (中国科学院院刊), 31(7), July 2016, 725-736.

[16] Zhang Xu (张旭), Liu Li (刘力), Guo Aike (郭爱克) in *Bulletin of Chinese Academy of Sciences* (中国科学院院刊), 31(7), July 2016, 737-746.

[17] Fan Lingzhong (樊令仲) and 13 others, primarily with Chinese institutional affiliations, in *Cerebral Cortex*, 26 (8), August 2016.

[18] Han Xue (韩雪), Ruan Meihua (阮梅花), Wang Huiyuan (王慧媛), Yuan Tianwei (袁天蔚), Wang Chaonan (王超男), Fu Lu (傅璐), Chen Jing (陈静), Wang Xiaoli (王小理), Xiong Yan (熊燕), Zhang Xu (张旭) in *Chinese Bulletin of Life Sciences* (生命科学), 28.11, November 2016, 1295-1307.

[19] Pu Muming (蒲慕明), Du Jiulin (杜久林), Nancy Y. Ip (叶玉如), Xiong Zhiqi (熊志奇), Xu Bo (徐波), Tan Tieniu (谭铁牛) in *Neuron* 92.3, November 2016. The Chinese version of the paper, issued separately, omits "Brain Diseases" from the title. It reads literally: "Comprehensive interpretation of the China Brain Project: from basic neuroscience to brain-inspired computing." The content of the two versions is comparable.

[20] Hannas and Chang, "China AI-Brain Research: Brain-inspired AI, Connectomics, Brain-computer Interfaces," Georgetown University / CSET, September 2020.

[21] The authors retrieved some 22,000 documents (2010-2019) from the China National Knowledge Infrastructure (CNKI) database of Chinese academic journals that responded to an abbreviated list of keywords on AI-brain topics. The chart is based on a hand-curated subset of papers that address the BI-AI topic specifically. The survey did not include papers in English or those whose primary authors are diaspora (overseas) Chinese.

[22] http://www.nsfc.gov.cn/publish/portal0/tab452/info69927.htm.

[23] http://www.research.pku.edu.cn/docs/2018-07/20180702201045167492.pdf.

[24] https://www.sciping.com/21237.html; http://www.cebsit.ac.cn/xwdt/202007/t20200722_5639392.html; http://news.sciencenet.cn/htmlnews/2021/1/452104.shtm; https://www.yicai.com/news/100028706.html.

[25] Some Chinese scholars add a fourth pillar: neuromorphic computing and chips. See Hannas and Chang, "China AI-Brain Research: Brain-inspired AI, Connectomics, Brain-computer Interfaces," Georgetown University / CSET, September 2020.

[26] IARPA, "IARPA Seeks Partners in Brain-Inspired AI Initiative," January 22, 2015, www.iarpa.gov/index.php/research-programs/microns.

[27] Olaf Sporns, *Discovering the Human Connectome*. The MIT Press, 2012. Nikola Kasabov. *Time-Space, Spiking Neural Networks and Brain-Inspired Artificial Intelligence*, Springer 2019. Also, Intelligence Advanced Research Projects Activity, "Machine Intelligence from Cortical Networks (MICrONS)" project, "Proposers' Day Briefings" (https://www.iarpa.gov/index.php/research-programs/microns/microns-baa).

[28] Xiamen, not a backwater by any means but not the first place one goes for cutting edge technology, has a history of AI research. Hugo de Garis, an AI pioneer and early AGI prophet, taught until 2010 at Xiamen University, where he built China's first "artificial brain." (https://en.wikipedia.org/wiki/Hugo_de_Garis). Ruting Lian, spouse of AGI's foremost proponent Ben Goertzel, did her doctoral work at Xiamen University's Fujian Key Lab for Brain-like Intelligent Systems (https://www.sciencedirect.com/science/article/abs/pii/S0925231210003498#!).

[29] https://braindata.bitahub.com/.

[30] Dr. Christof Koch, personal communication, August 2020.

[31] http://en.jitri.org/yanjiuyuan72.html.

[32] https://www.cingta.com/detail/17634.

[33] Zhou Wenting, "Insights to Come from New Brain Research Base," *China Daily*, July 19, 2018, http://www.chinadaily.com.cn/cndy/2018-07/19/content_36603871.htm.

[34] https://www.cbicr.tsinghua.edu.cn.

[35] Our thanks to DARPA contractor Dr. Jennifer Wang and CSET data scientist Daniel Chou for analysis and graphics. Affiliation names were normalized. If multiple authors identify with ABC in a given paper, then ABC's output tally increased by only 1. "Microsoft Research" (33) is different from "Microsoft Research Asia (MSRA)" (18) and the rest of "Microsoft" (25).

[36] Based on Microsoft Academic "AAAI Conference Analytics, January 2019. https://www.microsoft.com/en-us/research/project/academic/articles/aaai-conference-analytics/.

[37] https://zhuanlan.zhihu.com/p/81781547.

[38] https://www.baai.ac.cn/news_article?content_id=43&type=news. Interestingly, the three top-ranked Chinese institutes for accepted papers at the 2020 NeurIPS event are all located in Beijing—Tsinghua, Peking University, and Beijing Academy of Artificial Intelligence (北京智源人工智能研究院, BAAI). A Shanghai-based institute ranks only 8th after iFlytek, Alibaba, Huawei, and the University of Hong Kong.

[39] Some 7,077 affiliation instances were extracted from 1,589 AAAI 2020 accepted papers. Each affiliation in a given paper was labeled as China or non-China according to a hand-curated list of 616 affiliation name variants. https://aaai.org/Conferences/AAAI-20/wp-content/uploads/2020/01/AAAI-20-Accepted-Paper-List.pdf.

[40] https://zhuanlan.zhihu.com/p/81781547.

[41] See for example Remco Zwetsloot, "Keeping Top AI Talent in the United States," Center for Security and Emerging Technology, December 2019, https://cset.georgetown.edu/research/keeping-top-ai-talent-in-the-united-states/.

[42] There is a counter-argument that access to NHP's derails research from human-based studies and should be seen as a disadvantage, since discoveries about the one do not necessarily transfer to the other.

[43] David Cyranoski, "China is positioning itself as a world leader in primate research," *Nature*, April 20, 2016, https://www.nature.com/news/monkey-kingdom-1.19762#auth-1.

[44] Gretchen Vogel, "Animal rights conflict prompts leading researcher to leave Germany for China," *Science*, January 27, 2020, https://www.sciencemag.org/news/2020/01/animal-rights-conflict-prompts-leading-researcher-leave-germany-china.

[45] https://www.nature.com/articles/d41586-019-00292-w.

[46] Sarah Zhang, "China is Genetically Engineering Monkeys with Brain Disorders," *The Atlantic,* June 8, 2018, https://www.theatlantic.com/science/archive/2018/06/china-is-genetically-engineering-monkeys-with-brain-disorders/561866/.

[47] The IP Commission Report, *The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, February 2019; Wm. C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage* (London and New York: Routledge, 2013); Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy" (Washington, DC: Defense Innovation Unit Experimental, February 2017); Office of the United States Trade Representative, "Section 301 Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation," March 27, 2018; U.S.-China Economic and Security Review Commission, "2019 Annual Report to Congress," November 2019; Hannas and Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage*, Routledge, 2020; and Anastasya Lloyd-Damnjanovic and Alexander Bowe, "Overseas Chinese Students and Scholars in China's Drive for Innovation," U.S.-China Economic and Security Review Commission, October 7, 2020.

[48] Hannas and Chang, "China's Access to Foreign AI Technology—an Assessment," Georgetown University, Center for Security and Emerging Technology, September 2019; Hannas and Chang, "China's 'Artificial' Intelligence," in Hannas and Tatlow, eds. *China's Quest for Foreign Technology: Beyond Espionage*, Routledge, 2020; Hannas and Chang, "China AI-Brain Research," Center for Security and Emerging Technology, September 2020.

[49] We point out to analysts mired in the budget-as-progress paradigm that in China things work differently. Unless one factors in the operating costs of a multi-tiered transfer apparatus with over 100,000 operatives, hundreds of subsidized commercialization centers, and adds a constant for unearned advantages gained by tapping proprietary technology, China's visible R&D budgets have little meaning in cross-country comparisons.

[50] https://www.voachinese.com/a/kai-fu-lee-on-ai-development-2018116/4662278.html.

[51] Adapted from Hannas and Chang, "China's 'Artificial' Intelligence," in Hannas and Tatlow, eds. *China's Quest for Foreign Technology: Beyond Espionage*, Routledge, 2020, pp. 199-200.

[52] https://mp.weixin.qq.com/s/YtXW8HlWlRGGxQn5aOeabA.

[53] Qiushi (求是), April 2019. https:// www.kunlunce.com/llyj/fl11111/2019-02-28/131480.html.

[54] http://www.caeshc.com.cn/news_view.php?id=7997.

[55] http://news.stcn.com/2019/1017/15436849.shtml.

[56] https://www.nature.com/articles/d41586-019-02360-7.

[57] We dodge the question of whether foundational research should be subject to export control. This hot-button issue is currently a matter of debate among USG policymakers.

[58] Hannas and Chang, "China's STI Operations," Center for Security and Emerging Technology, January 2021.

[59] Cassio Pennachin and Ben Goertzel, "Contemporary Approaches to Artificial General Intelligence," in Goertzel and Pennachin, eds., Artificial General Intelligence, Springer, 2007, p. 1.

[60] Ibid.

[61] Hannas and Chang, "China AI-Brain Research: Brain-inspired AI, Connectomics, Brain-computer Interfaces," Georgetown University / CSET, September 2020. China's AI generalists were split on whether AGI could be achieved in 5-10 years or 10+ years. BI-AI specialists, facing real laboratory problems, opted for the latter prognosis.

[62] *S&T Daily*, June 20, 2019 (http://www.stdaily.com/qykj/qianyan/2019-06/20/content_773207.shtml).

[63] *Tencent Net* (腾讯网), October 31, 2019 (https://new.qq.com/omn/20191104/20191104A0BD9U00.html).

[64] *Qiushi* (求是), April 2019. http://www.qstheory.cn/dukan/qs/2019-02/16/c_1124114625.htm.

[65] *Guangming Daily* (光明日报), January 24, 2019. http:// www.cas.cn/zjs/201901/t20190124_4678012.shtml.

[66] Synthesized from Huang's address to the Future of Life conference on "Beneficial AGI," Puerto Rico, January 5, 2019, session 2 "Should we build superintelligence?" (https://www.youtube.com/watch?v=xLYE11yW-hQ&t=17s). Huang's Beijing academy announced its 2020 research would focus on the "cognitive neural basis of artificial intelligence" aimed in part at "building a functional brain-like intelligent system with performance that exceeds a brain" (构建功能类脑、性能超脑的智能系统) http://www.bj.chinanews.com/news/2020/0825/78660.html.

[67] A review of CNKI Chinese language academic journals shows a slight upward progression of papers mentioning "AGI" from 2014 through 2016, spiking sharply in 2017, the year after BI-AI took root, and rising thereafter.

[68] https://bigai.ai/index.html. "通用人工智能" ("GAI") is the Chinese term for AGI. Chinese reverses the English word order, hence the institute's name "Beijing Institute of General Artificial Intelligence" or "BIGAI."

[69] http://news.pku.edu.cn/xwzh/cc4e714d8d-ef4d1db071a43771c2bb41.htm, and https://www.sohu.com/a/420639562_260616.

[70] https://www.163.com/dy/article/G3C518KF0511DPVD.html.

[71] Ibid.

[72] Ming Dong, "Decipherer of 'Brain Language Code'." https://m.chinanews.com/wap/detail/zw/gn/2019/12-25/9042386.shtml. Ming is Dean of Tianjin University's Academy of Medical Engineering and Translational Medicine and Director of the Tianjin Key Laboratory of Brain Science and Neuroengineering.

[73] Specific proposals for a China-oriented technology transfer management regime are outlined in Hannas and Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage*, Routledge, 2020, pp. 329-332. Interdiction practices are also reviewed in chapter 18, "Mitigation Efforts to Date" by James Mulvenon, et al.

[74] Hannas and Chang, "China's STI Operations," Center for Security and Emerging Technology, January 2021.

Central Banks (Eric Prouzet, Unsplash.com)

The Pentagon's First Financial War

How DOD can fight back against China

By Justin Bernier

China's strategy for achieving its global ambitions is driven as much by bankers and bribes as bombs and bullets. The Chinese Communist Party (CCP) continues to take every step imaginable to appropriate dual-use technologies—those with both civil and military applications—from the United States and its allies, while attracting billions of dollars in Western capital used to finance a modernization program for the People's Liberation Army (PLA). The U.S. Department of Defense (DOD) reports that the strategic end state this program supports, if realized, would have serious implications for nothing less than "the security of the international rules-based order."[1] The extent of this threat implies that military tools alone may not prevent an undesirable outcome.

The Pentagon is dutifully preparing for the possibility of a kinetic war with the PLA, but DOD has a role to play on the financial battlefield, too. Defense leaders should consider three policy initiatives to curb the flow of technology and capital to China:

- Encourage compliance on technology transfer laws by rewarding companies and universities with strong export control practices when they compete for federal grants and contracts.
- Discourage investment in China's "bad actor" companies by supporting a government policy to assume custody of shareholder voting rights in certain state-owned enterprises (SOE).
- Track Chinese expansionism through business and financial channels with an all-source intelligence capability designed to provide U.S. officials with strategic warning and policy support.

A bureaucratic purist could paint these initiatives as inconsistent with the Defense Department's core competencies, but this view would be short-sighted. DOD may be the only government agency with the financial leverage, the knowledge base, and the political will to roll back China's strategy of stealing military technology and securing foreign capital for its armed forces buildup against the United States. More certain is the reality that U.S. servicemembers are endangered by ongoing technology and capital flows from the West to the People's Republic of China (PRC). These high stakes give the Pentagon little choice but to fight back

Justin Bernier is a Founding Partner of All Source Investment Management, a Connecticut-based wealth advisory firm. He advises clients in twenty states, focusing on portfolio management, alternative investments and risk management for accredited individuals and select nonprofit institutions. Nothing in this article should be construed as financial advice.

against the financial warfare that China is already waging around the world.

Money Bombs

Economic warfare is the age-old strategy of weakening a state through trade embargoes, tariffs, expropriation, and other sanctions. U.S. economic wars are normally orchestrated by the Treasury and State Departments, with DOD playing a supporting role in the enforcement of embargoes and the denial of defense purchases. Congress has also been an active participant in economic warfare, especially concerning sanctions against Iran, North Korea and Russia. Although a proven tool for policymakers, economic warfare can be politically difficult to manage because of its perceived effect on general populations and global commerce. U.S. tariffs on select Chinese sectors in 2019, for instance, generated frenetic media headlines despite causing only nominal changes in overall trade levels.

A subset of economic warfare—one more targeted and easier to control—is financial warfare; the denial of money or credit to specific entities. Restricting or redirecting capital with precision can maximize pressure on foreign leaders who need hard currency for operating expenses but also minimize the effects on legitimate commercial interests. In the example of Russia, the Small Business and Entrepreneurship Council (SBEC) has lobbied for financial penalties against President Vladimir Putin and other Kremlin insiders rather than broad economic sanctions thought harmful to American companies. Untargeted sanctions on Russia would "cascade down the supply chain," argues SBEC President Karen Kerrigan, hurting U.S. vendors in the aerospace, agribusiness, and energy sectors, while handing Chinese companies an opportunity to capture market share.[2]

Financial warfare is an option for those combatants armed with a large budget, like the Department of Defense, but Pentagon leaders may not realize their own potential. The DOD contract award process could be used to counter Chinese espionage and intellectual property theft by giving preference to companies and universities that safeguard sensitive technologies. Secondly, DOD leaders could discourage portfolio investment in companies within the PLA supply chain—so-called "bad actors"—by backing a plan to relieve shareholders of their voting rights in these state-owned enterprises. Finally, an all-source intelligence capability designed to track China's non-military expansion would support technology and capital control initiatives while helping U.S. officials develop future policies.

There may be fertile ground for proactive policies in Washington, where members of both political parties appear to recognize the present CCP threat. Several months into his administration, President Joe Biden has sustained some initiatives by President Donald J. Trump to strengthen export controls on China. In June 2020, then-National Security Advisor Robert O'Brien catalogued these accomplishments, including measures to stop the PLA from using student visa programs to place its personnel in American universities for the purpose of stealing technology, intellectual property, and sensitive data. Rounding out the list was a decision to "halt the investment of U.S. federal employee retirement funds into PRC companies..."[3]

The Wall Street Problem

President Trump's senior advisor on national security was referring to a seemingly obscure benefits debate in the first half of 2020, when Chinese stocks nearly became part of the Thrift Savings Plan (TSP), the retirement investment program familiar to Defense Department civilians and servicemembers. Based on financial advice from BlackRock, the Federal Retirement Thrift Investment Board had voted to replace the benchmark for its international fund (a.k.a. the "I Fund"), an index of some 900 companies based in developed markets.[4] The

proposed benchmark, known as the MSCI ex-USA Investable Market Index, would have expanded the I Fund to 6,600 components—almost every publicly traded company outside the United States—to include defense firms at the heart of China's "military-civil fusion" strategy for developing a world-class fighting force.

Aviation Industry Corporation of China (AVIC), with annual defense revenue comparable to Northrop Grumman, is an aircraft manufacturer listed on the Shenzhen exchange. AVIC is developing the PLA Air Force's next-generation Chengdu J-20 and Shenyang FC-31, the latter with technology stolen from the Joint Strike Fighter program.[5] China Shipbuilding Industry Company Limited (CSIC) is a subsidiary of the world's biggest maritime conglomerate, producing warships, weapon launchers and other offensive equipment for the PLA Navy. The Shanghai-listed company has more annual defense revenue than the largest military shipbuilding company in the United States, aircraft carrier builder Huntington Ingalls Industries. These two companies and other Chinese defense firms were part of the MSCI index.

Changing the I Fund's benchmark would have plowed roughly $10 billion dollars of TSP assets into Chinese listed stocks, including defense firms and other state-owned enterprises (SOE), inflating their prices and signaling financial strength that can help a company grow.[6] Companies with higher-priced shares often borrow at low interest rates for capital expenditures. Higher-priced shares also facilitate equity financing (selling shares to raise capital) and acquisitions through equity deals. In other words, Chinese defense firms would have been propped up with the retirement accounts of American servicemembers who might someday face the PLA weapon systems they produce.

BlackRock recommended the benchmark change ostensibly to give TSP participants exposure to companies outside of developed markets. There are sound reasons to include emerging market stocks in a retirement account. In addition to attractive growth rates, they offer diversification benefits that may improve long-term returns. BlackRock, however, took a scattershot approach that failed to exclude bad actors from the index. Although stock indices can be modified to reflect commonsense public policy concerns, none of the leading indexers—not Vanguard, State Street, or BlackRock—have voluntarily addressed the problem. As a result, millions of Americans are unwitting investors in China's publicly traded defense firms.

A Chinese flag flies outside the New York Stock exchange on May 30, 2013 in New York City. (Anthony Correia)

BlackRock may have had the best interest of TSP participants in mind when it recommended a broader international benchmark, but the asset manager also stood to expand its influence within 6,600 companies and their respective governments, exacerbating troubling—if not illegal—conflicts of interest. *The Wall Street Journal* has revealed systematic pandering by U.S. firms hungry for access to China's tightly controlled financial services market. In August 2020, after siding with Beijing during trade negotiations with Washington, BlackRock became the first non-Chinese firm to receive preliminary approval for a wholly owned mutual fund company on the mainland. Presumably for supporting Beijing in the same talks, J.P. Morgan, Goldman Sachs, and at least two other firms were granted similar entries to China's $17 trillion investment and asset management market. The very decision to include Chinese stocks in the MSCI indices, the newspaper reported, was championed by BlackRock in exchange for state approval of a private fund business in 2017.[7]

The BlackRock recommendation probably would have been adopted with little notice were it not for Roger Robinson, Jr., a past-Chairman of the U.S.-China Economic and Security Review Commission. Earlier in his career, Robinson had coordinated the Reagan Administration's economic war against the Soviet Union from his post at the National Security Council. Upon learning that the TSP intended to buy Chinese equities, Robinson gave a series of speeches and interviews to raise public awareness of the situation. President Trump took notice; he vetoed the benchmark change and then re-nominated three appointees for the investment board to ensure in hopes of better oversight going forward.

Although based on national security concerns, President Trump's decision to axe the new I Fund benchmark made sense from an investing perspective, as well. A study commissioned by the TSP investment board found that using the expanded benchmark would have resulted in similar returns over the last five years and *lower* returns over the last ten years in the target-date funds it tested.[8] The same review projected that swapping indices going forward would improve returns by ten basis points (0.10 percent) per year—just one-tenth of one percent.[9] One reason for the unimpressive returns is that the emerging market small cap index, a major component of the proposed benchmark, has underperformed over the last decade.

In practice, using a benchmark of 6,600 companies may be diversification overkill. Even if expected returns are slightly higher after including equities from China, India, Brazil, and other rapidly growing countries, a benchmark consisting of every global stock is unsuitable for the retirement accounts of most government employees and servicemembers. Many of these positions carry illiquidity risk because they are listed on exchanges with low trading volume and abbreviated hours. Such markets oftentimes have accounting standards beneath those found in developed markets. Beijing's notable refusal to comply with generally accepted accounting principles would expose TSP investors to business risks they may not expect.

In the final months of his term, President Trump issued an executive order banning financial transactions in companies recognized as "directly supporting the efforts of the PRC's military, intelligence, and other security apparatuses."[10] The original directive, E.O. 13959, and its amendment prohibited investment in forty companies traded on Chinese exchanges. The banned stocks and their subsidiaries were to become un-investable to funds inside employee retirement accounts as well as pensions and endowments, forcing indexers to remove the proscribed companies and re-weight their China benchmarks accordingly. "The underlying principle," said then-White House advisor Dr. Peter Navarro, "is that American capital should not be used to finance Chinese militarization, particularly weapons that

are going to be used to kill Americans."[11] The Biden Administration subsequently postponed full implementation following complaints from the financial services industry that the executive orders were too open-ended for Wall Street to comply.[12]

The Silicon Valley Problem

Self-defeating value transfers to China are not limited to the financial services industry. Silicon Valley companies have knowingly transferred next-generation technology to the People's Liberation Army at the expense of U.S. national security. In 2019, then-Chairman of the Joint Chiefs of Staff General Joseph Dunford testified to the Senate Armed Services Committee that Google was developing artificial intelligence (AI) capabilities for China even as it spurned similar efforts by the Pentagon. "The work that Google is doing in China is indirectly benefiting the Chinese military," said Dunford. "We watch with great concern when industry partners work in China knowing there is that indirect benefit…and frankly, 'indirect' may not be a full characterization of the way it really is; it's more of a direct benefit to the Chinese military."[13]

Venture capitalist Peter Thiel was even less circumspect: "The weird fact, that's indisputable, is that Google is working with communist China but not with the U.S. military on its breakthrough AI technology." The Facebook boardman speculated that Google sided with China because its leadership expected infiltrators to steal the technology otherwise. Nevertheless, said Thiel, Google's decision to abandon work on a set of computer-vision algorithms known as Project Maven—"a Manhattan Project for AI"—in favor of China was possibly treasonous given their dual-use military applications.[14]

Coupled with China's stated objective of becoming the world's first "AI Superpower," Google's behavior intimated a fundamental disagreement between the Pentagon and Silicon Valley. The reality, however, is a close partnership dating back years. In fact, the Department of Defense has awarded information technology companies thousands of contracts that could be leveraged to strengthen export controls against China. Tech Inquiry, a nonprofit organization led by former Google executive Jack Poulson, researched the breadth of these deals in 2020 as part of a broader transparency project. The study revealed how big tech companies are awarded DOD contracts through intermediaries, including traditional defense firms, like Dell and General Dynamics. Data pulled from federal procurement records showed that Microsoft held the largest number of subcontracts (6,680), followed by Amazon (477), Google (384), and Facebook (172). Also listed were graphics specialist NVIDIA (163), Twitter (43), and Palantir (26), a software company specializing in data analytics.[15]

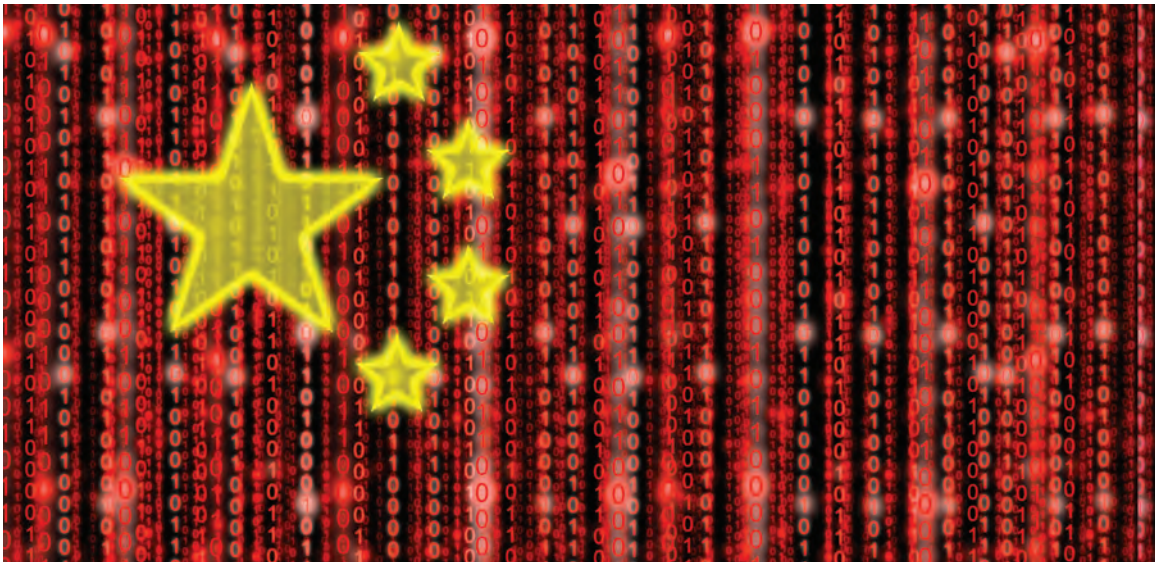
DOD's reliance on big tech companies that also work for the PRC suggests the U.S. export control system will continue to struggle absent structural reforms. After reviewing the responses of seven agencies on illicit transfers, the Senate Permanent Subcommittee on Investigations reported that the federal government has no comprehensive effort to counter Beijing's "strategic plan to acquire knowledge and intellectual property from researchers, scientists, and the U.S. private sector."[16] The subcommittee described a "whole-of-government campaign to recruit talent and foreign experts from around the world" for the purpose of making China the undisputed leader in science and technology by mid-century. The recruitment programs have incentivized thousands of U.S. citizens to transmit knowledge and research to China "in exchange for salaries, research funding, lab space, and other incentives."[17]

The PRC also obtains militarily useful technology through private equity and sovereign investment funds, hundreds of which have operated in the United States with some $600 billion in government-provided capital.[18] In 2014, for example, the Ministry of Finance and China Development Bank

Capital invested $20 billion to launch the National Integrated Circuit Industry Investment Fund with the stated goal of accelerating the semiconductor industry in the PRC.[19] The fund has reportedly invested in about two-dozen semiconductor makers, such as video-display processor Pixelworks and Black Sesame Technologies, an artificial intelligence company focused on autonomous driving and advanced driver-assistance systems.[20] The fund's second round of financing was seemingly unaffected by a recent drop in Chinese venture capital investments, raising $29 billion from an extended list of government entities, state media has announced.[21] The U.S. has stiffened regulations to slow China's acquisition of sensitive technologies, especially those associated with unmanned vehicles, but private equity deals that are potentially harmful to national security continue to be approved.[22]

The situation has been no less challenging in Europe, where Chinese state-owned enterprises have systematically acquired high-tech companies, spending hundreds of billions of dollars against nominal resistance from government regulators. China's European spending spree peaked in 2016, but only because Beijing re-imposed capital controls, concerned that its banking system had become overleveraged by purchasing foreign assets.[23] The three largest targets for Chinese capital—Germany, France, and the United Kingdom—have since improved their oversight of mergers and acquisitions that affect national security, while Brussels has implemented new guidelines to screen foreign direct investment within the greater European Union.[24]

A group of European governments recently rejected Huawei Technologies and ZTE Corporation as 5G equipment providers following a diplomatic row with Washington, which had designated the Chinese telecoms as threats to U.S. national security. Such intermittent progress is welcome news, but there remains much less transatlantic cooperation on export controls than in decades past, when NATO members adopted strict rules governing transfers to the Soviet Union and PRC. China's economy has since matured into a crucial market for European exporters, making technology and capital controls more painful than ever to the international



Structural reforms will be necessary to prevent science and technology transfers from Silicon Valley to the PLA, including Google's work developing AI capabilities for China, from harming U.S. national security. (New America at www.newamerica.org under Creative Commons license.)

business community. In 2020, Germany for the first time exported more goods and services to China than to any single European Union trading partner.[25] By the end of 2021, China could unseat the United States as Germany's largest importer. Other EU powers are less dependent on Chinese demand, but there is no mistaking that multilateral support for an export control regime directed at the second largest market in the world will require the United States and its closest allies to bring significant economic and diplomatic pressure to bear.

Impact Investing

The problem of technology transfers to China may have a financial solution. The U.S. government has authority to link federal funding to export controls in order to induce compliance across industry and academia. Ironically, the big banks may provide a blueprint for this approach. "Impact investing," J.P. Morgan explains, is a strategy for generating "measurable positive social or environmental impact alongside financial return."[26] Commonly known as "Environmental Social Governance" (ESG), the movement has gained popularity in recent years, with an estimated $30 trillion in assets now managed under some form of impact investing.[27] While the political values behind the ESG movement are not without controversy, the impact investing method itself is transferrable to financial warfare operations.

Impact investing is executed in one of two ways. Under the exclusion method, asset managers invest in only those companies with acceptable ESG scores. Businesses are rated based on a host of criteria, such as the number of females serving on the board of directors or the amount of greenhouse gasses emitted. The ratings determine whether an associated stock or bond is purchased. For example, low ESG scores might cause a portfolio manager to omit oil and mining stocks from a mutual fund in favor of companies that build renewable energy products.

A more direct method of impact investing uses shareholder activism to change or modify corporate behavior. Voting rights allow investors to weigh in on key corporate decisions, such as acquisitions and board elections. Shareholders may use proxy votes to cast a ballot when they are unable to attend meetings in person. Investors in a comingled vehicle—typically a mutual fund or exchange-traded fund—relinquish their voting rights to the asset manager, who can exercise policy preferences through a third-party company or internal governance team.

National Security Governance (NSG)

The Department of Defense can press industry to increase its efforts against Chinese espionage and influence operations by employing impact investing methods in its contract award process. Every company that competes for DOD work could receive an NSG rating that reflects its export control compliance record and its plan for protecting sensitive technology in the future. Under such a merit-based system, contractors that adopt best practices would be rewarded with NSG credits; those that continue to leak dual-use technology would receive debits. Integrating this system into the contract award process so that NSG ratings influence close competitions would strongly incentivize vendors to safeguard technologies from U.S. adversaries.

Educational institutions that apply for DOD research grants should also be rated on their record of protecting sensitive technologies. Many university leaders have neglected to take effective action against Chinese espionage and influence operations despite ample warning from government agencies. Some prestigious American schools have even accepted millions of dollars in unreported payments from China in exchange for access. The Federal Bureau of Investigation recently confirmed that China pays scientists at U.S. universities to steal technology, including "valuable, federally funded research," to the point where American taxpayers are "footing the

bill for China's own technological development."[28] Linking NSG ratings to research funding may prove the best way for DOD to protect its intellectual property on campuses where administrators have shown little interest in export controls.

NSG ratings could be managed by the Defense Technology Security Administration in conjunction with the Bureau of Industry and Security at the Department of Commerce and other agencies within the U.S. export control regime. Vetted service providers with expertise in industrial and cybersecurity policy could calculate NSG grades using the DOD model. Ultimately, the U.S. government could extend NSG ratings beyond defense vendors and grant recipients to include federal contracts of all kinds. American companies and universities that enjoy federal funding would almost certainly take preventative action if they stood to lose millions—even billions—of dollars for not protecting sensitive technologies.

Federal contractors with poor NSG grades would need to be held accountable for the system to work. Under U.S. law, contractors can be debarred or suspended under a variety of circumstances. Statutory debarments and suspensions for violating laws apply across the federal government and are often mandatory punishments with prescribed terms. Congress could also deny DOD research grants and contracts to institutions of learning that do not sustain a proficient NSG rating. One statutory debarment provides precedence by denying defense funds to schools that prohibit military recruiting on campus.[29] More flexibility is found under the Federal Acquisition Regulation (FAR), which authorizes the exclusion of contractors to protect government interests more broadly. The White House could issue executive orders that amend the FAR to exclude contractors—foreign and domestic—that fail the NSG test. As the largest buyer of goods and services in the world, the U.S. government is well positioned to require effective export controls from friends and allies in exchange for its business.

A New Kind of Proxy War

The National Security Governance framework might also help the Pentagon temper Wall Street's appetite for Chinese stocks. Ironically, the accumulation of shareholder voting rights in Chinese companies by U.S. asset managers offers the Department of Defense an opportunity to reduce technology and capital flows to the CCP's state-owned enterprises. Due to the large amount of proxy votes associated with them, modern index funds have become de facto partners of China's State Council, under which all SOEs are managed and regulated. While the Chinese Communist Party has firm control over the state-owned enterprises, a large percentage of their tradable shares are held by U.S. funds, exposing American investors to real business risk with only the illusion of influence. The power imbalance is made worse by the Chinese government's ability to suspend stock exchange activity at will. If Beijing can halt trading for indefinite periods of time when market conditions are volatile, then it can prevent investors from selling shares during a foreign relations crisis.

Beijing's unquestioned authority over all capital invested in China also raises issues for U.S. firms that possess sensitive technologies. The FBI explains that China uses not only its intelligence services, but also state-owned enterprises and supposed private companies, to steal data and know-how. Cyber intrusions and the corruption of trusted insiders are among the sophisticated techniques the Chinese military use to target individuals.[30] To help American companies avoid these traps stateside, the Department of Defense recently sent to Congress a list of PLA-linked companies operating inside the United States.[31] The next logical step is for DOD to produce a list of such companies operating inside the PRC itself.

The cleanest way to keep bad actors at a safe distance is to create a corporate buffer. U.S. asset managers who insist on holding stock in China's most suspect SOEs should be required to cede their

voting rights in those concerns. The federal government could then manage the proxy votes in trust using third-party fiduciaries who are familiar with the corporate governance rules in the PRC as well as the national security priorities of the United States. Uncle Sam would effectively replace BlackRock, State Street, and Vanguard inside the boardrooms of CCP-controlled companies. Complaints from Beijing over Washington's involvement in Chinese businesses would be expected but easily dismissed, given the PRC's ownership stakes in U.S. companies through state-backed investment funds.

Coercion is another reason for the U.S. government to assume the voting rights of many state-owned enterprises. The CCP has pressured Western investors to toe the party line on key corporate governance votes, research shows, with large mutual funds less likely to oppose reform proposals than smaller shareholders.[32] In 2017, BlackRock and other asset managers reportedly voted to require the boards of two Hong Kong-traded companies—China Petroleum & Chemical Corp and Industrial & Commercial Bank of China—to seek advice from the CCP on important decisions.[33] Boardroom bullying and intimidation tactics of this kind prevents civilian asset managers from acting independently on behalf of their clients, violating fiduciary standards that U.S. regulators expect of mutual funds and other publicly traded investments.

A proxy voting system based on NSG investing principles can be realized using the International Emergency Economic Powers Act (IEEPA), which gives the president broad authority to limit financial transactions in support of national security goals. The federal government has already recognized the PRC as a "foreign adversary," because it is "… engaged in a long-term pattern of serious instances of conduct significantly adverse to the national security of the United States…"[34] Upon determination that China's growing military power represents a national emergency, the executive branch could assume control of the voting rights in select CCP-connected companies. U.S. citizens, companies, and subsidiaries would ideally be covered so that offshore holdings are non-exempt.

Challenges to using IEEPA in this manner—even by powerful institutional investors—would probably be ineffective. Legal precedence is clear that U.S. citizens financially harmed by economic sanctions are not entitled to government compensation.[35] The court of public opinion offers plaintiffs even less promise. Retail investors whose voting rights are already held by asset managers are unlikely to be affected. Equally difficult to imagine is everyday Americans sympathizing with Wall Street executives who are denied access to the boardrooms of China's defense contractors.

The NSG proxy vote solution would be more effective than delisting all Chinese stocks from U.S. stock exchanges. Companies that fail to meet accounting standards should be expelled, but this gesture will not slow U.S. capital flows to Chinese companies operating in the global marketplace. Samsung Electronics is listed on the Korea Exchange without an American depository receipt that U.S. investors can purchase from home, yet a market capitalization of more than $400 billion makes it one of the world's largest companies.

Another questionable idea—outlawing all Chinese equities—would be politically challenging at home and potentially destabilizing abroad. Bloomberg notes that U.S. residents have amassed roughly $700 billion worth of Chinese stock, but the real figure is likely double that when offshore accounts are included.[36] Even if a ban on Chinese stocks became law, institutional investors have well-established workarounds to trade foreign securities. Chinese debt, for instance, already accounts for an estimated one-third of corporate bond investments made through the Cayman Islands.[37] Rather than tilt at windmills trying to keep dollars from entering Chinese exchanges, the U.S. government

should simply require shareholders of certain state-owned enterprises to relinquish their proxy votes to federal trustees. Such a policy would not end U.S. investment in China, but it would surely discourage ownership of bad actors by large institutions, forcing Beijing to reconsider its pursuit of American capital.

Employees in the United States could benefit from policies that discourage retirement fund managers from buying SOE shares in general. Back-testing shows the WisdomTree China ex-State-Owned Enterprise Index—a benchmark of Chinese stocks less those with at least twenty percent government ownership—dramatically outperforming the MSCI China Index in recent years (see figure 1). While past performance is no guarantee of future results, since inception the China ex-SOE Index has grown twice as fast as the standard China benchmark on an annualized basis, suggesting that average investors might fare better without exposure to companies directly controlled by the PRC.[38]

Similarly, American employees might be well served without the corporate bonds of many state-owned enterprises. Once thought to enjoy government backing, these bonds have exhibited higher default rates since 2018, when provincial authorities and regulators began letting some SOEs miss payments. The CCP's "orderly exit" approach to overleveraged SOEs appears part of a broader strategy to restructure debt at the expense of foreign bondholders. While perhaps orderly today, American investors could be left holding the bag if widescale defaults triggered panic selling out of SOE bonds.

The risk inherent to state-owned enterprises stems from the reality that many lack the controls and motives of conventional businesses. "Chinese regulators are often politically powerless to impose financial discipline on major SOEs," the U.S.-China Economic and Security Review Commission reports, "as officials often pressure banks to grant them favorable interest rates and even loan forbearance."[39] The absence of real accountability means that uncompetitive SOEs may operate as "zombies"—indebted companies that can only repay interest—long after becoming insolvent. On balance, state-owned enterprises are considered less efficient, less innovative, less growth-oriented and more corrupt than privately owned Chinese companies, all but ensuring underperformance over time. Newer state-controlled companies, such as Alibaba, may ultimately improve the performance of SOEs, but

Figure 1. Hypothetical Growth of $10,000, China ex-SOE Index vs. MSCI China Index, 2015 - 2021

the underlying risks that make many of these securities unsuitable for average investors will remain.

Financial Counterattack?

How might the PRC react to stronger technology and capital controls? The American press has speculated that China could dump its U.S. Treasury securities in anger or as part of a strategic plan to de-dollarize the global economy. The idea makes for excitable headlines but is improbable for the basic reason that China buys Treasurys so that America will buy its goods. A PRC selloff of Treasurys would create an excess supply of dollars, increasing the relative value of the Renminbi at the expense of Chinese exporters, who rely on a weak currency to make their products competitive in the U.S. market. Taken to the extreme, a strong Renminbi could devastate China's export-dependent economy. Now officially labelled a "currency manipulator" by Washington, Beijing has all but refused to discuss the issue, an advantageous foreign exchange rate—i.e., a relatively strong U.S. Dollar—being the lynchpin of its economic strategy.

China's financial system also needs the safety and stability of Treasurys. The People's Bank of China might ultimately reduce its reliance on the U.S. Dollar in favor of competing reserve currencies,

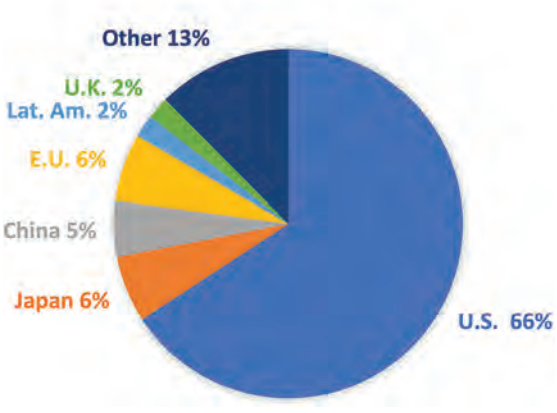


Figure 2. China holds about 5% of outstanding Treasury securities[40]

but such a move is unlikely anytime soon. The Chinese economy has never been so leveraged, with a record three-hundred percent debt to gross domestic product, putting its financial institutions in no position to dump dollars used for reserves and international payments.[41] China's central bank more likely worries about losing access to dollars in the event of a crisis. In July 2020, Chinese state lenders reportedly scrambled to secure alternate sources of liquidity after U.S. congressmen threatened financial sanctions on banks serving government officials behind the Hong Kong crackdown.[42]

Even if Beijing ignored the risks of dumping its dollar-denominated debt, the $1 trillion of Treasurys held by China could be absorbed by the $120 trillion global bond market. Treasurys have lower risk and higher yields than comparable sovereign debt instruments, making them attractive to fixed income buyers, including defined benefit plans, insurance companies, and bond funds. The yield on the U.S. ten-year bond hovered around 1.6 percent as of early-May 2021, characteristically higher than its counterparts in Germany (-0.2 percent), Japan (0.1 percent), and the United Kingdom (0.8 percent). A temporary spike in rates caused by Chinese selling would prompt asset managers to swap their corporate bonds for U.S. government debt with similar yields and durations as a way of de-risking portfolios. If the risk arbitrage trade failed to soak up excess Treasurys, the U.S. Federal Reserve, the European Central Bank, and the Bank of Japan could step in to purchase the remaining securities.

A more likely scenario is that China would strategically default on debt held by American investors. A decade-long credit expansion has left Chinese banks overextended. Rather than restructure non-performing loans at the expense of local banks, Beijing has propped up failing state-owned enterprises with foreign capital amounting to a managed opening of its financial market. The U.S.-China Economic and Security Review

Commission summarized the situation in its 2020 report to Congress:

> *"After years of unbridled lending, China's financial system is facing mounting problems. Local governments have recorded significant revenue shortfalls, banks remain undercapitalized, and an aging population threatens persistent current account deficits. The Chinese government seeks to attract large volumes of new foreign investment to meet these capital shortfalls. These circumstances provide the key context for the entry of foreign capital and expertise into the country's financial system."*[43]

Western asset managers in search of returns have accommodated the staged opening of China's financial market by stepping up their purchases of debt instruments. In late 2019, the Ministry of Finance issued the PRC's first Euro-denominated bonds in fifteen years, attracting €4 billion ($4.5 billion) from institutional investors, such as pension funds and insurance companies.[44] In 2020, U.S. private credit interests began moving into the Chinese market to buy up distressed debt instruments trading at a discount. Due to its total control over capital invested in China, the PRC could strategically default on debt issues disproportionately owned by foreign investors. Even while targeting the United States in this fashion, the PRC could continue holding Treasury securities, confident that Washington would not intentionally default.

A key lesson of the U.S.-China trade war is that the PRC has few economic weapons it can use against the United States without hurting itself. China's export-driven economy relies on the U.S. consumer for demand; its financial system depends on U.S. dollars for liquidity; its state-controlled businesses increasingly need U.S. capital. Shortly after President Trump raised sanctions in 2019, cracks emerged in the Chinese economy, its second quarter growth dropping by half. Within weeks, manufacturers based in China began offshoring operations to countries with better U.S. relations. Throughout the standoff, China's Treasury holdings remained stable, indicating that Beijing does not view debt dumping as a practical tool.[45] This finding should prompt the U.S. Intelligence Community to assess what financial weapons the CCP might consider using in the future.

Show me the Renminbi

Financial warfare requires financial intelligence. The defense intelligence community tracks the PLA's military capabilities around the world, but these efforts alone may not create enough understanding of China's asymmetric expansion strategy. Foreign policy analysts have warned that Chinese expansionism differs dramatically from the Soviet way. Although it has secured military outposts in several countries, the PRC's main approach is to ensnare governments economically and financially, oftentimes by compromising local elites. After flooding a state with strategic investments, loan packages and bribes, political resistance eventually fades away, leaving Beijing with the upper hand on national security matters.

"Debt trap diplomacy" appears central to Beijing's expansionist strategy across the African, Asian, and South American areas where China has become a dominant lender. By overextending credit to financially unstable countries, the PRC positions itself to extract political and economic concessions if repayment becomes difficult. Most of China's loan contracts have confidentiality clauses, but the terms that are observable usually prohibit debt restructuring, even in the event of financial distress.[46] Whether the PRC is consciously structuring loans to influence foreign capitals or simply practicing aggressive underwriting, indebtedness creates a power imbalance in favor of the creditor. Given its past efforts to diplomatically isolate

Taiwan through economic pressure, U.S. defense leaders may reasonably assume that China will pursue its national security interests by exploiting the financial weakness of its borrowers should opportunities arise.

The U.S. Intelligence Community is aware of the PRC's financial intrusions overseas, but there is no centralized effort to map this influence across multiple factors. The Defense Intelligence Agency (DIA) could fill this void by leading an interagency effort to understand the true state of Chinese expansionism. Civilian agencies and contractors are well suited to follow China's financial and business interests overseas. DIA, however, is most incentivized to understand the threat they pose to U.S. regional security commitments.

Africa Command, Central Command, Indo-Pacific Command, and Southern Command have a vested interest in knowing what national and commercial interests the PLA can impact within their respective areas of responsibility. Intelligence on seaports, airports, toll roads, and utilities controlled by the PRC is relevant to the combatant commands. Also salient is intelligence on Chinese state-owned enterprises active in the regions—especially those providing essential service and those involving local elites. Much of this information is obtainable through open source intelligence, but there is a role for other government agencies that can clarify informal business relationships.

Money Mindset

The U.S. government has a range of options to tighten technology and capital controls on China. This article has recommended that the Department of Defense spearhead three initiatives to: (1) promote compliance with export controls by leveraging federal grants and contracts; (2) discourage U.S. investment in certain state-owned enterprises by assuming custody of shareholder voting rights; and (3) develop an intelligence capability that can track Chinese expansionism through business and financial channels as well as traditional military metrics. Some financial warfare concepts may be unfamiliar to a DOD that has relied on other departments to manage the economic power of the United States. The U.S. military, however, is versatile enough to integrate financial warfare operations into its broader strategy for countering the China threat.

The Pentagon should view financial intelligence as a potential force multiplier against the People's Liberation Army rather than a subject "outside its lane." DOD, in fact, has more access to financial expertise than defense leaders may appreciate. The reserve component of the U.S. Armed Forces includes servicemembers with backgrounds in capital markets and international business. DOD contractors include Fortune 100 companies that can analyze the financial battlefield as expertly as any government agency. Agile firms, like Roger Robinson's RWR Advisory Group, are already tracking China's overseas business relationships through open source methods. Networking these resources into a formal structure would enable DIA to develop an early warning system for China's financial warfare activities.

U.S. policymakers for decades have assumed economic dominance when contemplating America's instruments of national power. This luxury of wealth encouraged the Department of Defense to outsource most non-military policy issues. Unfortunately, the federal government has largely failed to protect financial and economic interests central to the DOD mission of national defense. The unpleasant truth is that American-made technology sits at the heart of China's defense modernization program while American capital has fueled the growth of China's state-owned enterprises. Every passing year leaves U.S. servicemembers with a narrower advantage over a People's Liberation Army that sees no daylight between the economic and military objectives of the PRC. Following a military-civil fusion strategy is not an

option for a free-market United States, but neither is allowing China's financial warfare operations to go unchecked. PRISM

Notes

This article contains general discussion of the financial markets provided by All Source Investment Management ("All Source"). The information and opinions are theirs, but the accuracy and completeness cannot be guaranteed. Throughout the article, All Source may generally discuss different investments and historical events regarding the financial markets and various types of investments; however, nothing in the article should be construed as a recommendation to buy or sell any financial vehicle, nor should it be used to make decisions today about your financial situation. Please understand that All Source cannot make any promises or guarantees that you will accomplish such goals. All investments are subject to risk including the potential loss of principal. The purpose of the article is to provide general information on the subjects covered. The author of this article as well as the information presented in the article is not related to, endorsed by, nor connected with and not approved by any government agency or organization. Despite efforts to be accurate and current, this article may contain out-of-date information; the author is under no obligation to advise you of any subsequent changes related to the topics discussed in this article.

[1] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China: Annual Report to Congress," 2002, p. ii.

[2] Karen Kerrigan, "Russia Sanctions Bill Hurts U.S. Small Businesses, Not Vladimir Putin," *Issues & Insights*, March 12, 2020, accessed November 25, 2020, https://www.effectivesanctions.org/category/news/, ; Small Business & Entrepreneurship Council, "Fact Sheet: DASKA targets U.S. companies, not the Kremlin," January 20, 2020, accessed November 25, 2020, https://www.effectivesanctions.org/fact-sheet-daska-targets-u-s-companies-not-the-kremlin/

[3] The White House, "The Chinese Communist Party's Ideology and Global Ambitions," June 26, 2020, https://www.whitehouse.gov/briefings-statements/chinese-communist-partys-ideology-global-ambitions/

[4] BlackRock Institutional Trust Company, N.A. (BlackRock) manages the I Fund as well as the F, C and S Funds.

[5] Bill Gertz, "NSA Details Chinese Cyber Theft of F-35, Military Secrets," *The Washington Free Beacon*, January 22, 2015; Siobhan Gorman, August Cole and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009.

[6] $10 billion estimate is based on recent TSP fund values and a 12% country weighting to Chinese stocks in the MSCI ACWI ex USA IMI Index (USD).

[7] Lingling Wei, Bob Davis and Dawn Lim, "China Has a Friend In Wall Street," *The Wall Street Journal*, December 3, 2020.

[8] Aon Hewitt Investment Consulting, Inc., Report to Federal Retirement Thrift Investment Board, "I Fund Benchmark Study," October 2019, p. 5, accessed November 25, 2020, https://www.frtib.gov/ReadingRoom/InvBMarks/2019_Oct_Benchmark_Evaluation_Report.pdf.

[9] *Ibid*, Aon.

[10] The White House, "Executive Order on Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies," November 12, 2020; Humeyra Pamuk, Alexandra Alper and Idrees Ali, "Trump bans U.S. investments in companies linked to Chinese military," *Reuters*, November 13, 2020.

[11] Audrey Conklin, "Navarro: Trump admin 'tackling Chinese companies that mean to do America harm,'" *FOXBusiness.com*, accessed November 25, 2020, https://www.foxbusiness.com/markets/navarro-trump-chinese-companies

[12] Saleha Mohsin, "U.S. Extends Period for Investors Coping With China Stock Ban," *Bloomberg*, January 27, 2021, accessed April 30, 2021, https://www.msn.com/en-us/money/markets/us-extends-period-for-investors-coping-with-china-stock-ban/ar-BB1d8HkD

[13] Harper Neidig, "Top Pentagon officials say Google work is 'benefiting the Chinese military," *The Hill*, March 14, 2019, accessed November 25, 2020, https://thehill.com/policy/technology/434064-top-pentagon-officials-say-google-work-is-benefiting-the-chinese-military

[14] Suzanne O'Halloran, "Google working with China but not US military is 'peculiar': Peter Thiel," *FOXBusiness.com*, July 15, 2019, accessed November 25, 2020, https://www.foxbusiness.com/technology/google-working-with-china-but-not-us-military-is-peculiar

[15] Jack Poulson, "Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated," *Tech Inquiry*, July 7, 2020, accessed November 25, 2020 https://techinquiry.org/SiliconValley-Military/#conclusions

[16] U.S. Senate Committee on Homeland Security and Government Affairs, Permanent Subcommittee on Investigations, "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans, November 19, 2019, accessed November 25, 2020, https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated.pdf

[17] *Ibid*, U.S. Senate, p. 1.

[18] Mercedes Ruehl, James Kynge and Kiran Stacey, "Chinese state-backed funds invest in US tech despite Washington curbs," *The Financial Times*, December 2, 2020

[19] Wei Sheng, "China's second chip-focused 'Big Fund' raises $29 billion," *technode.com*, October 28, 2019, accessed on December 5, 2020, https://technode.com/2019/10/28/chinas-new-chip-focused-big-fund-raises-rmb-204-billion/

[20] *Ibid*, Ruehl, Kynge and Stacey; Charles Qi, "Black Sesame Technologies: Ensuring Safety in Innovation," *CIOReview.com*, 2019, accessed December 5, 2020, https://automotive.cioreview.com/vendor/2019/black_sesame_technologies

[21] *Ibid*, Sheng.

[22] Cassie Gao, Adam Lysenko, Mark Witzke, Thilo Hanemann, and Daniel H. Rosen, "Two Way Street – US-China Investment Trends – 1H 2020 Update," Rhodium Group Report, September 17, 2020.

[23] Thilo Hanemann, Mikko Huotari and Agatha Kratz, "Chinese FDI in Europe: 2018 trends and impact of new screening policies," *MERICS*, March 6, 2019, accessed November 25, 2020, https://merics.org/en/report/chinese-fdi-europe-2018-trends-and-impact-new-screening-policies

[24] *Ibid*, Hanemann, Huotari and Kratz.

[25] Federal Statistical Office (Germany), "Foreign Trade," November 2020, accessed November 25, 2020, https://www.destatis.de/DE/Themen/Wirtschaft/Aussenhandel/Tabellen/aussenhandel-detaildaten.pdf?__blob=publicationFile

[26] J.P. Morgan Private Bank, "Impact investing," accessed November 11, 2020, https://privatebank.jpmorgan.com/gl/en/services/investing/sustainable-investing/impact-investing

[27] Jacqueline Poh, "Conflicting ESG Ratings Are Confusing Sustainable Investors," *Bloomberg*, December 11, 2019, accessed November 25, 2020, https://www.bloomberg.com/news/articles/2019-12-11/conflicting-esg-ratings-are-confusing-sustainable-investors

[28] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Hudson Institute, Video Event: China's Attempt to Influence U.S. Institutions, July 7, 2020, accessed November 25, 2020, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states

[29] Congressional Research Service, "Debarment and Suspension of Government Contractors: An Overview of the Law Including Recently Enacted and Proposed Amendments," (RL34753), November 19, 2008.

[30] *Ibid*, Wray.

[31] *Ibid*, White House.

[32] Shunlin Song, "Shareholder voting in China: The role of large shareholders and institutional investors," *Corporate Governance*, Volume 28, Issue 1, January 2020, pp. 69-87, accessed November 25, 2020, https://www.onlinelibrary.wiley.com/doi/10.1111/corg.12303

[33] *Ibid*, Wei, Davis and Lim.

[34] Executive Order 13920, "Securing the United States Bulk-Power System," May 1, 2020.

[35] Congressional Research Service, "The International Emergency Economic Powers Act: Origins, Evolution, and Use," (R45618), July 14, 2020.

[36] Shuli Ren, "Treasury Has $541 Billion of Dirty Little Secrets," *Bloomberg*, September 21, 2020, accessed November 25, 2020, https://www.bloomberg.com/opinion/articles/2020-09-21/u-s-keeps-investing-in-china-as-value-investing-dies; Antonio Coppola, Matteo Maggiori, Brent Neiman and Jesse Schreger, "Redrawing the Map of Global Capital Flows: The Role of Cross-Border Financing and Tax Havens," July 2020, accessed November 25, 2020, https://globalcapitalallocation.s3.us-east-2.amazonaws.com/CMNS-Paper.pdf.

[37] *Ibid*, Coppola, Maggiori, Neiman and Schreger, p. 13.

[38] Index Performance Attribution: CHXSOE vs MXCN, 3/31/2015 - 3/31/2021, Bloomberg.

[39] U.S.-China Economic and Security Review Commission, 2020 Report to Congress of the U.S.-China Economic and Security Review Commission, (U.S. Government Printing Office, Washington): 2020, p. 240.

[40] U.S. Department of Treasury, "U.S. Liabilities to Foreigners from Holdings of U.S. Securities," accessed December 5, 2020, https://www.treasury.gov/resource-center/data-chart-center/tic/Pages/shlreports.aspx

[41] Chetan Ahya, Derrick Kam, Nora Wassermann, Julian Richers and Frank Zhao, "Global Debt Factbook," *Morgan Stanley Research*, July 22, 2020.

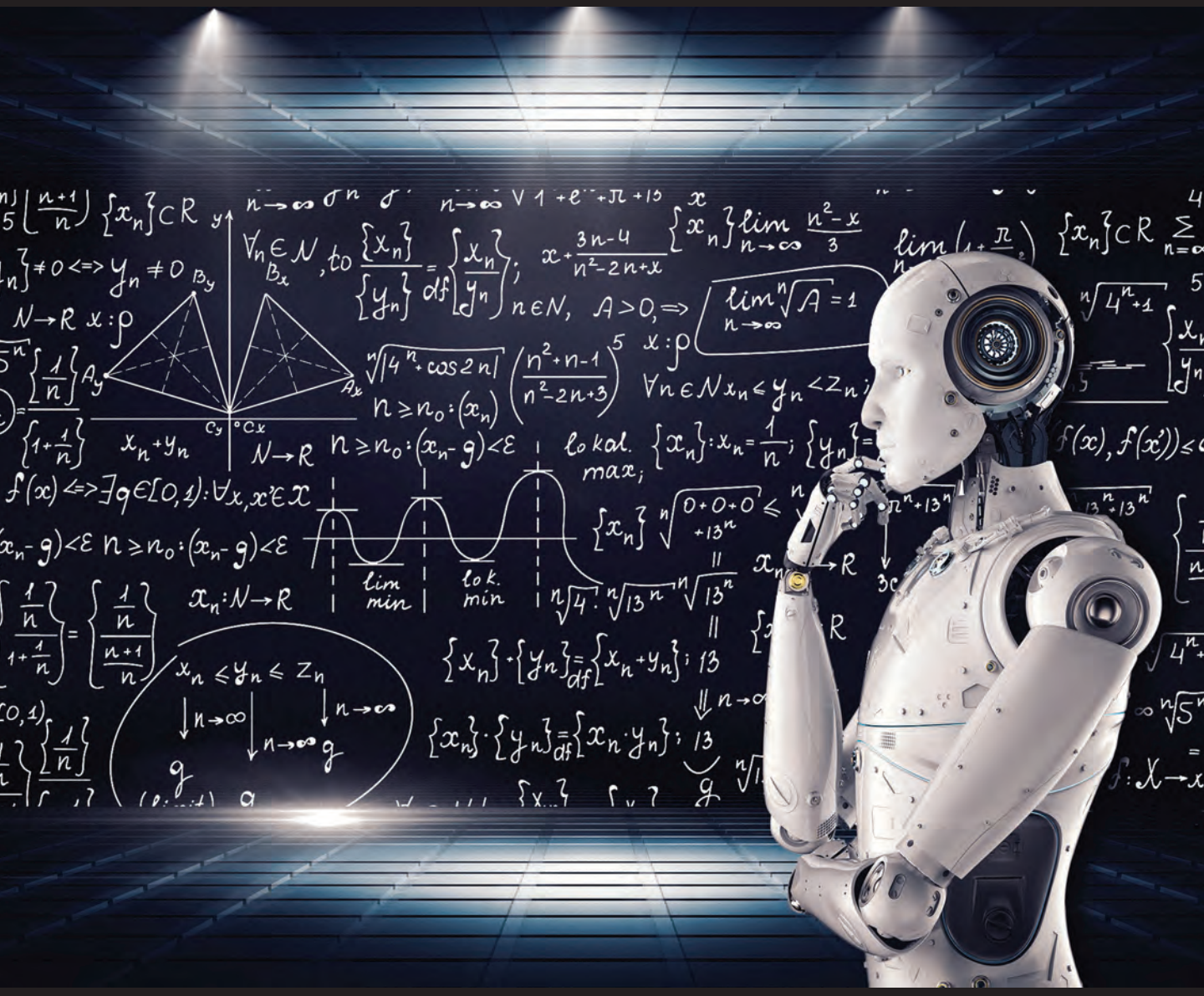
[42] Cheng Leng, Julie Zhu and Engen Tham, "Exclusive: Chinese banks prepare contingency plans over threat of U.S. sanctions, sources say," *Reuters*, July 9, 2020.

[43] *Ibid*, U.S.-China Commission, p. 10.

[44] Frances Yoon, "China Sells First Euro Bonds Since 2004," *The Wall Street Journal*, November 5, 2019.

[45] U.S. Department of Treasury, "Major Foreign Holders of Treasury Securities," October 21, 2020.

[46] Anna Gelpern, Sebastian Horn, Scott Morris, Brad Parks and Christoph Trebesch, How China Lends: A Rare Look into 100 Debt Contracts with Foreign Governments, *Center for Global Development*, March 2021, p. 45.



Artificial Intelligence and Machine Learning are changing future of war.
(mikemacmarketing (www.vpnsrus.com) is licensed with CC BY 2.0.)

AI is Shaping the Future of War

By Amir Husain

Several years ago, before many were talking about artificial intelligence (AI) and its practical applications to the field of battle, retired United States Marine Corps General John Allen, and I began a journey to not only investigate the art of the possible with AI, but also to identify its likely implications on the character and conduct of war. We wrote about how developments in AI could lead to what we referred to as "Hyperwar" — a type of conflict and competition so automated that it would collapse the decision action loop, eventually minimizing human control over most decisions. Since then, my goal has been to encourage the organizational transformation necessary to adopt safer, more explainable AI systems to maintain our competitive edge, now that the technical transformation is at our doorstep.

Through hundreds of interactions with defense professionals, policymakers, national leaders and defense industry executives, General Allen and I have taken this message to our defense community—that a great change is coming and one that might see us lose our pole position. During the course of these exchanges, one fact became increasingly clear; artificial intelligence and the effects it is capable of unleashing have been gravely misunderstood. On one hand, there are simplistic caricatures that go too far; the Terminator running amuck, an instantiation of artificial intelligence as a single computer system with a personality and a self-appointed goal, much like the fictionalized Skynet. Or an intelligent robot so powerful and skilled that it would render us humans useless. On the other hand, there are simplifications of AI as a feature; trivializations in the name of practicality by those who cannot see beyond today and misconstrue AI's holistic potential as the specific capabilities of one or two products they have used, or most likely, merely seen. I would hear from some that fully autonomous systems should (and more amusingly, *could*) be banned and this would somehow take care of the "problem." Others thought the proponents of artificial intelligence had overstated the case and there would never be synthetic intelligence superior to humans in the conduct of war.

But artificial intelligence is not like a nuclear weapon; a great big tangible thing that can be easily detected, monitored or banned. It is a science, much like physics or mathematics. Its applications will lead not merely to incremental enhancements in weapon systems capability but require a fundamental recalculation of

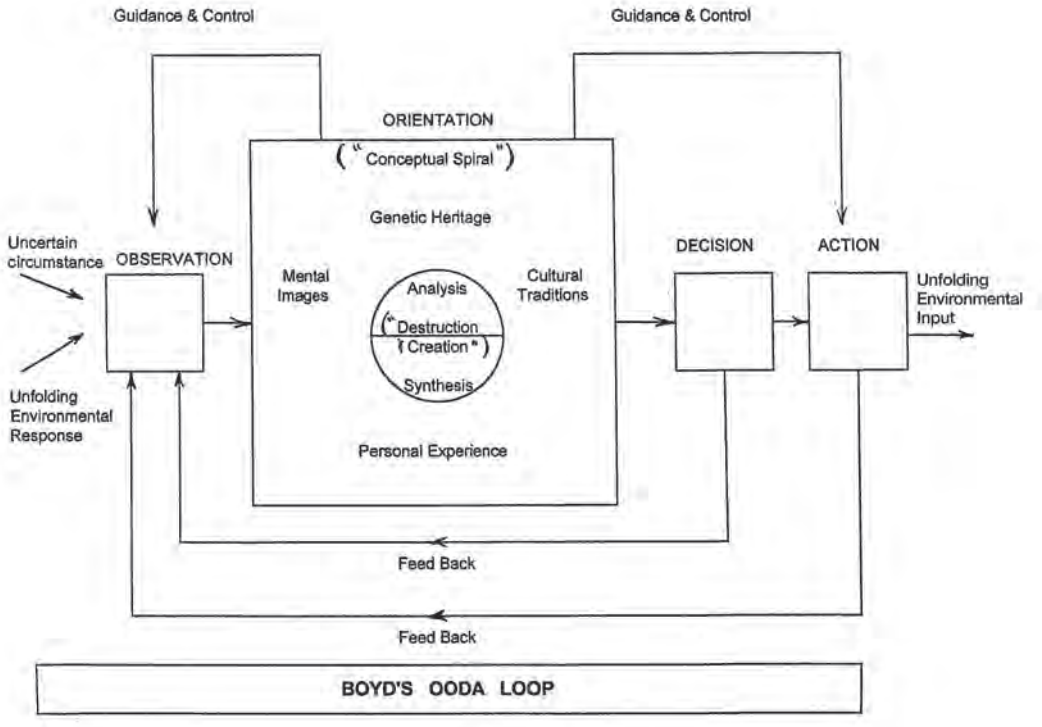
Amir Husain is a serial entrepreneur, inventor, technologist, and author based in Austin, Texas. He is the Founder and CEO of an award-winning artificial intelligence company, SparkCognition, and is the founding CEO of SkyGrid, a Boeing and SparkCognition joint venture.

what constitutes deterrence and military strength. For example, the combination of AI elements—visual recognition, language analysis, the automated extraction of topical hierarchies (or ontologies), control of systems with reinforcement learning, simulation-based prediction, and advanced forms of search—with existing technologies and platforms, can rapidly yield entirely new and unforeseen capabilities. The integration of new AI into an existing platform represents a surprise in its own right. But the complex interactions of such platforms with others like them can create exponential, insurmountable surprise. Which current conventional system deters such an AI creation?

These reactions were all telling. Rather than seeing artificial intelligence as a science, people were reacting to caricatures or linear projections based on the past. Specifically, the contention that since no AI has been built thus far that can exhibit long-term autonomy in battle, such an AI could never be built. Or that if it were, then it would take over the world of its own volition. These reactions would not be as problematic if they were coming from ordinary people playing the role of observers. But seeing people in positions of power and authority—*participants*—espouse such thinking was worrisome. Why? Simply because artificial intelligence will lead to the most important capabilities and technologies yet built by humankind, and a failure to understand the nature of artificial intelligence will cause us to fall behind in terms of taking advantage of all it has to offer in the near, medium, and long term. The stakes are high beyond description.

Hyperwar

Earlier in this piece, I described hyperwar to be a type of automated—potentially autonomous—conflict. But a deeper understanding of concepts



1st diagram incorporating Boyd's corrections, early 1993 (John R. Boyd Collection (COLL/2062) at the Marine Corps History Division, USMC Archives, Flickr.com Images.)

underpinning hyperwar requires exposure to the idea of the Observe-Orient-Decide-Act (OODA) loop; a cyclical process governing action both in the realm of war, and as many have recently pointed out, in commerce,[1] engineering,[2] and other peace-time pursuits.

Where did the idea of the OODA loop come from? While researchers in various fields throughout history have articulated the idea of a cognitive decision/action loop, the modern day conception of the OODA loop in a military context came from USAF Colonel John Boyd. Col. Boyd is famous both for the OODA loop and for his key role in developing the F-16 program. He is also remembered as that famed military strategist whose conceptual and doctrinal contributions, some would argue, quite directly led to the overwhelming U.S. victory in the first Gulf War. Acknowledging the impact of Boyd's work, then-commandant of the Marine Corps., General Charles Krulak said these words in Boyd's eulogy: "John Boyd was an architect of [the Gulf War] victory as surely as if he'd commanded a fighter wing or a maneuver division in the desert. His thinking, his theories, his larger than life influence were there with us in Desert Storm."

Of all Boyd's considerable contributions, perhaps the idea of the OODA loop is the most potent and long-lasting. OODA governs how a combatant directs energy to defeat an opposing force. Each phase of the OODA loop is itself a cycle; small OODA loops curled up within larger ones. As the OODA loop progresses, information processes feed decision processes that filter out irrelevant data and boil outputs down to those that are necessary and of the highest quality. In turn, these outputs become inputs to another mini OODA loop. Seen in this way, the macro OODA loop of war is a massively parallel collection of perception, decision, and action processes; exactly the types of tasks AI is so well suited to, running at a scale at which machines possess an inherent advantage.

AI in Perception, Decision, and Action

Just how good has AI become at these perception, decision, and action tasks? Take perception, an area where machines and the algorithms they host have made great strides over the past few years. AI systems can now beat Stanford radiologists in reading chest X-rays,[3] discern and read human handwriting faster than any human,[4] and detect extrasolar planets at scale, from murky data that would be a challenge for human astronomers to interpret.[5] The AI perception game is hard to beat, and operates at a scale and speed unfathomable to a human being.

The combined effect of millions of sensors deployed in space, in the air, on land, on the surface of the sea and under it, all being routed to a scalable AI perception system will be transformative. We are beginning to see shades of what this will feel like to military commanders. When the Russian military conducted a test of 80 UAVs simultaneously flying over Syrian battlefields[6] with unified visualization, Russian Defense Minister Sergei Shoigu commented that the experience was like a "semi-fantastic film" and that "they saw all the targets, saw the launches and tracked the trajectory." This, of course, is just the beginning.

What about decisionmaking? How would AI fare in that domain? Today, planners use tools such as "Correlation of Forces" (COF) calculators[7] to determine the outcome of a confrontation based on the calculated capability of a blue force versus a red force. They use these calculations and projections to make logistical and strategic decisions. If you divide the battlespace into a grid that constrains both space and time, in some sense the only COF calculation that matters inside each cell is the COF calculation for the cell itself, not for the entire grid. Taking this idea further, given the presence of assets in each cell, one could calculate their area of impact, under the constraint of a time bound. Obviously, a hypersonic missile will have a larger area of impact with a smaller time bound in comparison to a tank. An

AI trying to solve this problem would use sensors to identify assets present in each grid, calculate COF coefficients for each cell for a given time bound, and then seek to generate and optimize a plan of action that results in the smallest own-force maneuvering most efficiently to inflict maximum attrition on the enemy. All while suffering the least damage itself. A proxy for determining how much damage you could inflict while minimizing own-losses is the COF coefficient itself. The larger your advantage over the enemy, the greater the chances of a swift victory. An AI could also play this per-cell "COF" optimization game with itself millions of times to learn better ways of calculating COF coefficients.

This is one simple example of how a strategic hyperwar AI could seek advantage. There are others. The key point is that no human commander could even properly process thousands of fast-changing, per-cell COF calculations, much less act on them with the speed of a purpose-built machine running a rapidly improving algorithm.

Finally, let us come to action. In 2020, the Defense Advanced Research Projects Agency (DARPA) organized a dogfight competition[8] between human F-16 pilots and various AI algorithms, called "AlphaDogfight." The result was a landslide. AI won 5-1. There are many points of view about this competition and questions raised as to whether the rules of engagement were determined fairly. From my own personal experience applying AI to autonomous piloting applications, I know this: AI eventually wins. In 2017, SparkCognition, the AI company I founded, worked to develop technology to identify the conditions for an automated take off rejection. Using reinforcement learning, the AI we developed exceeded human performance both in timeliness of decision-making and accuracy of decisions made. The following year we worked on multi-ship defensive counter air (DCA) scenarios and found that, once again, AI performed amazingly well. In time, AI will win. Is someone making bets to the contrary? And if not, why aren't we moving faster to embrace the inevitable?

The fusion of distributed artificial intelligence with highly autonomous military systems has the potential to usher in a type of lightning-quick conflict that has never been seen before. The essential findings of my work in collaboration with General

"Screenshot of the DARPA AlphaDogfight Trial final round between a Heron Systems AI algorithm and a human pilot using a F-16 simulator" (DARPA)

Allen discussed above revealed that if artificial intelligence was aggressively applied to every element of the OODA loop, in essence, the OODA loop could collapse on itself. Artificially intelligent systems would enable massive concurrent coordination of forces and enable the application of force in optimized ways. As a result, a small, highly mobile force (e.g. drones) under the control of AI could always outmaneuver and outmass a much larger conventional force at critical points. Consequently, the effect of platforms under AI control would be multiplied many fold, ultimately making it impossible for an enemy executing a much slower OODA loop to contend or respond.

What, then, are the larger implications of AI's dominance in perception, decision, and action tasks? What happens when the OODA loop collapses? Let us examine a few implications.

Regional Powers and the "AI-Enabled Skirmish"

Previous work indicates that AI would provide a significant increase in the latitude of action available to both nation states and non-state actors. Smaller scale autonomous operations have an inherent quality of deniability in that there are no humans to capture or interrogate. And it is not just conventional, kinetic actions that AI can control but also cyber operations. The applications of AI to cyber are tremendous and range from automatic development of cyber weapons to the continuous, intelligent scanning of enemy targets to identifying pathways for exploitation, to the autonomous conduct of large scale, distributed cyber operations.

The onset of hyperwar type conflicts will have a great effect on almost all our current military planning and the calculations on which these plans are based. The most potent teeth to tail ratios sustainable by a human force will seem trivial when autonomous systems are widely deployed. The idea that training will always enable dominance will have to be questioned. And the already outdated notion of platform versus platform comparisons will become completely extinct.

Most of the scenarios described in "Hyperwar: Conflict and Competition in the AI Century," have already come to pass. In one conceptual vignette, we outlined how autonomous drones could be used to attack oil installations. Two years later, this actually happened against a Saudi oil facility in Abqaiq. We also highlighted how existing conventional aircraft would be reused as autonomous drones. The Chinese did exactly that with their J-6 and J-7 aircraft. Integrating AI into current systems presents the opportunity to build a potent capability at low cost and create significant complications for planners looking to counter these threats.

When kinetic or cyber effects can be employed over great distances, with great precision and with no human involvement, the likelihood that countries and groups will use these capabilities increases. And when autonomous systems begin to blunt the training-enabled human edge, the potency of such actions is amplified.

The Rest of the World is in on the Secret: the Future is Autonomous

Every day brings with it new announcements in military technology developments. And most of these are not taking place in the United States. Consider just the following recent news from around the world:

1. Russia announced that they deployed 80 drones simultaneously in Syria for ISR (Intelligence, Surveillance and Reconnaissance) coverage and were able to see "everywhere all at once."
2. The Russians have also tested the Mi-28N attack helicopter with a new drone launcher[9] that can be used to deploy ISR systems and intelligent loitering munitions. In January, 2021 Iranian media showed images of a similar system mounted on a helicopter.

3. During the Azerbaijan-Armenia conflict, Turkish TB2 drones were used to devastating effect in contested airspace. Mass deployment of these systems in combination with loitering munitions took out S-300 surface to air missile sites, armor, and infantry. TB2s are being produced at the rate of at least one per week at a cost that is a tenth, possibly a twentieth of U.S. MALE (Medium Altitude Long Endurance) drones.
4. Israeli Harop drones delivered to Azerbaijan are also being used—both kinetically and for propaganda. A recent Azerbaijani martial music video shows a convoy of Harop trucks, each equipped with nine launchers. One can literally see the Azerbaijani military showcase—in a music video, no less—the lethal capability to concurrently deploy a swarm of at least 36 drones.
5. Azerbaijan converted old soviet-era biplanes into DEAD (Destruction of Enemy Air Defense) drones by using them to both identify SAM sites and destroy them via kamikaze attacks.
6. Baykar Makina, the Turkish company that manufactures the Bayraktar TB2, has test flown the Akinci, a drone with a broader mission profile, greater capabilities, and lower cost in comparison to deployed U.S. drones. They have also announced an air-to-air mission capability for the same platform, potentially integrating the Turkish Gokdogan[10] and Bozdogan air to air missiles.
7. The Chinese, in the last few months of 2020, announced and tested two drones; a 100kg payload twin rotor aircraft that can supply troops at high altitude,[11] and a high-speed drone designed for ISR, electronic warfare, and ground strike.
8. Iranian drone production, by all accounts, has ramped up tremendously and a huge range of designs are being produced,[12] including a MALE system. Iran recently demonstrated a combination of small, high speed boats with an autonomous drone, raising the possibility of (UCAV) drones being deployed from (USV) drones.[13]
9. Ukraine has formed a joint venture company with Turkey to manufacture a modified version of the TB2. The initial plan is to produce at least 48 aircraft.[14]
10. The variety and scope of Chinese drone developments is incredibly impressive, and unmanned systems now address every application, from low-end tactical to high-end strategic.

There is also a considerable amount of work going on in Pakistan, India, Israel, South Korea, Brazil, and elsewhere. The list truly goes on and on. In a world where strategic competition between near-peers is once again at the fore, the pace of military innovation is skyrocketing.

While the volume and pace of these developments is impressive, nothing in the list above should be truly surprising. For years, General John Allen, former Deputy Secretary of Defense, Robert O. Work, and others have been pointing to the potential of autonomous technologies, inexpensive sensors, and fast spreading technical knowledge combining to yield potent and inexpensive capabilities.

Cost is a Competitive Advantage

Countries across the globe are leveraging low-cost frameworks for innovation, combining open source software and systems with inexpensive, commercial grade electronics, domestic software prowess and a willingness to experiment and rapidly iterate using methodologies often referred to as "Agile." Not only does this result in lower development costs, it also leads to speed of innovation.

In contrast, in the United States we spend large sums of money on incredibly expensive platforms that work well when they are maintained at great cost, and that perform when they are piloted or controlled by humans in whom we have invested

millions of additional dollars of training time. Is this the best strategy? Or are we doing to ourselves what we did to the Soviet Union in the 1960s and 1970s… encouraging military spending into broader economic oblivion?

Our opponents will increasingly use inexpensive technologies that are easily produced, employable in large quantities, and that continue to deliver results even when they are left to their own devices without any need for a highly trained human operator.

While the United States is the richest nation on earth, too great a disparity in cost-per-capability cannot be sustained even by the world's apex military power. We are walking a dangerous path if we continue to provide lip service to emerging, disruptive technologies while making the real, significant investments in legacy platforms. It is not enough to talk about technological disruption, we must actually disrupt our funding and spending patterns.

Let us apply the cost-per-capability lens to just a few of our high-end platforms that have traditionally been force multipliers and differentiators for our forces. U.S. attack helicopters are the most potent in the world. But recent export orders show that they now cost between $100-125 million per aircraft.[15] While capabilities vary based on platform, in general, these helicopters carry anywhere between 8 and 16 anti-tank guided missiles (ATGMs), enjoy a loiter time of about 2.5 hours, and carry two pilots on board. In contrast, the Bayraktar TB2 currently being used in Libya and Nagorno-Karabakh has a loiter time of 24 hours, carries 2 ATGMs, requires zero on-board pilots, and costs about $2M[16]. It's quite apparent that armor is vulnerable to these drones, much as it is to attack helicopters. But have we considered how these drones can be employed in swarms as an alternative to the expensive attack helicopter? How many TB2s can be delivered via a single transport aircraft? How many conventional attack helicopters? How much training is required for on-board pilots versus for an autonomous system complemented by a remote operator? A new, distributed lethality alternative to attack helicopters has advantages beyond the obvious lower cost.

It might be tempting to look at tactical drones and dismiss them as relatively simple systems that were bound to proliferate. Of course, I agree with both those points; many are simple systems and they have indeed proliferated. However, the drones now being developed in a number of countries are not necessarily just tactical or low-end. Complex high-end capabilities are proliferating, too. AI is being applied to other complementary areas, such as jamming, to create cognitive EW (Electronic Warfare) pods that can be flown into action by a UAV.

And it is not just about the drones alone, but rather the fact that their employment in real theatres of conflict also entails a significant shift in the entire concept of operations. For example, it has been theorized that TB2 drones over Azerbaijan were controlled from Turkey, with larger Akinci drones acting as relays. ATGMs delivered at scale, against a peer-force by attritable, long-endurance platforms controlled by pilots hundreds of miles away… never before was this concept of operations employed. But even newer methods of employment are coming.

Turkish Aerospace and Bayraktar are collaborating with Aselsan to incorporate the Koral EW system onto their drones. Russia's Uran-9 UGVs have been improved after their performance in Syria was studied and gaps were identified. Chinese UAV developments are progressing at such a significant rate that it is difficult to capture them in a work that falls short of book-length. Sensors, control systems, vehicles, and conops are all evolving fast on the global scene and this means complex, multi-system threats employed in surprising ways.

Michael Peck, writing in National Interest suggests that "Turkey may have won the laser weapons race" when it deployed a laser weapon system in Libya that was able to shoot down a Chinese Wing Loong drone. He goes on to quote Alexander

Timokhin of Army Recognition; "the interesting thing in this whole story is how essentially newcomers to the laser theme occupy that niche in which the 'grandees' of laser business, such as Russia and the USA, do not even think to climb." Indeed, space that is ceded will be occupied. Technological gaps between several leading nations of the world are no longer so insurmountable so as to allow complacency. And cost matters! How is it that Turkey, with a $22 billion defense budget, is able to drive so much innovation in air-to-air missiles, lasers, EW, drones, and many other areas, whereas our dollars do not quite seem to go as far in the United States.

Cost is a critical feature, too! Big, expensive, slow-to-evolve, slow-to-build and complex to maintain platforms need to be re-thought in an age where software is the most lethal weapon. One that is growing exponentially in capability over months, not years. You can not bend new metal fast enough to keep up. It is the relationship between the software and the metal that truly matters. In this context, how does the $35 billion carrier strike group evolve in the age of inexpensive DF-21D missiles and next-generation AI-powered cruise missiles? What about the tank? General Tony "T2" Thomas, the former commander of the United States Special Operations Command (USSOCOM), recently discussed this point with me and wondered whether Nagorno-Karabakh pointed us to the end of the tank-as-platform. General Thomas has also publicly tweeted his views on this topic; "The real debate is the role of massed armor in future warfare (there is a reason the Marines just gave up their tanks)."

There are signs of progress and improvement. Certainly, the United States has not been sitting entirely still. The Air Force's announcement of the first test of a sixth generation platform is encouraging, in particular because it was developed so quickly. Also encouraging are the three Boeing, General Atomics, and Kratos "SkyBorg" prototype development efforts for loyal wingmen drones. But given history, one wonders how expensive new systems will be by the time they are deployed. Will future programs be able to avoid the types of issues that the F-35 program encountered? A $120 million, fifth-generation stealth platform for use against near-peer threats, but only used in anger with non-stealthy, externally mounted munitions to conduct missions in uncontested airspace. Are these missions not better suited to a 40-year old F-16 or A-10? Consider further the case of our B1s, which are exquisitely complex aircraft designed for low-altitude, high-speed penetration of highly defended airspace. To find some use, they were eventually used to drop conventional bombs in Afghanistan. Mundane, low-end work for a high-end platform.

It is high time we got over the platform and focused on the mission. If we keep buying $120 million jets with $44,000/hr flight costs to use them on missions better suited to $2 million drones that could cost us $2,000/hr, we will eventually find that financial oblivion we seem to be looking for. We do not need all high-end, all the time. And there are more imaginative ways of employing our existing high-end platforms than as frontline bomb trucks.

AI for Sense-Making, Cyber, and Space

While AI will play a huge role in augmenting conventional platforms, it will also play four additional roles. First, it has the potential to automate planning and strategy. Second, it can revolutionize sensor technology by fusing and interpreting signals more efficiently than ever before. Third, it has a massive role to play in space based systems; particularly around information fusion to counter hypersonics. Fourth, it can enable next generation cyber and information warfare capabilities.

Imagine an ocean in which submarines cannot hide effectively, negating one leg of the triad. Imagine middle powers fielding far more competent forces because while they lack the resources to train human pilots to the level of the United States

Air Force, they are capable of the design expertise required to field AI-powered platforms. Imagine cyber attacks engineered by AI and executed by AI at scale. Imagine long-running, fully automated information warfare and espionage programs run by AI systems. If AI is applied creatively in nation state competitions, it has the potential to create significant, lasting impact and deliver a game-changing edge.

Software: The Ultimate Weapon

Software, AI, autonomy—these are the ultimate weapons. These technologies are the difference between hundreds of old Mig-19 and Mig-21 fighter jets lying in scrap yards, and their transformation into autonomous, maneuverable, and so-called "attritable," or expendable, supersonic drones built from abundant air frames, equipped with swarm coordination and the ability to operate in contested airspaces. Gone are the days when effectiveness and capability could be ascribed to individual systems and platforms. Now, it's all about the network of assets, how they communicate, how they decide to act, and how efficiently they counter the system that is working in opposition to them. An individual aircraft carrier or a squadron of strategic bombers are no longer as independently meaningful as they once were.

In the emerging environment, network-connected, cognitive systems of war will engage each other. They will be made up principally of software, but also of legacy weapons platforms, humans, and newer assets capable of autonomous decision and action. The picture of the environment in which they operate across time and space will only be made clear by intelligent systems capable of fusing massive amounts of data and automatically interpreting them to identify and simulate forward the complex web of probabilities that result. Which actions are likely to be successful? With what degree of confidence? What are the adversary's most likely counter-moves? The large scale, joint application of autonomously coordinated assets by a cognitive

"Software Data analysis for an integrated computer system" (Ilya Pavlov, Unsplash Photos)

system will be unlike anything that has come before. It is this fast-evolving new paradigm, powered by artificial intelligence at every level, from the tactical to the strategic, that demands our attention. We must no longer focus on individual platforms or stand-alone assets, but on the cognitive system that runs an autonomous "Internet of War."

Integrating the "LEGO bricks" of intelligence and autonomy into conventional platforms results in unconventional upgrades. A Chinese-built Shenyang J-6 Farmer fighter jet with autonomy is not just a 1950s era write-off. It becomes a system with new potential, diminished logistics dependencies, and an enhanced efficacy that goes far beyond an engine or radar upgrade. Broadly, the consequences of the use of AI to revitalize and reinvent conventional platforms will be hard to ignore.

Preparing for an Autonomous, Software-Fueled Future

Despite the change occurring globally in value shifting from the physical to the digital, and the tremendous latent potential of AI, the U.S. Department of Defense has not traditionally been at its best when it comes to understanding, acquiring, or deploying software capabilities. Hardware platforms come far more naturally to our acquisition professionals. We can hope for a change of heart and perspective, but absent that, in order for AI to be meaningful to them in the near term, we must reinvent, enhance, and reimagine existing platforms just as we build new ones. It is only then that we will cost-effectively fulfill needs and create significant new capabilities that open the door to even greater future potential. Briefing after briefing on the potential of AI, or distributing primers on machine learning inside the confines of the Pentagon will not lead to critical adoption; the performance gains that result when AI is integrated into platforms will be the proverbial proof that lies in the eating of the pudding.

We have made the mistake of being too slow to adapt, and not predicting the next conflict well enough to be prepared. Perhaps some of our allies have made the same mistake. In fact, a report from the European Council on Foreign Relations (ECFR) concluded that "the advanced European militaries would perform badly against Azerbaijan's current UAS-led strategy."[17] The truth is that we have developed an inflated opinion of the quality of our readiness because over the past 40 years we have not had to face opponents that were able to turn our omissions into unforgivable sins. The future may not be so kind.

To compete in this new era of exponential technologies, the U.S. military and our intelligence agencies need to go all-in on digital and physical systems powered by artificial intelligence. Imbued with synthetic cognition, such systems can make a meaningful difference to every branch of our armed services and our government organizations. A serious effort to fuel the development of such systems will lay the groundwork for true, full-spectrum AI adoption across government. But for any of this to become reality, long held views and processes in the Defense Department must change. In order to turn the tide, at a minimum, we need to:

1. Take a "let a thousand flowers bloom" approach with ideation and experimentation. Financially incentivize startups to contribute to innovation and encourage them to rethink platforms (Note: $50,000 is not an incentive especially in the context of the massive hurdles companies need to overcome to be a government supplier). Red tape—from clearances to past performance requirements—often makes it impossible for young companies to participate and should be re-thought. The focus should be on delivering capability, not how the capability is delivered.
2. Use existing platform upgrade opportunities to source autonomy and AI technology—particularly from younger, innovative companies—and

incorporate it into systems that already exist. Rather than transforming platform upgrades into a vendor annuity, DOD can use upgradation roadmaps to accelerate a broad based AI transformation and build subsystems that will find use across many areas.

3. Connect successful experiments with "end users" in our services early and quickly, capturing feedback and allowing rapid iteration.
4. Make fast funding mechanisms available directly to smaller, innovative companies to convert successful experiments to deployable systems. We must reduce bureaucratic burdens on smaller companies so that they can directly deliver to government customers. Presently, many smaller companies have no choice but to deliver their capabilities through a handful of primes. This can be both monetarily inefficient and unhealthy for the growth of the defense ecosystem.

If we are to remain competitive, an aggressive, fast-track effort to incorporate AI into existing and new platforms must be adopted. In the age of hyperwar, our willingness to embrace commercial innovation, our decisiveness in acknowledging that we live in a post-platform era, and most importantly, the speed with which we operationalize new investments, will be the attributes that lead to victory. PRISM

Notes

[1] What Do AI And Fighter Pilots Have To Do With E-Commerce? Sentient's Antoine Blondeau Explains | GE News.

[2] How Great Engineering Managers Identify and Respond to Challenges – the OODA Loop Model - Waydev.

[3] https://hitconsultant.net/2019/08/22/ai-tech-beats-radiologists-in-stanford-chest-x-ray-diagnostic-competition/.

[4] https://www.labroots.com/trending/technology/8347/ai-reads-handwriting.

[5] https://news.sky.com/story/ai-algorithm-identifies-50-new-planets-from-old-nasa-data-12057528.

[6] http://newsreadonline.com/russia-in-syria-simultaneously-launched-up-to-80-drones/.

[7] Demystifying the Correlation of Forces Calculator (army.mil).

[8] AlphaDogfight Trials Go Virtual for Final Event (darpa.mil).

[9] Russia bets big on Mini Drones for Attack Helicopter, Combat Troops (defenseworld.net).

[10] Military Watch Magazine.

[11] China's Autoflight puts a canard twist on its latest long-range eVTOL (newatlas.com).

[12] Iran showcases Shahed 181 and 191 drones during "Great Prophet 14" Exercise - The Aviationist.

[13] Iranian press review: Revolutionary Guard equips speed boats with suicide drones | Middle East Eye.

[14] Ukraine Forming Venture with Turkey to Produce 48 Bayraktar TB2 Drones (thedefensepost.com).

[15] Apache attack helicopters and weapons: $930 million price tag is unreal (nationalheraldindia.com).

[16] UK eyes cheaper armed drones after Turkey's successful UAV program | IRIA News (ir-ia.com).

[17] Air Forces Monthly, January 2021.

Gray zone aggression is an attractive option for Western rivals because it exploits the openness of Western societies. (American Society for International Law; Hybrid Warfare: Aggression and Coercion in the Gray Zone, November 29, 2017)

Countering Aggression in the Gray Zone

By Elisabeth Braw

In recent years, much has been written and said about conflict in the so-called "gray zone," often described as conflict below the threshold of combat. Gray zone aggression is an attractive option for Western rivals because it exploits the openness of Western societies. The fact that Western countries are characterized by small governments with limited powers to dictate the activities of their populations and businesses makes these countries even more attractive targets for nonkinetic aggression, ranging from hostile business activities, to cyber attacks, to kidnappings, assassinations, and even occupation by unofficial militias aligned with foreign powers. Resourceful adversaries use such actions to force wedges into the fault lines of open societies. With innovative thinking, however, liberal democracies can develop effective gray zone deterrence while staying within the norms of behavior they have set for themselves.

The Case of Sergey Skripal

On March 4, 2018, former Russian intelligence officer Sergey Skripal and his daughter Yulia were found in "an extremely serious condition" on a park bench in the English cathedral town of Salisbury.[1] The UK government's first task was to determine precisely what had happened to the Skripals and who was responsible. On March 12, then-Prime Minister Theresa May informed the UK Parliament of the findings of the government's investigation: "It is now clear that Mr. Skripal and his daughter were poisoned with a military-grade nerve agent of a type developed by Russia. . . . The Government has concluded that it is highly likely that Russia was responsible for the act against Sergei and Yulia Skripal." She continued ominously, "Mr Speaker, there are therefore only two plausible explanations for what happened in Salisbury on the 4th of March. Either this was a direct act by the Russian state against our country, or the Russian government lost control of this potentially catastrophically damaging nerve agent and allowed it to get into the hands of others."[2]

Although the attack was primarily a Russian assassination attempt against the traitor Skripal, it was also a chemical weapon-aided attack on the United Kingdom; when state-sponsored assassinations occur—when they are not deterred—they can dangerously weaken the stability of the countries in which they are carried out. While true with respect to assassinations, this also holds for other forms of gray zone aggression. With

Elisabeth Braw is a Resident Fellow at the American Enterprise Institute, where she focuses on defense against emerging national security challenges, such as hybrid and gray zone threats.

Interview taking place near the Maltings Police forensics tent following the attempted assassination. (Peter Curbishley, March 7, 2018)

such below-the-threshold aggression, the targeted country faces an awkward predicament: how to respond forcefully without violating the ethical standards liberal democracies have set for themselves, and more importantly, how to communicate deterrence to prevent such attacks?

Deterring Gray Zone Aggression

The primary reason gray zone aggression is an attractive option for countries seeking to increase their power at Western expense is that the West's traditional deterrence policy—based on conventional military strength and ultimately backed by nuclear weapons—has been successful in deterring traditional military aggression. Deterrence always poses a basic challenge: its effectiveness is virtually impossible to measure or prove. An absence of aggression is not a confirmation that deterrence has been successful; it may simply mean the adversary was never planning to attack in the first place. Nevertheless, nation-states have long known that they need to signal to potential attackers and the wider world that military attacks will not be tolerated and will not be successful. Some countries have projected more forceful deterrence through the course of the Westphalian world order, some less so, but all know that signaling weakness is in no country's interest.

In addition, as Hathaway and Shapiro and others such as the Uppsala Conflict Data Program have shown, armed conflict has lost significant lure among industrialized nations.[3] In this context, Russia's intervention in Crimea and Eastern Ukraine is an aberration. Geopolitical competition has, however, not vanished. The decline of inter-state war makes

gray zone aggression a convenient tool and alternative strategy for advancing standing and weakening opponents in the competitive global arena. Gray zone aggression bedevils the targeted country not just because it primarily targets civil society but because it is hard to identify, to attribute to a specific sovereign perpetrator, or both. Cyber attacks are notoriously difficult to trace to a sponsoring government, partly because no digital trail may link the perpetrators to their sponsors. Alternative forms of land acquisition as practiced by China through the gradual construction of islands in disputed South China Sea waters defy any obvious retaliatory response as no individual Chinese step seems sufficiently significant to warrant retaliation or even explicit deterrence signaling. Hostile business acquisitions by foreign entities may seem like cutthroat business as usual until a country has lost a significant number of key firms to a rival country. Crucially, because it is so difficult to establish suitable defense and response, establishing credible deterrence is a vexing challenge. What punishment or denial to signal when the nature of a prospective or even an executed attack is not even clear?

The UK government's response to the attempted assassination of the Skripals was innovative. The government quickly assembled a coalition of allies, all of which expelled Russian intelligence officers working under diplomatic cover. The United States not only expelled 60 Russians working under diplomatic cover but also ordered Russia to close its consulate in San Francisco.[4] A total of 28 countries expelled 153 Russian intelligence officers. This was not without cost to UK allies—Russia retaliated by expelling 189 individuals working in Russia on diplomatic passports.[5] The UK government also launched a communications offensive, which in combination with the muckraking efforts of investigative journalists, resulted in the two Russian perpetrators quickly being identified along with Russia's GRU military intelligence agency and shamed for their incompetence.[6]

In October 2020, soon after retiring from government service, Mark Sedwill—the UK government's national security advisor at the time of the Skripal attack—revealed that the government had struck back in other ways as well. "We also took a series of other discreet measures," Sedwill told the British newspaper *The Times*.[7] Sedwill declined to identify the discrete measures, explaining only that "we will use different techniques. We need to play to our strengths and focus our attention on their vulnerabilities. We are not going to conduct illegal operations, but there are things we can do. There are some vulnerabilities that we can exploit too." Those vulnerabilities, he said, include "tackling some of the illicit money flows out of Russia, and covert measures as well."

"Play to our strengths and focus our attention on their vulnerabilities" is a promising approach to deterrence in the gray zone. In the case of the Skripal attack, the UK actions were retaliatory, coming as they did after the attack. Successful deterrence would have signaled that such punishment would be metered out on any country attempting gray zone aggression on UK soil. UK deterrence signaling in the gray zone prior to the attack was, in fact, indisputably insufficient. The country had suffered a litany of previous gray zone aggressions including cyber attacks and even the previous successful assassination of Russian former spy Alexander Litvinenko, which also featured a toxin.

Indeed, as demonstrated by the Skripal attack, continuing cyber attacks by the governments of China, Russia, Iran, North Korea, and their proxies; coercive Chinese diplomacy; and subversive business practices, gray zone aggression persists because it is not deterred—perpetrators have been confident they can get away with impunity. Their confidence is based on the vexing difficulty of designing effective gray zone deterrence. Unlike deterring the armed forces of rival states, where countries seek to match or counter each other's military capabilities, the diversity and unpredictability of gray zone aggression leaves

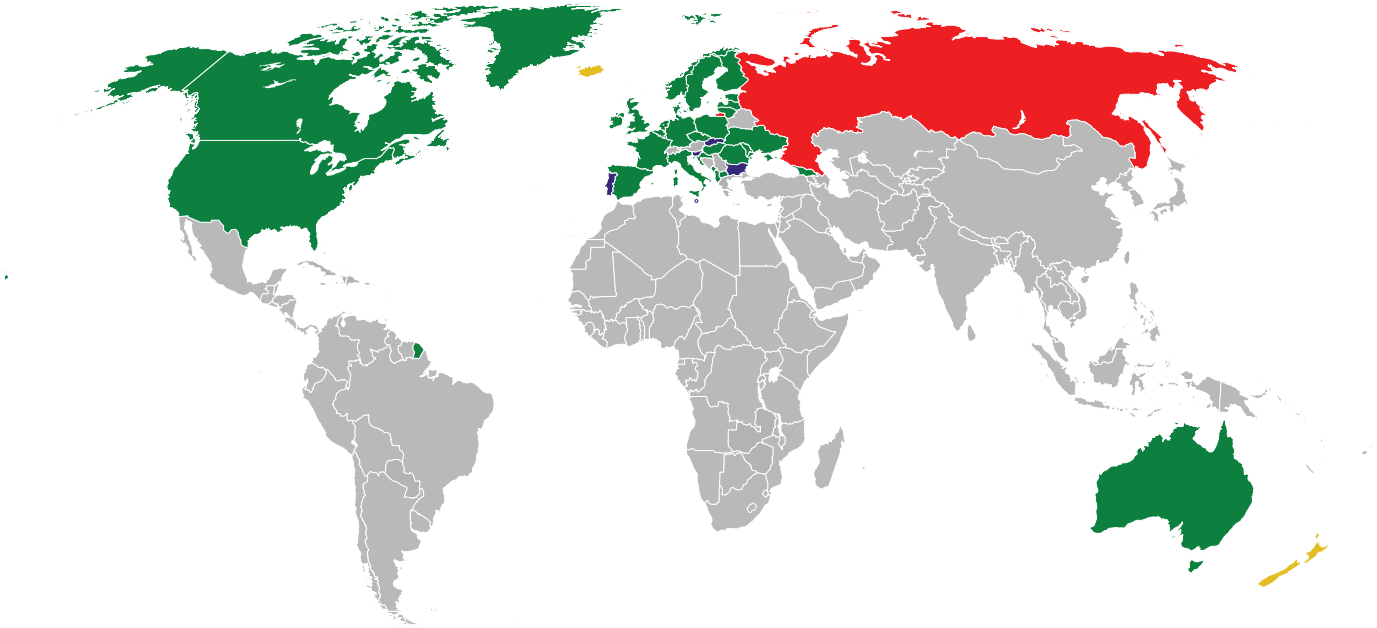
the defender one step behind. Indeed, part of the beauty of gray zone aggression is its surprise element, not only in timing but also in its methods.

The challenge presented by the diversity of methods is not only in trying to predict them but also the fact that liberal democracies are often not able to retaliate using the same methods. It would, for example, not behoove a Western country to signal that a chemical weapon-powered assassination attempt on its soil will be avenged with a corresponding assassination attempt on the adversary's soil, or that concerted use of intellectual property theft will be avenged in kind. Because the West's rivals know the ethical standards Western governments set for themselves, and that any deviation from these standards might be severely criticized by opposition parties, civil society watchdogs, and voters, deterrence that does not adhere to such standards would not be credible.

Like traditional deterrence, deterrence signaling in the gray zone must be credible. Signaling kinetic punishment for an act of gray zone aggression would be disproportionate and escalatory and thus not credible. To date, the only kinetic response to gray zone aggression has been Israel's 2019 bombing of a Hamas building in Gaza in response to a cyber attack.[8] As a result, NATO's long-serving deterrence tools, including the U.S. nuclear umbrella, are of minimal use for deterrence in the gray zone. Somewhat surprisingly, the UK government states in its Integrated Review—published in March 2021—that the UK will, in practice, seek to deter new technological threats with its nuclear arsenal. "The UK will not use, or threaten to use, nuclear weapons against any non-nuclear weapon state party to the Treaty on the Non-Proliferation of Nuclear Weapons 1968 (NPT). This assurance does not apply to any state in material breach of those non-proliferation obligations. However, we reserve the right to review this assurance if the future threat of weapons of mass destruction, such as chemical and biological capabilities, or emerging technologies that could have a comparable impact, makes it necessary." Adversaries may take this to understand that the UK will avenge devastating cyber attacks with nuclear strikes. The question is whether the adversaries will regard the threat as credible.[9]

Nevertheless, the UK government's cumulative response to the Skripal attack holds important lessons. It has almost become an article of faith that liberal democracies are powerless to deter gray zone aggression because the attacks target their vulnerable civil societies, and because they cannot avenge most attacks in kind, and thus lack punishment tools with which to deter such aggressive behavior. Russia's interference in the 2016 U.S. elections is a good case in point. The Russian disinformation campaign left many Americans convinced that their government could not protect itself against election meddling by hostile states. A September 2020 poll by the University of Chicago found that 69 percent of Americans believed Russia tried to influence the 2016 vote, while only 29 percent believed Russia did not. Fully 74 percent were concerned that foreign governments would try to tamper with voting systems or election results, and 74 percent were also concerned that foreign governments would try to influence what Americans think of their political candidates.[10]

During the 2020 U.S. election campaign, there was considerable concern that Russia would replicate its interference efforts of the 2016 election campaign. In the end, Russia's interference in the 2020 election was markedly below the level of 2016. This suggests that targeted countries are, in fact, capable of deterring gray zone aggression through resilience, punishment, or both. In the case of the 2020 U.S. elections, successful deterrence can credibly be attributed to DOD's Defend Forward offensive strategy, CISA's defense of the election infrastructure, and Americans now being on their guard against disinformation.[11] Similarly, while the UK's open borders and freedom of movement make



Poisoning of Sergei and Yulia Skripal – Countries in green expelled Russian diplomats. (Map created by Mykola Vasylechko, March 27, 2018)

it easy to attempt a government-sponsored assassination, the UK government's swift and innovative response to the Skripal attack imposed a significant cost to Russia, and thus is likely to deter similar aggression in the near future.

Liberal Democracies Fight Back

What can we learn from these recent possible examples of success? How can liberal, democratic states persuasively signal that gray zone attacks will be resisted and avenged? Western governments need to rethink deterrence. Or rather, they need to remember how successful deterrence works. The sum of deterrence by denial and by punishment aims to, in the words of Dr. Strangelove, instill in the enemy the fear to attack. It is primarily about changing an adversary's cost-benefit calculation through psychology, not specific tools. Indeed, because gray zone deterrence may require a different toolbox than that used by the adversary, the psychological factor is even more important than is the case with deterrence of traditional armed attacks. As demonstrated by the UK government's response to the Skripal incident, the West has options that are both legal and ethical. And because gray zone aggression targets civil society, societal resilience presents an enormous potential, not only as defense but also as a deterrent.

First, governments should signal that while they may not be able to prevent every attack, widespread and well-organized societal resilience means a gray zone attack will have limited impact. Such deterrence by denial was a pillar of Sweden's deterrence posture during the Cold War. While Sweden had large armed forces, with a mobilized strength of some one million, military power alone was plainly insufficient to deter the Soviet Union. Instead, deterrence relied heavily on the civil defense arm, which involved no fewer than 2.2 million Swedes,[12] who in case of an attack would maintain vital societal functions and support the armed forces, thus denying an attacker a swift victory and changing the attacker's cost-benefit calculation. Deterrence by denial—as exemplified by

the societal resilience just described—is by definition reactive. As such, it is an insufficient deterrent in and of itself. It is, however, a vital twin to deterrence by punishment as it demonstrates that even successful attacks will have relatively limited effect and will present to a prospective aggressor an unattractive cost-benefit calculation.

Second, specific retaliatory measures in the context of deterrence by punishment need not be identified in deterrence messaging. In what the author calls the "horse's-head-in-the-bed strategy," a targeted country only needs to communicate to the country sponsoring gray zone aggression that it will retaliate and impose an unacceptable cost. Deterrence by punishment should signal both to known gray zone actors such as Russia and China as well as to other countries that gray zone aggression will be avenged, and that the aggrieved state will choose the time, manner, and target to maximize effect.

Third, governments must establish who should be deterred. This is a critical departure from centuries of deterrence, where the only recipient of deterrence messaging was a rival government. Today, in the many cases where no government declares itself the perpetrator or sponsor of gray zone activities, addressing deterrence to a presumed sponsoring government is ineffective. As a result, Western governments should build targeted deterrence messaging directed at governments, government-linked companies, and individuals, respectively.

There should, in other words, be no ambiguity regarding the intention to respond to gray zone aggression and that this response will range from societal resilience to punishment of the attacker.

Putin's Palace, near the village of Praskoveevka in Krasnodar Krai, Russia. (Экологическая Вахта по Северному Кавказу, Дмитрий Шевченко, February 11, 2011)

There should, however, be ambiguity as to how the attacker will be punished, when it will be punished, and indeed which individuals or individual companies will be punished. This ambiguity is perhaps the most useful tool that Western countries can use in deterrence of gray zone aggression. It is highly beneficial for three reasons:

1. It does not lock the targeted country into responding with the same means as those used by the aggressor. This is important as the means used by the aggressor may fall outside liberal democracies' ethical norms.
2. It does not lock the targeted country into immediately responding to an attack. This is particularly beneficial as the perpetrator of a gray zone attack—whether a state or non-statal entity—can often not be immediately identified.
3. It leaves the targeted country the liberty to choose whether, when, and how to retaliate. This uncertainty itself—not knowing whether the targeted country will avenge the attack, and if it does, with which allies, and in which manner—in fact increases deterrence.

This leads to the question of which kinds of punishments liberal democracies can signal to the various targets of their deterrence. Sedwill's observation that "we need to play to our strengths and focus our attention on their vulnerabilities. We are not going to conduct illegal operations, but there are things we can do. There are some vulnerabilities that we can exploit too," is crucial. During the 2020 U.S. election campaign, presidential candidate Joe Biden referred to these vulnerabilities when he explained how he would seek to counter election interference: "I will direct the U.S. Intelligence Community to report publicly and in a timely manner on any efforts by foreign governments that have interfered, or attempted to interfere, with U.S. elections. I will direct my administration to leverage all appropriate instruments of national power and make full use of my executive authority to impose substantial and lasting costs on state perpetrators," he wrote, adding that the punishment could include "financial-sector sanctions, asset freezes, cyber responses, and the exposure of corruption."[13]

While sanctions are a much-used but not particularly effective punishment, the exposure of corruption suggests an agile approach badly needed in gray zone deterrence, and not just with regard to election meddling. Russian opposition activist Alexey Navalny's early 2021 exposé of a magnificent palace, apparently built by President Vladimir Putin through dubious means, appeared to rattle Putin more than any other allegations against him.[14] Let us not forget the resignation of Iceland's Prime Minister Sigmundur Davio Gunnlaugsson in 2016 following the release of the Panama Papers which implicated him in corrupt activities. Such exposure is clearly viewed as very threatening to corrupt leaders.

Another Russian vulnerability, shared by China and Iran, is systematic discrimination against minorities. At the time of writing, China appears to have decided that sending Uighurs to "reeducation camps" and thereby earning the opprobrium of the West is preferable to allowing the spread of Uighur separatism. Separatism is, in other words, a key concern for Beijing. Although the plight of persecuted minorities should emphatically not be leveraged in Great Power politics, Western governments could, for example, signal the possibility of intrusive examination and reporting of China's domestic conflicts and tensions. While interference in the internal affairs of other countries is decidedly a contravention of Westphalian norms and can violate international law, doing so on behalf of minorities subject to discrimination and internal to a country against their popular will is less self-evident.

Western countries also have assets their adversaries lack, and which they can employ in deterrence. The most important of these is the desirability of their countries as destinations for

visits, investment, education, or even residence. People from every country in the world want to visit or even live in the West. In countries with autocratic regimes, such as Russia and China, people with money, connections, high positions, or a combination thereof visit the West for private purposes. In many cases, their families visit Western countries with great frequency; indeed, children of such officials and businessmen often attend schools and universities in the West and stay on to work after graduation. Even after the United States and the EU imposed sanctions on, among others, Deputy Duma Speaker Sergei Zheleznyak after Russia's annexation of Crimea, his daughter Anastasia continued working as a production assistant at the BBC's prestigious Ellstree Studios. Anastasia is a graduate of Queen Mary University in London and the American School in Switzerland (TASIS), a boarding school for the moneyed global elite. North Korean ruler Kim Jong-Un also attended a Swiss boarding school.[15] Many children of top Chinese officials attend top U.S. universities, including the daughter of current Chinese leader Xi Jinping, who graduated from Harvard University in 2014. Typically, the children use assumed names.[16]

Officials and well-connected businessmen from countries hostile to the West often own property in the very countries they denigrate and sabotage. The UK Parliament's Intelligence and Security Committee noted in its Russia report—released in July 2020—that the UK has welcomed Russian money, with few questions asked about its provenance. In so doing, the Committee said that the UK "offered ideal mechanisms by which illicit finance could be recycled through what has been referred to as the London 'laundromat'. . . . Russian influence in the UK is 'the new normal'."[17] It is, however, not known to the wider public which officials from hostile countries own which properties or bank accounts in countries such as the UK. With the permission of the Western schools, universities, and employers of family members, as well as banks and property developers, Western governments can signal to perpetrators that they will reveal such facts to both their own domestic publics as well as the local community. The author refers to such public dissemination of uncomfortable facts as second-strike communications.[18] Signaling of punishment featuring such revelations could be coupled with entry bans not just for the targeted officials but for their family members as well.

To be sure, this would require cooperation from civil society entities not ordinarily involved in national security. It would also entail reaching those regimes' citizens. Chinese state authorities spare no effort to prevent such access by banning Western social media platforms such as Twitter. Nevertheless, many ingenious Chinese citizens do manage to access proscribed content. While Russians—often with justification—distrust Western criticism of their government, exposés of officials' families living large in the West on taxpayer money could cause a stir. Neither Western banks nor universities would delight in cooperating with their home governments in exposing some of their well-paying customers. The issue of Chinese and Russian influence in the West is, however, gaining so much attention in the public debate that both educational institutions and commercial firms may be convinced to do so, if only to cleanse their brands.

In response to, say, a new case of systematic intellectual property theft by companies linked to the Chinese government, one possible response might be to draw attention to the U.S. university enrollment of certain Chinese officials' children. Better yet, it should signal that such revelations may be part of the punishment. This should not be a general accusation—if nobody is named, nobody will be shamed—but signaling that specific individuals, officials, and their families will be singled out.

Traditionally, Western governments have not highlighted foreign leaders' private associations

Justice Department charges five Chinese members of APT41 over cyberattacks on U.S. companies. (Federal Bureau of Investigation, September 19, 2020)

with their countries, as it seemed irrelevant to Great Power politics and was at any rate considered contrary to diplomatic protocol. With hostile governments hiding behind gray zone acts to weaken the West it is, however, imperative that Western governments be more innovative and daring, while yet adhering to their ethical standards. Indeed, if Western governments demonstrate an ability to think creatively about retaliation, they will constantly keep the attackers in uncertainty and fear, thereby reducing the country's appetite for aggression. As Thomas Schelling reminded policymakers, surprise is a key element of deterrence.[19]

There is precedent in communicating with rivals' publics. During the Cold War, governments on both sides established radio stations serving the populations of their rival states. Radio Free Europe/Radio Liberty, initially funded by the CIA, was part of that effort.[20] Of course, if Western governments increase their already existing efforts to communicate with rivals' citizens, they cannot criticize rival governments for communicating with theirs.

Retaliation could, as Biden suggested, also include publicly sharing information about corruption. In addition, it should clearly include Defending Forward and its sister policy, criminal indictments against individual perpetrators. The Trump administration continued its predecessor's nascent practice of not just naming and shaming countries to which it had attributed cyber attacks, but of indicting individual perpetrators as well. On September 16, 2020, the Department of Justice charged five Chinese nationals with cyber attacks on more than 100 companies in the United States and elsewhere;[21] one month later it charged six officers in Russia's military intelligence agency with cyber attacks against Ukraine, Georgia, the 2017 French election campaign, and the 2018 Winter Olympics.[22] The officers were also charged with having perpetrated the devastating NotPetya attack in 2017, which was directed against Ukraine but brought down a range of international companies as well. In July 2020, the EU issued its first-ever sanctions over a cyber attack, imposing a travel ban and other penalties on six Russian and Chinese nationals involved in NotPetya and several other attacks.[23]

Criminal prosecutions constitute an even stronger deterrent but are only possible if the defendant is present; and a targeted foreign official is highly unlikely to present him- or herself for prosecution abroad. Because indictments, however, effectively bar the accused from entering the country (for reasons other than presenting him- or herself to law enforcement authorities), and subject them to possible extradition to the United States if apprehended in third countries, they block an attacker from benefits available to the general public. The attacker thus has to weigh participating in gray zone aggression on behalf of a government against being able to travel freely abroad or visit the United States.

These examples illustrate some of the possibilities of targeted deterrence. The author refers to the this as *personalized deterrence*.[24] Its basic operating assumption is that many officials and other perpetrators and sponsors of gray zone aggression are likely to be more loyal to themselves than to their regimes, and that the prospect that they will personally suffer retaliation by the United States can substantially change their cost-benefit calculation. The objective—following Schelling's surprise element dictum—is to keep representatives of the hostile country guessing as to which punishment will be meted out, whom it will target, and when—and whether—it will take place.

As with deterrence by punishment, deterrence by denial should be demonstrated and thereby communicated to countries already engaged in gray zone aggression and countries flirting with the prospect. Military exercises do not just serve the purpose of soldiers perfecting their skills but the equally important message of signaling those skills to potential attackers. Specially designed exercises can also be used to signal to would-be adversaries that their efforts to subvert our interests through gray zone aggression will yield insufficient gains to justify the costs. To date, although government agencies have practiced for contingencies related to gray zone aggression, there have been no specific gray zone defense exercises. The closest existing exercise is Sweden's *Total Defense 2020* exercise, which focuses on traditional threats but does include all parts of the government as well as businesses and volunteers. During the Cold War, Sweden regularly held total defense exercises; this exercise is the first such since 1987.[25] Given the nature of gray zone aggression, such exercises should involve the armed forces, the government, industry, and civil society volunteers, and be of a purely defensive nature.

The author has proposed a concept for gray zone exercises involving the armed forces, industry, and other relevant government agencies. The government would identify private companies that would benefit from gray zone preparation; that is, most companies engaged in critical national

infrastructure in the wider sense. Businesses would also be able to apply to participate. Upon conclusion of the exercises, participating businesses would be awarded ISO-style certification, which they could keep current through renewed participation in gray zone exercises.[26] In January 2021, the Czech Republic premiered the concept with a pilot exercise.[27]

In the six years since Russia's annexation of Crimea—the event generally considered the West's wakeup call concerning Russia's ability to use gray zone aggression—the focus has been on Western vulnerabilities in the face of their adversaries. There is no doubt that the open borders and free societies characteristic of liberal democracies that allow citizens and foreigners alike to pursue their lives unimpeded by government present countless opportunities for gray zone aggression by unscrupulous adversaries. By thinking innovatively, however, Western countries can improve both their deterrence by resilience and deterrence by punishment to at least discourage if not prevent gray zone aggression. By creatively using their advantages, Western countries in cooperation with their allies can mitigate their vulnerabilities. Indeed, innovative thinking is a deterrent in itself, one that keeps the attacker uncertain about the resilience and punishment that might ensue, and thus changes the cost-benefit calculus. PRISM

Notes

[1] "Russian spy poisoning: What we know so far," BBC, October 8, 2018, available at <https://www.bbc.co.uk/news/uk-43315636>.

[2] Prime Minister Theresa May, "Oral statement to Parliament: PM Commons statement on Salisbury incident," March 12, 2018, available at <https://www.gov.uk/government/speeches/pm-commons-statement-on-salisbury-incident-12-march-2018>.

[3] Oona A. Hathaway and Scott J. Shapiro, *The Internationalists: How a Radical Plan to Outlaw War Remade the World* (New York: Simon and Schuster, 2018). For figures since 1946, see, Uppsala Conflict Data Program, "Armed Conflicts by Region and Year, 1946–2019," available at <https://ucdp.uu.se/downloads/charts/>.

[4] Julian Borger, "US orders Russia to close consulate and annexes in diplomatic reprisal," *The Guardian,* August 31, 2017, available at <https://www.theguardian.com/us-news/2017/aug/31/us-russia-san-francisco-consulate-close>.

[5] Alia Chughtai and Mariya Petkova, "Skripal case diplomatic expulsions in numbers," Al Jazeera, April 3, 2018, available at <https://www.aljazeera.com/news/2018/4/3/skripal-case-diplomatic-expulsions-in-numbers>.

[6] Elisabeth Braw, "Second Strike Communications," *Royal United Services Institute (RUSI) Newsbrief* 39, no. 4 (May 17, 2019), available at <https://rusi.org/publication/rusi-newsbrief/second-strike-communications>.

[7] Tom Newton Dunn and Mark Sedwill, "We always hit back hard. Russia paid a high price for Salisbury poisonings," *The Times*, October 24, 2020, available at <https://www.thetimes.co.uk/edition/news/mark-sedwill-we-always-hit-back-hard-russia-paid-a-high-price-for-salisbury-poisonings-5v3n3hngk>.

[8] Zak Doffman, "Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First," *Forbes,* May 6, 2019, available at <https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=3209e8caafb5>.

[9] *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, presented to Parliament by the Prime Minister by Command of Her Majesty, March 2021, 77, available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969402/The_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf>.

[10] *Americans Split on Relationship with Russia*, University of Chicago Harris School of Public Policy and The Associated Press-NORC Center for Public Affairs Research, September 11–14, 2020, available at <https://apnorc.org/wp-content/uploads/2020/10/topline_release1.pdf>.

[11] Elisabeth Braw, "This Time, the Meddling Is Coming From Inside the House," *Foreign Policy,* November 5, 2020, available at <https://foreignpolicy.com/2020/11/05/election-hacking-domestic-trump-biden-vote/>.

[12] Försvarshögskolan, *Förutsättningar för krisberedskap och totalförsvar i Sverige* (2019), 19, available at <https://www.fhs.se/download/18.165b2e611685dbe45333940a/1549227413452/F%C3%B6ruts%C3%A4ttningar%20f%C3%B6r%20krisberedskap%20och%20totalf%C3%B6rsvar%20i%20Sverige%202019.pdf>.

[13] John Verhovek, "Biden warns against foreign interference in US elections: 'I am putting the Kremlin and other foreign governments on notice'," ABC, July 21, 2020, available at <https://abcnews.go.com/Politics/biden-warns-foreign-interference-us-elections-putting-kremlin/story?id=71886014>.

[14] "Vladimir Putin: Russian palace in Navalny video not mine," BBC, January 25, 2021, available at <https://www.bbc.co.uk/news/world-europe-55799143>.

[15] Elisabeth Braw, Educating Their Children Abroad Is the Russian Elite's Guilty Secret, *Newsweek,* July 30, 2020, available at <https://www.newsweek.com/2014/08/08/educating-their-children-abroad-russian-elites-guilty-secret-261909.html>; see also "Tuition and fees," The American School in Switzerland, available at <https://www.tasis.ch/page.cfm?p=736>.

[16] Andrew Higgins and Maureen Fan, "Chinese communist leaders denounce U.S. values but send children to U.S. colleges," *Washington Post,* May 19, 2012, available at <https://www.washingtonpost.com/world/asia_pacific/chinese-communist-leaders-denounce-us-values-but-send-children-to-us-colleges/2012/05/18/gIQAiEidZU_story.html>.

[17] Intelligence and Security Committee of Parliament, *Russia Report*, presented to Parliament Pursuant to Section 3 of the Justice and Security Act of 2013, July 21, 2020, available at <https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo1Y2RhMGEyN2Y3NjM0OWFl>.

[18] Braw, "Second Strike Communications," May 17, 2019.

[19] T. C. Schelling, *The Reciprocal Fear of Surprise Attack* (Santa Monica, CA: RAND, April 16, 1958), available at <https://www.rand.org/content/dam/rand/pubs/papers/2007/P1342.pdf>.

[20] "History," Radio Free Europe/Radio Liberty, available at <https://pressroom.rferl.org/history>.

[21] Department of Justice, "Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," press release, September 16, 2020, available at <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>.

[22] Department of Justice, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," press release, October 19, 2020, available at <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>.

[23] Lorne Cook, "First ever EU cyber sanctions hit Russian, Chinese, NKoreans," AP, July 30, 2020, available at <https://apnews.com/article/malware-technology-foreign-policy-international-news-military-intelligence-978f1494313a545e6e7e568e5f9782bf>.

[24] Elisabeth Braw and Gary Brown, "Personalised Deterrence of Cyber Aggression," *The RUSI Journal* 165, no. 2 (March 18, 2020), 48–54.

[25] *Försvarsmakten/MSB*, Totalförsvarsövning 2020. Tillsammans försvarar vi Sverige, <https://www.forsvarsmakten.se/contentassets/dd56a6422b8e496ab552c5f4186da291/tfo_faktablad_se-faststalld.pdf>; see also, Gerhard Wheeler, "Northern Composure: Initial Observations from Sweden's Total Defence 2020 Exercise," RUSI, September 3, 2020, available at <https://rusi.org/commentary/northern-composure-initial-observations-swedens-total-defence-2020-exercise>.

[26] Elisabeth Braw, "The Case for Joint Military–Industry Greyzone Exercises," *RUSI Briefing Papers*, September 28, 2020," available at <https://rusieurope.eu/publication/briefing-papers/joint-military-industry-greyzone-exercises>.

[27] Helen Warrell, "Czech Republic turns to war-games to build cyber defences," *Financial Times,* February 17, 2021. <https://www.ft.com/content/8c018644-3866-4f69-9105-d3c0e68ca491>.

STRATEGIC LANDPOWER SYMPOSIUM

REGISTRATION AND CALL FOR PAPERS

10-12 MAY 2022
US ARMY HERITAGE EDUCATION CENTER
CARLISLE, PA

The **USAWC** in partnership with **HQDA G3/5/7** are pleased to announce the first annual Strategic Landpower Symposium (SLS), to solicit research and encourage professional discussion on "Strategic Landpower in Cooperation and Competition."
(see Chief of Staff Paper #1)

Papers should consider:
The Future Role of Strategic Landpower in Integrated Deterrence; Cooperation; Competition; and/or, Joint All Domain Operations.

Submissions on related topics are also welcome.
Call for papers submission deadline is 1 December 2021.

See website for details:
https://csl.armywarcollege.edu/landpower/

Dr. Greg Cantwell
email: gregory.l.cantwell.civ@mail.mil
THE UNITED STATES ARMY WAR COLLEGE

The fall of the Berlin Wall - November 1989 (Gavin Stuart, January 30, 2006)

The New Geopolitics of Human Rights

By Seth D. Kaplan

As economic and military strength become more evenly distributed among major actors around the globe, ideas are taking on an outsized role in geopolitics. In the United States' effort to outcompete China, Russia, and other rivals, its ideas are likely to play a defining role in determining the strength of alliances and the vulnerability of foes. The more its ideas have an inherent appeal based on their universality—transcending culture and context—the more likely the United States will be able to leverage them to forge a coalition that can withstand geopolitical threats and apply pressure for reform in places like China.

During the Cold War, America's security enabled its ideas to flourish; the latter complemented the former in a virtuous cycle. By winning over elites and populations to its ideas (which were shared across the West but promoted most assertively by Washington), it built partnerships, added countries to its orbit, and eventually converted many behind the Iron Curtain—strengthening its alliances and thus security while weakening those of the communist bloc in the process. As such, while a robust nuclear weapons program and military deterred direct aggression, they were at best defensive measures that provided time and space for the United States to strengthen its position by promoting several core ideas: capitalism, the rule of law, democracy, and human rights.[1]

Human rights played a prominent role in the American arsenal. They contributed to the wave of democratization that started in the 1970s in Southern Europe and spread across Latin America, Africa, and Asia, securing many allies along the way. Starting in the 1960s and building steam with the 1974 Jackson-Vanik Amendment, which tied Soviet-American trade to the treatment of Jewish refuseniks, and the 1975 Helsinki Final Act, which inspired the establishment of human rights monitoring groups across the Soviet Bloc, human rights slowly worked to undermine the legitimacy of the entire communist enterprise—achieving America's most important security goal without the use of force.[2]

The coming decades will likely see another protracted battle, this one with the Chinese Communist Party (CCP). Although the fight for global supremacy will be the same, the nature of the competition will inevitably be different given China's economic dynamism, the two country's interdependencies, and the great cultural gaps. China's enormous economic clout presents a particularly difficult challenge. It is the world's largest exporter,[3] trading more with 128—and twice as much with 90—of the World Trade Organization's 190 members than the

Seth D. Kaplan, a Lecturer in the Paul H. Nitze School of Advanced International Studies (SAIS) at Johns Hopkins University, is the author of Human Rights in Thick and Thin Societies: Universality Without Uniformity (Cambridge, 2018).

United States in 2018.[4] It is one of the two largest suppliers (with the United States) of grants and loans to developing countries,[5] and was, for the first time, the largest recipient of foreign investment in 2020.[6]

Despite its economic strength, the CCP is vulnerable to any competition of ideas centered on human rights. Since Xi Jinping took power in 2012, China has imprisoned over a million Muslim Uighurs in internment camps because of their faith and ethnicity, detained hundreds of lawyers and grassroots activists, closed churches across the country, and arrested scores of people in Hong Kong just for protesting. Former Secretary of State Mike Pompeo's State Department determined that China was engaged in a genocide, noting that its mistreatment of the Uighurs extended even to their most intimate matters: "PRC authorities have conducted forced sterilizations and abortions on Uighur women, coerced them to marry non-Uighurs, and separated Uighur children from their families." His successor, Anthony Blinken, quickly concurred.[7]

We clearly need to leverage American ideas to face China's rising influence, yet the idea of human rights has been badly tarnished. Instead of reflecting a common, universal heritage, human rights are too often politicized, oriented around Western concerns, and cheapened as they grow in number. This both diminishes their appeal and enables foreign leaders to oppose them on charges of imperialism. The Commission on Unalienable Rights, which the U.S. State Department established in 2019 to address the severity of this human rights recession, states in its final report, "in today's multipolar world… it is plain to see that the ambitious human rights project of the past century is in crisis. The broad consensus that once supported the Universal Declaration of Human Rights (UDHR) principles is more fragile than ever, even as gross violations of human rights and dignity continue apace."[8]

How can the United States restore this consensus? A return to basics in how it promotes human rights will strengthen alliances with other countries—alliances that will be needed to challenge China and to catalyze pressure from within to delegitimize the regime among the population. This would replicate the formula that made human rights so essential to America's victory in the Cold War.

How Human Rights Helped Win the Cold War

Although the idea of human rights barely existed before World War II and there was resistance to its universality after it, the concept came to have striking influence on East–West relations during the later years of the Cold War. This influence, however, took time to emerge and depended on a series of initiatives that put rights at center stage. Looking closer at the historical dynamics that led to human rights' success can help us find a pathway to restore their influence in the decades ahead.

Despite the adoption of the UDHR in 1948, human rights did not start to play a major role in Western thinking until concerns over civil rights began to emerge in a significant segment of Western populations. In 1961, Amnesty International was established to campaign for political prisoners and human rights worldwide. Starting in the United Kingdom, it evolved to develop chapters in many European countries as well as the United States, with each dedicated to forming small groups of members to campaign on behalf of specific adopted prisoners. Support for a more proactive human rights effort grew stronger as decolonization created dozens of new states (who immediately became advocates); the crisis in Rhodesia in 1965 pushed the U.S. to take a stronger stand (to win the new states to its side in the Cold War); and the Greek coup in 1967 produced concerns over the treatment of prisoners in what was considered the birthplace of democracy.

In contrast, the Soviet Union actively supported human rights internationally—especially with regard to decolonization, economic and social

rights, and women's rights—from early on, even while the regime was repressive at home. This came back to haunt it when a movement among its *intelligentsia* emerged in the mid-1960s. As Eric D. Weitz writes, the vocabulary of rights entered the country's discourse through its leaders' use of the term at the United Nations—most notably, Andrei Gromyko in 1947 and Nikita Khrushchev in 1960—and the country's active participation in its Commission on Human Rights. The loud proclamation of rights within the country's own constitutions—1936 as well as 1977—were then used to demand the right to free speech, assembly, and emigration and an end to the extra-judicial, callous treatment of those who dared to violate these. Eventually, the homegrown activists emerging from the *intelligentsia* movement formed a number of organizations (e.g., Initiative Group to Defend Human Rights in the USSR, Moscow Human Rights Committee) and drew upon the UDHR to internationalize their movement, helping to spur Western support.[9]

Among these activists, Jews seeking religious freedom or the right to emigrate from the Soviet Union became prominent voices, especially after the Israeli victory in the 1967 war. These refuseniks—including Anatoly Shcharansky—attracted significant sympathy in the United States, where the large Soviet Jewry Movement developed to promote their rights. The Jackson-Vanik Amendment was passed in 1974—over the opposition of the Nixon administration—tying American trade to the issuance of exit visas. However, the Soviet Union reduced rather than increased emigration and suppressed dissent (Shcharansky was imprisoned in 1977 and spent nine years in jail).

The turning point came in 1975 with the Helsinki Final Act, an agreement among members of the Conference on Security and Co-operation in Europe (now known as the Organization for Security and Co-operation in Europe). The accord had been originally sought by the Soviet Union in order to secure its hegemony in Eastern Europe. It was designed to reduce tensions by securing common recognition of the post-World War II European boundaries, incorporating commitments to safeguard human rights and expand travel, communication, and information flow between the two blocs as the price for Western support.[10] Moscow was reluctant to accept these terms but it believed any challenges to its rule that they brought could be easily crushed.

The agreement spurred the establishment of human rights monitoring groups—most notably the Moscow Helsinki Group—across the Eastern Bloc. It, Sarah Snyder writes, detailed rights violations on "issues as varied as national self-determination, the right to choose one's residence, emigration and the right of return, freedom of belief, the right to monitor human rights, the right to a fair trial, the rights of political prisoners, and the abuse of psychiatry." In time, it would report on its own members' arrests.[11]

The formation of the Moscow Helsinki Group catalyzed the development of a network of monitoring groups both within the Soviet Union—in places such as Georgia, Ukraine, and Lithuania—and abroad. These, in turn, spurred further organized dissent as activists, journalists, lawyers, and diplomats worked across borders to publicize the jailing of dissidents and the government repression within communist countries. Czechoslovakia's Charter 77 (established in 1977) and Poland's Solidarity (established in 1980), both of which would go on to play prominent roles in the 1989 roll back of communism in Eastern Europe, were offshoots; two of many initiatives inspired by the original group in Moscow. Helsinki Watch (today Human Rights Watch), established in the United States in 1977, supported these myriad efforts by compiling comprehensive reports on specific issues and promoting the cause through the media and participation in CSCE meetings. The Helsinki Federation for Human Rights (IHF), founded in 1982 by leading

monitoring groups, both increased the weight of the organizations' criticisms in international debates and helped the groups within the Soviet Bloc withstand the rising crackdown.

This altered and energized international landscape, combined with greater orientation toward civic causes domestically, made human rights a much greater theme in American foreign policy starting in the mid-1970s. Congress established the human rights bureau within the U.S. State Department in 1976. President Jimmy Carter's declared in his inaugural address in 1977 that "Our commitment to human rights must be absolute"[12] and then tried to make the issue a prominent part of his foreign policy. He corresponded with Andrei Sakharov and criticized East Bloc countries over their repression in a way previously not done.[13]

While he started off hesitant, President Ronald Reagan became an enthusiastic supporter of human rights during his time in office, at least partly, as an internal State Department memo wrote, because it helped in the "Battle for Western Opinion"—winning support on the left and right at home and in Western Europe—and because it offered "the best opportunity to convey what is ultimately at issue in our contest with the Soviet bloc."[14] He repeatedly used the bully pulpit to speak out, most famously in Berlin in 1987 when he challenged Mikhail Gorbachev to "tear down" the Berlin Wall. When Reagan visited Moscow in 1988, he applauded the progress Gorbachev was making in reforming his country but demanded more, asking for further improvement, especially on the freedoms of religion, speech, and travel.[15]

In the end, Eastern Europe freed itself and the Soviet Union dissolved. Snyder explains how,

> Protest movements inspired in part by Helsinki principles; reforms formulated in part to comply with Helsinki commitments; and new leaders, many of whom were active in Helsinki groups, all came to the fore… internal and external forces advocated for a new relationship between the state and society in Eastern Europe.[16]

Ambition and Ascendant Authoritarianism

Today, the human rights field has mostly failed to inspire this kind of international movement to support people threatened by authoritarianism, most notably in China. There are many activists on the mainland and in Hong Kong and a number of major human rights organizations outside the country promoting rights in it. But there is nothing like the war of ideas or international pressure on the regime that compares to what happened during the Cold War.

China's economic success, deep trade linkages with countries around the world, huge investment in infrastructure in many countries (most notably through the Belt and Road Initiative), and the CCP's generally high popularity at home can partly explain why it pays little price for its suppression of Christianity and Islam; mass detention, surveillance, and even forced separation of parents and children who are ethnic Uighurs; silencing of dissidents on the mainland; and actions in Hong Kong that turned one of the world's freest places into one with severe political restrictions. Countries are reluctant to criticize a country they depend so much on—even Muslim countries that freely disparage the United States and other Western democracies for far lesser flaws don't criticize Beijing. But economics don't explain the whole problem; the human rights field's evolution since the Cold War is also responsible.

Human rights face a growing backlash in many countries because leaders feel the emerging agenda does not represent their values and needs. In such places, there is not necessarily a disagreement with the broad goals, but rather, as Brazilian academic Oliver Stuenkel writes, the "operationalization of liberal norms," and the "implicit and explicit hierarchies of international institutions" that privilege Western countries and concerns.[17] Freedom House reports

Close to two million people hit the streets on Sunday (16th June 2019) to call on the Hong Kong government to withdraw a controversial extradition bill. (Etan Liam, June 16, 2019)

that democracy, which is practically synonymous with human rights in the West, "is under assault and in retreat around the globe."[18] The organization's measurements of political rights and civil liberties have registered 14 consecutive years of decline.[19] Meanwhile, foreign-funded civil society organizations that promote human rights are increasingly viewed suspiciously. This is true not only in authoritarian regimes such as Russia, Azerbaijan, Turkey, Sudan, Egypt, and Venezuela, but also democracies such as Mexico, Malaysia, Nigeria, Hungary, and Israel, all of which have passed or are considering passing legislation regulating the sector.[20]

There are many reasons for this pushback, but the most important is the overweening dual ambition born of success. Human rights advocates have broadened the scope of issues covered by human rights while narrowing the room for differences in bringing those rights to life. Whereas once the focus was on upholding human dignity in places such as China by safeguarding a small number of basic rights—freedoms of religion and speech, protection from arbitrary arrest and imprisonment, access to fair and fast trials—today the number of rights, and rights claims, has risen steeply as various well-meaning special interest groups have sought to harness the moral authority of the human rights idea to their causes.[21]

Calls to make everything from access to the internet to free employment counseling a human right have cheapened the meaning and multiplied the clashes of rights. China can, for example, correctly claim that it is doing quite well on most rights even if it is locking up dissidents, crushing free speech, imprisoning people because of their religious

Egyptian security forces fire tear gas canisters in to a large crowd of protesters gathered near the Ministry of Interior. (Alisdare Hickson, February 4, 2012)

identities, and preventing some citizens from traveling abroad. Yet, as Jacob Mchangama and Guglielmo Verdirame, co-founders of the Freedom Rights Project, note with disappointment, "much of the human rights community has not only shied away from expressing qualms about rights proliferation, it has often led the process."[22] In addition to supporting rights inflation, human rights activists have invited controversy—something the UDHR drafters knew could only hurt their cause—by often emphasizing new or novel interpretations of rights with no historical basis and giving them unequal weight.

Meanwhile, attempts to enforce a uniform conception of rights has reduced the space for local actors to formulate their own pathways,[23] fueling skepticism about the rights themselves and even criticism that they are just another plank in the long reach of Western imperialism. Today's human rights discourse is controlled by advocacy organizations, lobbyists, academics, and journalists that share a remarkably similar interpretation of rights based on individualistic Western normative assumptions that are controversial even in the West—and quite different from those that underlaid the human rights project in its first few decades. This naturally excludes those who have a more communitarian or religious vision of the good life—arguably a significant majority of the world's population—undermining the very legitimacy of human rights in their eyes. As a result, governments can hide behind the cultural card when criticized precisely because of the unease created by the overly narrow approach adopted. This holds back efforts aimed at separating legitimate cultural concerns from criticisms that merely advance the interests of self-serving leaders and governments abroad.

These changes ignore the historical dynamics that led to human rights' success. The Universal Declaration, the foundation for much of the post-World War II rights project, sticks to a modest set of principles that no nation would wish openly to disavow, principles that can inspire people across different cultures by appealing to a common sense of what everyone could believe was morally binding. It focuses only on a small number of rights, and avoids issues that would in any way be controversial. Moreover, only a handful of the rights are considered core "primary rights" specifying strict restrictions on things like torture, enslavement, degrading punishment, discrimination, and limits to religious freedom. The rest of the rights are meant to be flexibly interpreted depending on the context.[24]

This suggests that although all rights in the UDHR are important and need to be upheld, there is universal agreement that a few have special priority and thus require more rigid enforcement in all contexts—the very rights that emerged as flashpoints during the Cold War due to the work of the Moscow Helsinki Group and Amnesty International in its early years. This idea is echoed in the many subsequent human rights treaties that have a set of legally-binding, non-derogable or emergency-proof rights.[25] (In contrast, many of the emerging rights have little basis in international agreements. For example, LGBT (lesbian, gay, bisexual, and transgender) rights may be important, but they do not appear in any major global agreement because there is no international consensus on them—and many countries are opposed to the idea. Women's rights, on the other hand, were recognized in the Declaration—it uses phrases such as "all human beings" and gender neutral language.

Western human rights organizations have also enlarged the international legal infrastructure that supports their efforts, creating state-like supranational institutions such as the International Criminal Court (ICC), and multilateral doctrines such as the "Responsibility to Protect," over which they have significant influence. But these have limited support outside the West; even democracies such as Brazil and South Africa are at best ambivalent. Moreover, they only focus on countries with weaker geopolitical standing—as of this writing, all 29 cases taken up by the ICC are in Africa[26]—because states such as China refuse to join and can block referrals. The ICC, for example, has no jurisdiction on cases within China, while governments such as Syria's can commit atrocities with little fear of prosecution or intervention due to a Russian veto. The emphasis on multilateralism actually plays to China's strength—it can block criticism and shift the emphasis of human rights activity through its United Nations veto, membership in the U.N. Human Rights Council, and influence with governments worldwide.[27] During the Cold War, by contrast, the movement was led by the spirited action of a large number of activists on both sides of the Iron Curtain, yielding a popular movement with a simple message that could resonate far and wide.

While the existing Western outlook and approach could be sustained in a unipolar world—which existed in the immediate aftermath of the Cold War—it is unsustainable in today's multipolar world, in which the greatest challenge to freedom emanates from authoritarian, geopolitical rivals. The rise of China as a competing model and the weakening of U.S.—and Western—influence around the world reduces the effective reach of any ideas (such as those not included in the main international human rights treaties) that are not morally binding across all the world's major philosophical and religious systems.[28] Countries that once accepted human rights ideas out of deference to Western accomplishment or power (e.g., Southeast Asia, Middle East, Africa) today can easily push back on them if the ideas do not have local roots—as Stephen Hopgood argues in *The Endtimes of Human Rights*.[29] (The United States' historical

inconsistency in promoting rights—by, for example, supporting authoritarian regimes that backed its side in the Cold War—does not help.) The great cultural differences that exist between the West and China—a contrast to the situation during the Cold War when East and West were both centered on Europe and its common heritage—makes this challenge even greater. Rights claims must be based on principles that are indisputable across cultures if they are to have the moral force necessary to be effective—as was the case in the Declaration. This moral force is what will arouse people everywhere—especially within China—to act.

Reclaiming Core Human Rights

Only by concentrating on the protection of a few practical rights—the core rights in the UDHR—can human rights again be the rallying cry that unites people and countries into a coalition against an authoritarian powerhouse while working to eat away at that state's legitimacy from within. This return to basics approach—aiming first and foremost at eliminating the "great evils of the human condition"[30]—would have relatively little difficulty gaining support from a wide set of people who normally are far apart in their philosophical and cultural outlook. It would not end debates over rights—these are inevitable—but would make attacks on them far easier to fend off, strengthening the legitimacy of the whole human rights project in the process. Other rights would still matter, but they would receive less priority and countries would be given more flexibility on how they achieved them.

This focused approach would hit China where it is most vulnerable. Whereas there are legitimate disagreements on how important many rights are, including whether democracy is necessary to uphold basic rights and develop economically, there are few people around the world—including in China—who would not support the core rights that millions of Chinese citizens are currently denied. Moreover, it is hard to argue that eliminating discrimination based on ethnicity or religion, safeguarding religious freedom, and offering due process and fair trials to dissidents (who are mostly seeking only to improve the rule of law in the country, not overturn its power hierarchy) would actually hurt the country's economic prospects. In fact, it could be argued that a stronger rule of law and a more inclusive polity would enhance its human—and thus economic—potential.

The State Department's Commission on Unalienable Rights reached similar conclusions. Although it sought to ground American human rights policy in both "our nation's founding principles and the 1948 Universal Declaration of Human Rights" and thus placed a greater emphasis on civil liberties and the right to pursue the fruit of one's labor,[31] the Commission's final report also emphasized the importance of both maintaining a global consensus on core human rights and accommodating diversity in cross-cultural implementation. The "interplay between universal principles of human rights and the variety of human realities in which they must be honored is at the heart of the challenge of making human rights effective," it says.[32] Similarly, the report emphasizes the importance of the UDHR both as a rights framework and as an example of how an international consensus around rights can be built. The goal was to be a political and moral document, "not as a legal instrument creating formal law."[33]

The report (like the UDHR) goes on to make a sharp distinction between unalienable and positive rights.[34] Whereas unalienable rights are universal and pre-political, positive rights depend on context: They are the product of custom, tradition, and civil society established through politics, and may change over time. The commission makes clear that both are important and can be closely linked but that their roles are different. For example, even though there is no global consensus on elderly rights,

Singapore has mandated since 1995 that anyone over 60 years old is entitled to financial support from their children if they need it.[35] The core rights in the UDHR are unalienable—with universal support—while many of the rights promoted today are positive, and thus dependent more on context.

The Biden Administration: Tools and Possibilities

Ideally, the Biden administration would take this report to heart, make it a centerpiece of its human rights strategy worldwide, and use it in the ideological confrontation with China and other geopolitical threats. But new Secretary of State Anthony Blinken said he would "repudiate" the report during his confirmation hearings,[36] calling into question whether the new administration will learn the lessons of recent decades. Nevertheless, given its longstanding prominence in United States foreign policy (and the new administration's early statements on, among other things, Myanmar and Hong Kong), it is likely that human rights will play a prominent role. What strategy should it adopt vis-à-vis China?

A Helsinki duplicate won't work in Asia because China would never sign a similar agreement, and many of the countries whose support the United States needs—such as Vietnam and Thailand—would be at best ambivalent about doing so. In addition, the region lacks the multilateral frameworks—NATO, the Warsaw Pact, the European Economic Community, and COMECON—that formed the building blocks for a regional accord.

Trade-related possibilities remain: a restoration of the Jackson-Vanik Amendment, which once applied to China, could link trade privileges to a small number of core rights, as was done during the Cold War vis-à-vis the USSR. Even though its application for China was annually waived starting in the late 1970s as relations between the two countries warmed and eventually ended when the country joined the World Trade Organization in 2002, the very process of renewal focused attention on China's human rights record, often creating great controversy and threats in Congress to overturn the waiver, especially after the Tiananmen Square killings of 1989.

Restoring the amendment (or legislating something similar) and ensuring it focused only on the few primary rights from the UDHR—all easily translatable across the world—would significantly alter the landscape. By penalizing China's exports—through a tariff based on an annual highly independent, not easily-politicized, public assessment of its human rights record in the few specified areas—it would both generate global publicity of the abuses and force Chinese exporters (on whose lives tens of millions of people depend) to come to grips with the CCP's poor behavior. This would create internal and external pressure for at least some alteration of the government's course, opening the door for further change in time—as happened with Helsinki. If the Biden administration could convince American allies in Europe, Australia, Japan, India, and elsewhere to line up with the United States and pass parallel legislation (possibly tied to the same assessments), then the effect would be that much greater.

Public Opinion and Grassroots Advocacy

What are the chances this will occur? Given the inclination of most American (and Western) governments towards conciliation rather than conflict—as was often the case vis-à-vis the Soviet Union—not very likely. As such, a more bottom-up approach that electrifies public opinion in support of core rights at home and abroad—as in the Cold War—may be necessary to shift public policy in this direction. David Satter writes, "the dissident movement acted to push Western societies, sometimes unwillingly, toward attention to first principles. The dissident movement had a profound impact on Western public opinion." Helped by outsized coverage in the media, their

No Muslim Ban 2, Washington, DC USA 00521. (Ted Eytan, February 4, 2017)

work made it "undeniable that the element holding the system together was fear." The effect was to "establish a source of truthful information independent of, and in some cases competing for attention in the West with, the disinformation apparatus of the Soviet state."

The impact on public opinion forced change in the policies of governments. Many working in official positions "would have preferred to deal with the Soviet Union 'pragmatically,' concentrating on what they imagined to be 'mutual interests.'" But the change in public opinion "made such policies politically impossible." The result was an "ideological counteroffensive directed against the moral vulnerability of the Soviet Union," and a stronger stance on the part of Western governments to tie measures advantageous to the country—such as trade—to basic human rights.[37] Despite the violations to core rights exposed by Black Lives Matter (BLM) and other social movements in recent years, the United States and its Western allies still hold a predominant position on their protection—and the more our human rights agenda focuses on these, the easier it will be to "convey what is ultimately at issue in our contest" with China. In fact, the rise of BLM is a testament to America's basic freedoms and ability to withstand criticism when it falls short in safeguarding them—a great contrast to what is possible in China and other authoritarian regimes.

The American Soviet Jewry Movement, mentioned above, was the best example of this approach during the Cold War. Spurred by two small grassroots groups—one based in Cleveland that ultimately joined up with newer groups all over the country, the other based in New York City and geared towards students—and working far outside the American Jewish establishment, a relatively small number of activists spurred the development of a national movement. The movement catalyzed establishment actors to address the issue more

forcefully, leading to the founding of the National Conference on Soviet Jewry, and shifted government policy when it fully supported the Jackson-Vanik amendment—the strongest exercise of political power in the history of the community.[38]

The movement kept a bright spotlight on human rights abuses by vigorously campaigning for specific Soviet Jewish refuseniks (those who had sought to leave the country but were refused), making Anatoly Shcharansky, the most famous refusenik, a household name in the United States by the end of the 1970s. It established a slew of initiatives to draw attention to the hardships these Jews suffered—the wearing of bracelets inscribed with names of refuseniks, the twinning of young children with their counterparts who had fewer freedoms, writing campaigns, mass rallies, protests, lobbying, and even traveling to the Soviet Union to meet and support refuseniks directly. As Elliot Abrams writes, "In the 1970s and 80s it seemed as if every synagogue in America had a huge poster outside of it demanding freedom for Soviet Jewry."[39]

Christian or Muslim groups—those most egregiously treated in China today—could catalyze a similar movement today. If the movement could also win allies in Muslim and Christian countries worldwide (roughly half the world's population is affiliated with these two faiths), then its impact would be multiplied, with a greater chance of a dramatic geopolitical turn towards the restored vision of human rights and broad, sustained pressure on the Chinese government. All of this would strengthen regime opponents domestically and create growing pressure on the regime to at least partially reform, a crack that could lead to greater changes over time.

The rising influence of China, Russia, and other authoritarian regimes marks the first time since the 1970s that liberal democracy is challenged globally by an alternative political framework.[40] It is essential that the United States launches a human rights counteroffensive, as the Commission on Unalienable Rights sought. But given the confusion on human rights today, this likely depends on the development of a grassroots movement to pressure the CCP and give American leaders and their allies the political will to pursue and uphold a targeted approach. Only by making clear to people everywhere, at home and abroad, just what the difference is between the United States and these regimes—a difference that is too easily lost in the way human rights are promoted today—can ideas once again become part of the American arsenal.

The focus on core rights should be seen as just one element in a broader recalibration of U.S. policies intended to better confront the challenges posed by these states, and designed to build a broad coalition incorporating countries from across the world. Given the economic interdependencies, this will inevitably mean sacrificing some interests in the short term and overcoming resistance from those who most benefit from the status quo (such as firms sourcing goods in China). But challenging Beijing should be seen as in our greater national interest—essential to ensuring that China never gains a geopolitical position that could threaten our own security and, in turn, our liberties. The strength of human rights ideas undermined the legitimacy of the Soviet Union and its Warsaw Pact allies, and that strength can be summoned again. PRISM

Notes

[1] Michael Mazarr, "The Essence of the Strategic Competition with China," PRISM 9, no. 1 (October 2020): 3–22.

[2] Sarah Snyder, "Human Rights and the Cold War," in Artemy Kalinovsky and Craig Daigle (eds.), The Routledge Handbook of the Cold War (New York: Routledge, 2014), 237–248.

[3] "Is China the World's Top Trader?" China Power, March 28, 2019, updated August 25, 2020, https://chinapower.csis.org/trade-partner/, accessed February 3, 2021.

[4] Alyssa Leng and Roland Rajah, "Chart of the week: Global Trade Through a US-China Lens," The Interpreter, December 18, 2019, https://www.lowyinstitute.org/the-interpreter/chart-week-global-trade-through-us-china-lens.

[5] Joe McDonald, "Report: China Catching up to US in Foreign Aid Flow," AP News, October 11, 2017, https://apnews.com/article/5f816fec396a463cb3c130e1ec44c58f.

[6] Paul Hannon and Eun-Young Jeong, "China Overtakes U.S. as World's Leading Destination for Foreign Direct Investment," Wall Street Journal, January 24, 2021, https://www.wsj.com/articles/china-overtakes-u-s-as-worlds-leading-destination-for-foreign-direct-investment-11611511200.

[7] Eugene Kontorovich, "A Genocide Test Faces the West," Wall Street Journal, January 27, 2021, https://www.wsj.com/articles/a-genocide-test-faces-the-west-11611775797.

[8] U.S. Department of State, "Report of the Commission on Unalienable Rights" (Washington, D.C.: U.S. Department of State Office of Policy Planning, 2020), 5.

[9] Eric Weitz, "The Soviet Union and the Creation of the International Human Rights System," Zeitgeschichte-online, December 2018, https://zeitgeschichte-online.de/themen/soviet-union-and-creation-international-human-rights-system.

[10] "Helsinki Accords," Encyclopaedia Britannica Online, July 25, 2020, https://www.britannica.com/event/Helsinki-Accords, accessed December 13, 2020.

[11] Snyder, "Human Rights and the Cold War," 241.

[12] Jimmy Carter, "Presidential Inaugural Address," delivered January 20, 1977, https://jimmycarter.info/presidential-inaugural-address-of-jimmy-carter/.

[13] Snyder, "Human Rights and the Cold War," 243.

[14] Tamar Jacoby, "The Reagan Turnaround on Human Rights," Foreign Affairs 64, no. 5 (1986): 1066–1086, 1072.

[15] President Ronald Reagan, "Remarks to Soviet Dissidents at Spaso House in Moscow," May 30, 1988, https://chnm.gmu.edu/1989/archive/files/reagan-speech-5-30-88_81685301b8.pdf.

[16] Snyder, "Human Rights and the Cold War," 245.

[17] Oliver Stuenkel, Post-Western World (Malden, MA: Polity Press, 2016), 184–185.

[18] Freedom House, "Democracy in Crisis: Freedom House Releases Freedom in the World 2018," January 16, 2018, https://freedomhouse.org/article/democracy-crisis-freedom-house-releases-freedom-world-2018.

[19] Freedom House, "NEW REPORT: Freedom in the World 2020 Finds Established Democracies are in Decline," March 4, 2020, https://freedomhouse.org/article/new-report-freedom-world-2020-finds-established-democracies-are-decline.

[20] See, for example, Thomas Carothers and Saskia Brechenmacher, "Closing Space: Democracy and Human Rights Support under Fire," Carnegie Endowment for International Peace, February 2014, http://carnegieendowment.org/2014/02/20/closing-space-democracy-and-human-rights-supportunder-fire/h1by.

[21] Jacob Mchangama and Guglielmo Verdirame, "The Danger of Human Rights Proliferation: When Defending Liberty, Less Is More," Foreign Affairs, July 24, 2013, www.foreignaffairs.com/articles/139598/jacob-mchangama-and-guglielmo-verdirame/the-danger-of-human-rightsproliferation.

[22] Mchangama and Verdirame, "The Danger of Human Rights Proliferation."

[23] Sally Engle Merry, Human Rights and Gender Violence: Translating International Law into Local Justice (Chicago, IL: University of Chicago Press Books, 2006), 220–221.

[24] Mary Ann Glendon, A World Made New: Eleanor Roosevelt and the Universal Declaration of Human Rights (New York, NY: Random House, 2001), 230.

[25] See, for example, Council of Europe, Collected Edition of the 'Travaux Préparatoires,' Volume VI (Dordrecht; Boston; Lancaster: Martinus Nijhoff, 1985), 78–81 and 126–129; Thomas Buergenthal, "The American and European Convention on Human Rights: Similarities and Differences," The American University Law Review 30 (1980–1981): 155–166, 165.

[26] International Criminal Court, "Cases," webpage, available at: https://www.icc-cpi.int/Pages/cases.aspx#Default=%7B%22k%22%3A%22%22%7D#2ae8b286-eb20-4b32-8076-17d2a9d9a00e=%7B%22k%22%3A%22%22%7D, accessed January 20, 2021.

[27] Ted Piccone, "China's Long Game on Human Rights at the United Nations," Brookings Institution, September 2018, https://www.brookings.edu/research/chinas-long-game-on-human-rights-at-the-united-nations/.

[28] Seth Kaplan, "Will Human Rights Survive in a Multipolar World?," The Washington Quarterly 42, no. 1 (Spring 2019): 111–127.

[29] Stephen Hopgood, The Endtimes of Human Rights (Ithaca, N.Y.: Cornell University Press, 2013).

[30] William Galston, The Practice of Liberal Pluralism (Cambridge, UK: Cambridge University Press, 2004), 181.

[31] U.S. State Department, "Report of the Commission on Unalienable Rights," 12–14.

[32] U.S. State Department, "Report of the Commission on Unalienable Rights," 32–33.

[33] U.S. State Department, "Report of the Commission on Unalienable Rights," 31.

[34] U.S. State Department, "Report of the Commission on Unalienable Rights," 12.

[35] Puay Ling Lim, "Maintenance of Parents Act," Singapore Infopedia, Singapore National Library Board, 2009, https://eresources.nlb.gov.sg/infopedia/articles/SIP_1614_2009-11-30.html.

[36] John Riley, "Biden's Secretary of State Nominee Vows to Allow Embassies to Fly Pride Flags Again," MetroWeekly, January 21, 2021, https://www.metroweekly.com/2021/01/bidens-secretary-of-state-nominee-vows-to-name-lgbtqi-envoy-allow-embassies-to-fly-pride-flags/.

[37] David Satter, "Soviet Dissent and the Cold War," *Hoover Digest* 2003, no. 2 (April 2003), https://www.hoover.org/research/soviet-dissent-and-cold-war.

[38] Gal Beckerman, "The Soviet Jewry Movement in America," My Jewish Learning, https://www.myjewishlearning.com/article/the-soviet-jewry-movement-in-america/

[39] Elliott Abrams, "Lessons of the Soviet Jewish Exodus," *Jewish Review of Books* 19, no. 1 (Spring 2019), https://jewishreviewofbooks.com/articles/5151/lessons-of-the-soviet-jewish-exodus/.

[40] Christopher Walker and Jessica Ludwig, "From 'Soft Power' to 'Sharp Power': Rising Authoritarian Influence in the Democratic World," in "Sharp Power: Rising Authoritarian Influence," report, International Forum for Democratic Studies (Washington, DC: National Endowment of Democracy, 2017)

If Sweden is attacked, the Swedish Armed Forces, with the support of the rest of the total defence, will defend Sweden in order to buy time, create room for manoeuvre and ultimately safeguard the country's independence. The resistance will be resolute and sustained. (Jimmy Croona/Swedish Armed Forces)

Rebuilding Total Defense in a Globalized Deregulated Economy

The Case of Sweden

By Karl Lallerstedt

National defence is often focused on military strategy, i.e. various ways of reducing an adversary's physical capacity and/or willingness to fight. However, the military assets of a state are only one aspect of its potential to deter and withstand aggression. The military capacity becomes largely irrelevant without broader societal resilience to withstand efforts to incapacitate the functionality of society, upon which both sustained military capacity and the political decision-making apparatus are dependent. Hence, military capacity needs to be seen in a broader context of total defense, or comprehensive defense.

During the Cold War, Sweden had one of the most comprehensive total defense systems in the world, only to dismantle it following the collapse of the Warsaw Pact. This article gives a background on Sweden's decision to reestablish total defense, highlights some of the shortcomings in national preparedness laid bare by the early phase of the COVID-19 pandemic, lists a number of inherent challenges in creating a new total defense structure, and proposes some solutions to addressing these challenges. Perhaps some of the lessons being learned in Sweden could be of value to other states deciding to orientate toward a more comprehensive defense approach.[1]

Building up an effective total defense system is both complex and costly, and political wishful thinking about the true costs of establishing a robust total defense system likely constitutes the single biggest threat to its effective implementation.

Sweden's Decision to Reestablish a Total Defense System

The Western optimism that characterized the early post–Cold War era has increasingly been replaced by concerns about the state of the global order, with 2020 being the 15th consecutive year of declining global freedom.[2] Democratic institutions are even under assault in some European NATO member states.

At the same time as Western values and cohesiveness are weakening, technological developments are making our societies more vulnerable. Digitalization has made key functions of modern society vulnerable to cyberattacks and has created new possibilities for influence operations. The development of long-range precision munitions has also made key infrastructure easier to target than ever before.

Against this backdrop of a more vulnerable West, Russian and Chinese power projection capacities and assertiveness have grown. For European states, the Russian invasions of Georgia in 2008 and Ukraine

Karl Lallerstedt is a Senior Advisor on Security Policy, Confederation of Swedish Enterprise.

in 2014, where conflict is still ongoing, as well as massive regional military exercises, have been particularly alarming.

Albeit perhaps somewhat late in the game, several European states have finally woken up to the realization that the previous neglect of territorial defense in the early post–Cold War era can no longer continue. All European NATO states (except Belgium and Croatia) spent greater proportions of gross domestic product (GDP) on defense in 2019 than they did in 2014.[3]

The dismantling of the Warsaw Pact and the dissolution of the Soviet Union has shifted the key military focus in Europe from the former West German border to the Baltic region where Estonia, Latvia, and Lithuania constitute a vulnerable de facto NATO "island" directly on the Russian border.

A conflict in the Baltics between NATO and Russia would almost inevitably involve the territory of neighboring non-NATO states Sweden and Finland. Use of their airspace would be key to shielding the Baltic States, or conversely to prevent NATO's access. Consequently, NATO partners Sweden and Finland have reversed their previously declining military expenditure trends in the last few years.

Finland, having won its independence from Russia only in 1917, having suffered a communist-backed civil war and two Soviet invasion attempts since, as well as sharing a 1,340 kilometer long border with its eastern neighbor, is an exceptional case amongst Western European states. It never dismantled its conscript-based military and has the capacity to mobilize over 200,000 reservists should the need arise.[4] Sweden, on the other

Finnish conscripts giving their military oath. They are wearing camouflage uniforms m/91 and carrying Sako m/95 7.62x39 assault rifle (Kalashnikov variant). (Karri Huhtanen from Tampere, Finland)

hand, abandoned its conscript training system for all practical purposes, only to reinstate it in 2018. But Swedish conscription is at present limited, and unlike in Finland, far from universal.

In addition to not having abandoned conscription, the Finnish state also maintained its total defense system—named comprehensive national defense—since 2010. Considering that Sweden swiftly and comprehensively dismantled its total defense system after the Cold War, it is somewhat ironic that Finland's total defense concept was initially inspired by the Swedish total defense system.

With the renewed perception that territorial defense must be the priority for Sweden's armed forces, it logically follows that some form of the total defense concept needs to be reestablished. In the summer of 2016, the Swedish Armed Forces and the Swedish Civil Contingencies Agency published a document outlining a common vision for planning the country's total defense system.[5] Since then planning regarding total defense has been ongoing, including various government commissioned inquiries and a total defence exercise.

In 2021 a government commissioned enquiry presented its recommendations for the organization of the civilian side of total defense , and the government announced that a new government authority for psychological defense[6] was to be established in 2022.[7] Other government enquiries have been commissioned, and are planned, and although miniscule sums compared to the planned military budget the defense budget for 2021-25 does include increased spending on the civilian side of total defense.[8]

Background to the Present Situation Regarding Total Defense

During the peak strength of the Swedish armed forces in the 1960s, with the military possessing 1,000 aircraft and 1,500 combat vehicles, around 850,000 men and women could be mobilized. The mobilized armed forces were to a great extent self-sustaining during the initial stages of a conflict, with an abundance of stores of every conceivable type, and with their own field hospitals, slaughterhouses, field bakeries, and kitchens, etc.

Whereas in the past, the Swedish military was in a position to support society, today the roles have been reversed. At fully mobilized strength, the armed forces today number around 50,000 uniformed personnel, a small number compared to today's Swedish population, which exceeds 10 million inhabitants. The military is also less self-sustaining than in the past, with private companies supplying food services, and reliance on mobilized field hospitals being replaced by a reliance on the regular health system in the case of conflict.

The old total defense system rested on four pillars: military, civilian, psychological, and economic defense. The military's own significant total defense capacity under the command of the military commander in chief, a civilian commander in chief headed the National Board of Civilian Preparedness, and two separate director generals headed the National Board of Psychological Defense and the National Board of Economic Defense.

Of these four pillars, only the much reduced military structure, which was primarily orientated toward foreign operations under UN aegis in the post–Cold War era, remained. This radically downsized military no longer saw a need for self-reliance, as had been the case during the period of focus on territorial defense until the collapse of the Soviet Union. In turn, it became much more dependent upon private service suppliers, rather than maintaining its own extensive in-house logistical capacity.

Yet despite the effective dismantling of many of the structures of an all-encompassing total defense system, a number of the laws granting the state significant rights to commandeer private individuals, firms, and property remain on the statute books. For practical purposes, however,

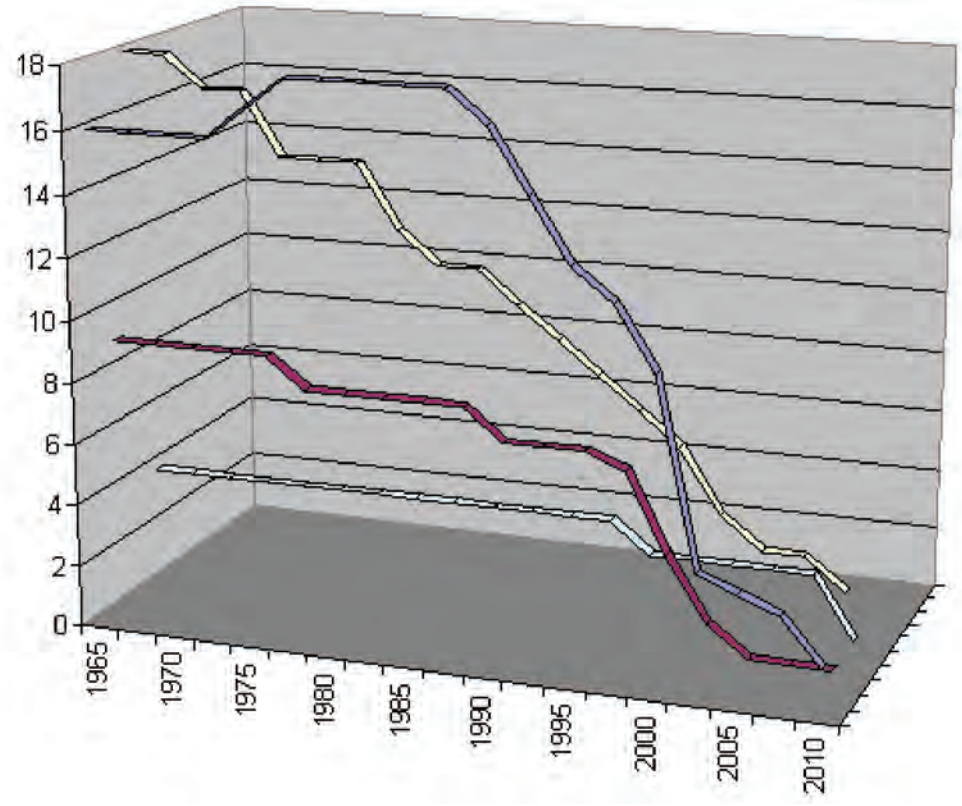


Chart showing the size of the Swedish Armed Forces 1965–2010. Yellow = number of air wings; Blue = number of infantry regiments; Red = number of artillery regiments; Green = number of coastal artillery and amphibious regiments. (Walle83)

without the proper structures and preparedness through regular and extensive exercises, the very wide legal powers enjoyed by the state will be extremely difficult to implement should the preconditions for their use arise. Under present law a state of war, or a government decision to "raise readiness" due to a perceived imminent threat of war, is required for most of these legal instruments to become available to the state.

The more limited powers—available to the state under normal peacetime conditions—do empower the state to place certain demands on private enterprise and to require them to participate in exercises. Yet there are many challenges and uncertainties regarding how this will be implemented in practice considering that the structures for use of such legislation are not yet in place, and a considerably greater proportion of important infrastructure is not only in private hands, but also exposed to much fiercer global competition than in the past. This means that any burdens placed on Swedish businesses without adequate compensation risks hurting the the very enterprises most needed in a robust total defense system.

Lessons from COVID-19

The early stages of the pandemic illustrated the shortcomings in Sweden's national preparedness, which have implications for the future development of total defense:

- When the pandemic hit, several Swedish regions had no stockpiles of personal protective equipment, despite recommendations from the

National Board of Health and Welfare to have such. Stockpiles of a range of other essential items—such as foodstuffs—do not exist either.

- No preexisting structures or preparedness existed to utilize the capacity of domestic producers to start producing essential items such as protective equipment and disinfectants.
- Emergency legal frameworks to facilitate the production of essential items did not exist, but had to be developed during the crisis, such as exceptions or simplifications of complex regulatory requirements required by the Swedish Chemicals Agency.
- Despite reliance on global supply chains, structures for coordination and cooperation proved insufficient, and early stages of the crisis showed that even within the European common market, individual member states blocked delivery of protective equipment en route to Sweden from third countries.
- Beyond handling the threat to life and health posed by the pandemic, the economic consequences of the crisis proved even more significant. Here Sweden was lucky that its relatively recent experience of a financial crisis in the 1990s and the financial consequences of the 2008 Lehman bankruptcy had left an institutional memory enabling it to relatively rapidly adopt measures to prevent an economic free fall. Yet there were aspects of the measures implemented—such as relatively high interest rates for loans offered to firms—suggesting that parts of the response were more of a copy-paste of the last economic crisis, rather than a ready-made and updated solution taken off the shelf for a contemporary crisis.

In short, the pandemic showed in a very concrete way that stockpiles, structures for coordinating private sector efforts, emergency legislation to reduce red tape, and economic recovery plans all need to be in place before a crisis occurs. From the perspective of total defense—where a conflict in the region is the likely scenario—disruptions to society would be much greater than those caused by a pandemic. The shortcomings in the medical field would extend to all critical sectors of the economy, and the economic effect would be of a much greater order of magnitude. Under present conditions, it is very likely that the result of such a scenario would have been an utter collapse of the functionality of the economy.

The utility of Sweden's armed forces—if society ceased to function—would become irrelevant. It is therefore apparent that securing a holistic total defense should be the primary national security priority of the Swedish state. Yet in practice, the Swedish focus the last few years has been too one-sided, rightly reestablishing military territorial defense but neglecting the more comprehensive defense requirements of the economy, upon which the military's functionality is dependent.

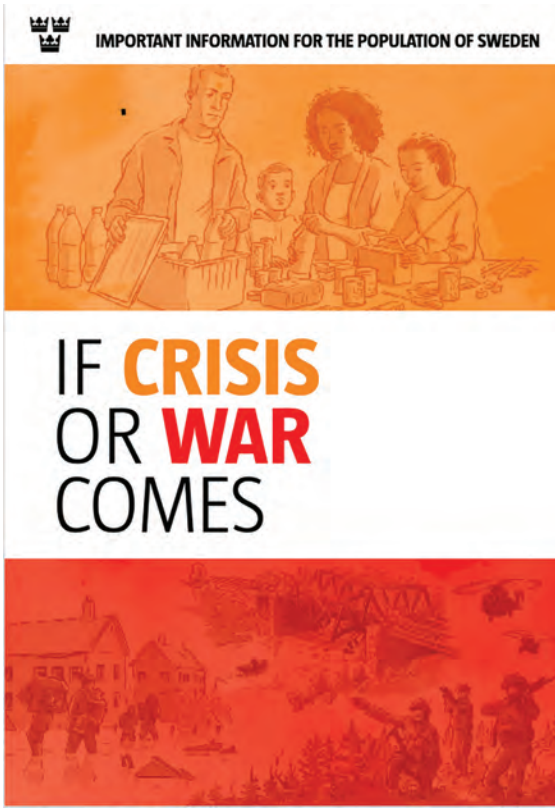
Challenges in Reestablishing a Total Defense System

The Swedish state is committed to the reestablishment of a total defense structure, yet the process is taking a long time—hardly surprising considering the immense complexity of the task.

There are a number of key challenges a state faces in such a process, which are listed below (not in order of priority):

The Inherent Difficulty in Building Up a System Without Setting Goals

Although the Swedish Armed Forces and the Civil Contingencies Agency formulated their common basic vision document for total defense back in 2016, concrete levels of "resilience" (such as stockpile levels and redundancy requirements in critical infrastructure) have not yet been set. Creating a new structure without having a clear goal in mind about the desired outcome is inherently difficult.



If Crisis or War Comes:" pamphlet distributed by Swedish government to every household in Sweden in 2018. (Chris Redan)

A number of government commissions have been established to investigate particular aspects of total defense, but the approach so far has been a patchwork lacking an overarching strategy. Arguably, it would have made more sense to start with a holistic approach, determining what actually needs to be achieved and the overarching structures required to realize this vision, and following that tasking the specific government commissions with implementation. The current approach of starting with the specifics is like putting the cart before the horse—it has made the findings of the commissions less useful, and as the overarching questions have not yet been answered, much valuable time has been lost and the window of opportunity that an opponent can utilize to strike an ill-prepared society will be left wide open for longer.

Outdated Legislative Framework

As mentioned previously though the total defense structures were dismantled after the Cold War, much of the legislation remains on the statute books. In one sense this is positive—at least there are some legal powers that can be utilized by the state—but in practice it contributes to a false sense of security. The fact that the law empowers the state to place significant requirements on both public and private actors does not account for the radical change in how the economy is structured since the introduction of those laws.

Before the end of the Cold War, a much larger proportion of Swedish critical infrastructure was in the hands of public monopolies, including telecommunications, the postal service, pharmacies, the health care system, public transportation, the railways, and TV and radio. Furthermore, most of the energy supply was controlled by the state. Since then privatization, deregulation, and entry into the European Common Market transformed most of these parts of the economy to areas where private actors exposed to competition play a dominant role. Consequently, in the past, large total defense costs for stockpiling, redundancy, and readiness training could be concealed in the operational costs of public monopolies. However, this is impossible in the current reality where private actors exposed to constant transnational competition, is the norm.

Requiring a Swedish company to absorb higher costs due to total defense requirements will make that company less competitive compared to its commercial rivals abroad or at home. Hence, there is a risk that requirements placed on Swedish commercial actors—intended to raise the nation's total defense capacity—would have the opposite effect. Companies may shift production of key materiel out of Sweden if it becomes more expensive. Transportation firms may choose to register their assets, such as lorries or aircraft, abroad to avoid extra costs and regulatory requirements.

This new reality implies that there must be adequate economic compensation for the punitive defense readiness requirements placed on firms.

Expense

If the true costs of total defense can no longer be absorbed by public enterprises, they need to be covered in the government's budget. And not only will significant capacity cost a lot of money, it will also cost much more in the early stages of building new structures to handle stockpiles and creating adequate redundancy in critical capacity. Once established, the annual maintenance costs will be lower. Politically, this is very challenging, since securing financing for temporary high costs is harder than relatively low constant running costs.

Keep It Simple

When new interfaces between the public and private sectors are established to coordinate the new total defense system, it is essential that this is as simple as possible for the private firms involved. The number of public contact points for the firms concerned needs to be minimized—ideally a one stop shop, rather than a jungle of different actors with separate requirements. A firm operating in several locations in the country also needs to be assured that there are standardized solutions developed across the country, so that requirements from different regions, municipalities, and government authorities are as similar as possible.

Such simplicity will not only keep costs down, but since the private sector is the backbone of the economy, it is essential that the firms see their involvement is made as simple as possible. If their contributions are perceived to be overly bureaucratic, complex, and onerous, their willingness to constructively deliver will be undermined, hampering the actual effectiveness of their potential contributions and creating unwilling partners who feel forced to comply with yet another set of unnecessary regulatory requirements. From the perspective of total defense, keeping the morale of businesses up is no less important than keeping the morale of troops in the field up.

Competitive Equality[9]

Simplicity of implementation and adequate cost coverage help facilitate the implementation of total defense requirements in the private sector in a manner that is competitively equal.

As mentioned above, overburdening firms without compensation risks undermining the very firms that total defense relies upon. Yet it is also important to bear in mind that firms should not benefit excessively either. If the state overcompensates a firm by covering costs that would also benefit them versus competitors, that becomes problematic for other firms and the overall functioning of the free market. Therefore, the Swedish Competition Authority should play a key role in ensuring that market interventions seeking to boost total defense capacity are as competitively equal as possible.

To the extent possible, public procurement tenders should be used as a mechanism to secure the contribution of the private sector. In this context, it is important to bear in mind that there should be no discrimination against foreign firms. Not only is it important for domestic firms that there is a level playing field—as Swedish firms provide services and goods to foreign states that have a bearing on their national security—but as a part of the European Common Market, a level playing field is also a constitutional requirement. To ensure this, the state must formulate its tender requirements in such a way that national security needs are adequately met, and the firms participating in a tender must be able to obtain the requisite security clearance where that may be appropriate.

The instinct may be to promote greater national autonomy in certain fields, but the emphasis must be

on ensuring supply chain security. National autonomy for a small economy tied up in a complex web of global interdependence is impossibile. Even if it might be possible in certain areas, it would still leave the nation dependent upon others in several other areas.

International Flows and Integration with Other States

In the past, the total defense approach was to ensure domestic capacity in a range of areas. In the recreation of a new total defense system, the early focus has naturally been on the role of national authorities and key domestic sectors such as energy, transportation, health care, telecommunications, financial services, food and water supply, and security services.

This focus is logical, but the challenge is to integrate the complex international requirements in existing—as well as future—structures that are by their very nature state-centric, focusing on international capacity when cross-border flows are, in several cases, even more important.

Since 2009, Nordic cooperation on crisis preparedness has been formalized around ministerial meetings within the so called Haga-initiative. This is positive but insufficient, and cooperation must be both deepened and extended beyond the immediate neighbors to include key trade partners. In January 2021, the Swedish and Finnish governments endorsed a high-level binational initiative to train public and private sector representatives in crisis preparedness and civil defense (as well as to identify areas of future development), which was another movement in the right direction, but still a baby step toward what is ultimately needed.

New forms of transnational cooperation are needed. These will require deeply institutionalized cooperation, likely hosting personnel from other states inside Sweden, as well as posting Swedish representatives abroad, embedded within foreign government authorities.

Political Ownership

The reality for top-level political decisionmakers has changed in the past few decades. Not only has the complexity of society, and its web of intricate interdependence, increased, but so has technological complexity and the speed of information flows. Whereas in the past, a high-level political executive might have had both less complex issues to handle and more time to focus on them, today's more complicated challenges and the urgency of the 24-hour news cycle make it abundantly clear that even the most competent statesman is hard pressed to cope without an adequate structure in place, including collecting a holistic synthesis of a complex picture and distilling this down to key strategic decisions that need to be addressed by the political system. Without such a structure—which appears to be lacking—there is unlikely to be informed strategic leadership at the highest level, something that has certainly been absent in Sweden these last few years.

At the same time, the budget challenge prevents genuine political interest in addressing the problem, as the focus is on the next election and ensuring that adequate resources are directed toward policy areas most likely to win elections, rather than securing society against threats that are deemed unlikely by politicians (and the public) to actually constitute a clear and present danger.

In the Swedish case, the responsibility of the civilian side of total defense lies under the justice ministry, which is also the ministry responsible for crime prevention. As Sweden has seen an enormous upswing in the number of public shootings and criminal use of explosives in the last few years, the political attention span has been preoccupied by these pressing challenges that dominate the headlines, likely stealing attention from total defence.

Peacetime Domestic Security

Although Sweden is still a relatively peaceful society gang shootings and explosions are now more

common. The police estimate 5,000 members of criminal gangs are in residential areas deemed "vulnerable." Non-ethnic Swedes are playing a dominant role in much of organized crime, and this has raised the prospect of crime becoming an instrument of foreign powers.

The growth of Islamist groups with international connections, extremist nationalist groups (of which some members have received weapons training in Russia), and left-wing radicals also threaten disruption. Consequently, ensuring domestic stability has become a much more important component of total defense than it was historically.

The police established the new temporary border control at, among other places, Hyllie station in Malmö. (Johan Wessman)

The transformation of Swedish society, with decades of large-scale immigration, has made it much less homogenous than before, and created new tensions to be exploited by foreign influence operations. As in all open societies, media consumption patterns have also been revolutionized. In the past, the state's monopoly on television and radio broadcasts, and the limited number of national daily newspapers meant that there was a fairly homogeneous view of societal developments and the outside world. With alternative media now complementing mainstream media, social media as a new form of information dissemination, and the easy availability of international news sources, society has become much more fragmented from an information consumption perspective, leading to a greater polarization of views, and making the job of psychological defense much more challenging.

The increased presence of populations originating in countries such as Russia and China also implies new security challenges. In 2019,[10] there were over 22,000 persons born in Russia living in Sweden, and over 35,000 born in the Peoples Republic of China. The total number of people with connections to these countries grows if those born to parents originating there, or if ethnic Russians from the former Soviet Union are included. Furthermore, much larger numbers of residents have origins in countries such as Iran and Syria, which are on friendly terms with Russia and China. Over 80,000 Swedish residents were born in Iran, and over 191,000 in Syria in 2019.

Economic Integration with Potentially Hostile Powers

During the Cold War, economic interdependence with the Warsaw Pact and other Communist regimes was limited. Today, economic interaction with China in particular, is vast, both in terms of trade and investments. Economic exposure to Russia is much more limited, but over a quarter of Swedish crude oil imports originate from the Russian

Federation. Total trade with Russia was worth almost 60 billion kronor (Swedish currency, SEK) in 2019, and trade with China approached 150 billion SEK, close to the value of trade with the United States, which slightly exceeded 160 billion SEK.

A Swedish Defence Research Agency report from 2019 identified 51 majority acquisitions and 14 minority stake acquisitions of Swedish firms by Chinese firms since 2002.[11] Several Swedish firms have production in China, and many more are dependent upon Chinese suppliers. Chinese firms have also been free to participate in infrastructure bids in Sweden—not least Huawei as a leading supplier to telecom operators.

Although Sweden has been slow to react to this new reality, new legislation implemented in 2019 empowered the state to block the transfer of ownership of certain assets on security grounds. Signalling a new security consciousness relating to the role of foreign companies, the Swedish Post and Telecom Authority decided to exclude Chinese firms from participating in developing the country's 5G networks in October 2020, a move that has been criticized by the Chinese Government and by the affected companies who have challenged the decision's legality.

Yet the assessment of the strategic implications of deep economic interconnectedness with the world's most powerful authoritarian state is still in its infancy. Heavy economic exposure to China, and Sweden's economic dependence on international trade, will guarantee a conflict of interests in balancing security concerns against perceived economic gains.

Transparency in an Open Society

Sweden rightly prides itself on being a highly open and transparent society, but this transparency creates an asymmetry potentially benefitting an adversary. Open intelligence collection, facilitated by digitalization, empowers foreign powers to map individuals, firms, and public authorities.

New, smarter approaches must be developed to secure the benefits of societal transparency while protecting against the digital vacuuming of public data that can be used against society or for targeting individuals or firms by states or criminals. In Sweden—unless an individual enjoys protected identity—a citizen's address, vehicle type, income, convictions, and much more detailed information are instantly available online.

Possible Solutions

Although the challenges in building up a total defense structure are numerous, there are a number of take-aways from the above that would help Sweden or other countries intending to implement a new total defense structure to move ahead more effectively. These possible solutions are not listed in any order of priority.

Setting the Bar Before Real Work Begins

A group of senior civil servants, business leaders, and politicians, with support of several staff, should be commissioned to develop an overall total defense concept and set goals for what the future total defense structure should achieve. Once the overall ambition is set, the government commissions can work out the details of implementation. In Sweden, either this has not yet been done or it has been done poorly.

Develop Exceptional Funding Mechanisms

The unavoidable reality, as has already been mentioned, is that building up a total defense structure is going to cost a lot of money—at least if it is to have any real effect. The COVID-19 pandemic illustrated that when the problem is acute, the state can make large amounts of money available. In the case of Sweden, the government debt levels are still low—26 percent of GDP at the end of 2020[12]—much lower than the Organization for Economic Cooperation and Development average. As it concerns national security, one solution would be an exceptional

debt financing for total defense costs. The political danger of this solution of course is that the political parties will then want to use similar funding for all sorts of unrelated "investments," opening a Pandora's box of fiscal irresponsibility. An alternative solution would be a total defense or "readiness" fee, the revenues of which are allocated to financing total defense costs, such as exists in Finland. In the case of Finland, the fee is placed on energy sales, but it is not the only revenue generated for the Finnish National Emergency Supply Agency. The Agency, which is technically not a government agency, also generates revenue from commercial holdings, so it receives its financing independently of the state budget, allowing the agency to operate outside the EU framework of state aid restrictions. Whether the Finnish solution is practical in the Swedish case is potentially doubtful as the Finns set up their system in conjunction with their EU accession. If Sweden were to set up a similar system—as long-time members of the EU—it might be construed as an effort to consciously circumvent EU state aid rules. The fact that the Finnish National Emergency Supply Agency is maintaining an existing system also means that it does not have the Swedish problem of needing to ensure very large funding at the early costlier stages of creating the structures of total defense.

The proposed budget allocations for total defense from 2021 through 2025 are such that allocations to the civilian side are disproportionately small compared to the military allocations. In 2025, the proposed military budget will be more than 20 times greater than the funding for the civilian side.

Consequently, some sort of loan structure appears to be necessary, as the political reality will almost certainly ensure that sufficient funding will not be secured through the regular government budget.[13]

One Bite at a Time

The old total defense system did not appear all at once; it evolved over time. Likewise, it would be unwise and unmanageable to try to implement new total defense structures all at once. It would be logical to start with the most acute needs first. Considering that even basic emergency response structures are insufficient or lacking, fixing these would be a good place to start.

Address the Organized Crime Problem

Organized crime has grown to such an extent that it constitutes a potential threat to national security and stability. Robust crime prevention strategies should therefore be seen as an integral part of total defense efforts. These efforts also enjoy the advantage of delivering value even if a future conflict or crisis does not materialize. Crime prevention expenditure should furthermore be politically easier to justify politically than most other areas of expenditure relating to total defense.

Create a Well-Staffed National Security Council and a New Agency for Total Defense

The Swedish governance model with small ministries and large and independent government agencies has some advantages but it does not facilitate effective coordination between the different arms of the state.

A proper national security council would fill an important function by ensuring that the nation's leaders have to take proper account of security dimensions of their decisions. It could furthermore ensure that the independent government authorities take action based on an informed holistic security assessment, reducing the risk of individual authorities operating as if in uniform silos focusing autistically on their own narrow remits.

A new authority responsible for the coordination of total defense, with clear powers to influence other authorities, would also be a prerequisite to ensuring all authorities act in a coordinated manner. Presently no such authority exists. The closest thing is the Swedish Civil

Contingencies Agency, but this agency has an enormously broad range of responsibilities preventing its leadership from adequately focusing on total defense. Furthermore, it lacks power of command over other government agencies. (Note: a government commission of enquiry recommended in 2021 that the Swedish Civil Contingencies Agency should be given broader powers.[14])

Focus on Problematic Firms

International interdependence is a fact and it is a strength that Sweden contributes to the security of other states. New restrictive and cumbersome legislation that complicates foreign firms' participation in total defense would add a further layer of regulatory burdens on firms. Rather the focus must be on identifying those particular firms where foreign ownership is considered problematic from a security perspective. The crass reality is that there are firms that could be swayed by foreign or domestic hostile actors. Hence, the reliance should be on security agency assessments of individual firms in sensitive sectors or those bidding to participate in related bids. Key personnel or owners need to be screened, and legal mechanisms developed to exclude potentially problematic actors on security grounds. This will be much more effective and pragmatic than onerous regulatory hoops that are applied to all firms.[15]

Take Political Responsibility for Social Media Regulation

It is a positive development that a recent government commission of enquiry proposed the creation of a new government authority for psychological defense, something that has been lacking since the abolition of the former National Board of Psychological Defence. The new agency will, according to a government decision, start operating in January 2022.

With digitalization and transformation of the media landscape, social media platforms have grown to become a new critical component of information operations. So far, the Western approach to social media platforms has largely been to abdicate political responsibility and rely on self-regulation. This is unsustainable. Regulating social media is inherently difficult and raises several dilemmas concerning the right to freedom of speech in open societies. However, it is far more democratic to have clear and transparent rules set by parliaments than to rely on opaque decisions by corporate giants primarily driven by commercial interests, which may at times be at odds with broader national interests. Consequently, difficult political decisions need to be taken based on broad parliamentary support and clear principles that do not result in outcomes favoring particular ideologies or party interests.

Broaden Conscription

Sweden has already reactivated its military conscription and is set on increasing the numbers of conscripts. This is a necessity as the military was not able to recruit and retain enough soldiers under a purely professional military system.

The civilian side of total defense would also benefit from the activation of civilian conscription. The police force has not achieved its recruitment goals in the past few years; support from civilian conscripts could unburden police officers and personnel with simpler tasks, enabling the force to be more effective in its crime prevention efforts. Staffing of future stockpiling structures could also be partially filled by civilian conscripts, who could also serve to boost resilience in other aspects of critical infrastructure.

Focus on Strategic Resources

As illustrated by the COVID-19 pandemic, states will naturally prioritize securing their own national needs in time of crisis at the expense of other states. A lesson learned from this experience might be that individual states should develop self-sufficiency in every essential area .However, this is an economic impossibility.

The lesson should rather be to understand that if states are primarily driven by self-interest, we need to ensure that we have something to offer in return in order for us to get what we need.

Consequently, a focus on securing stockpiles of critical goods and ensuring enhanced resilience in our critical systems is insufficient. Every state should identify what raw materials, energy supplies, transportation capacity, industrial production capacity, and services will be essential to other states in a time of crisis. That strategic capacity, critical for other states, must be mapped and identified actors should be included among the prioritized sectors where future stockpiling and resilience is to be developed.

The Reality Ahead

Barring unexpected developments, most likely the political will to secure adequate funding for total defense will be left wanting. The rhetorical commitment to building up total defense will remain, but there will be a significant gap between required capacity and actual deliverable capacity. There may very well be efforts to fill some of this gap by placing significant and underfinanced burdens on the private sector. There are significant risks that this approach will result in suboptimal outcomes in sectors exposed to competition—in the worst case actually undermining the desired outcome.

Only clear political ownership and commitment to adequately fund total defense can ensure that the required societal resilience is actually achieved. Consequently, political wishful thinking and delusions that legislation can force the private sector to fulfill what is the core responsibility of the state constitute the greatest threats to the future of the Swedish total defense project. PRISM

Notes

[1] Even states predominantly concerned with power projection capacity, rather than national territorial defense, need to consider a comprehensive defense approach, lest a distant enemy disposes asymmetric means to strike at the homeland, which could threaten both the ability and will to actually deploy military force. The advent of the nuclear missile was a paradigm shift in the sense that, in the case of a nuclear war, the United States was no longer a strategic island. Today the vulnerabilities due to digitalization and precision munitions imply that even under a much lower conflict threshold, America can no longer be considered a strategic island. Expeditionary conflict far afield could imply highly destructive strikes against homeland infrastructure. Without adequate comprehensive defense structures, even the military credibility of a superpower would be in doubt.

[2] Sarah Repucci, A Leaderless Struggle for Democracy, Freedom House, Washington, DC, 2020, available at <freedomhouse.org/report/freedom-world/2020/leaderless-struggle-democracy>.

[3] NATO, "Defence Expenditure of NATO Countries (2012–2019)," press release, June 25, 2019, available at <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/20190625_PR2019-069-EN.pdf>.

[4] "Europe," in *The Military Balance 2020* (Washington DC: International Institute for Strategic Studies, February 2020), available at <https://www.iiss.org/publications/the-military-balance/military-balance-2020-book/europe>.

[5] Swedish Armed Forces and Swedish Civil Contingencies Agency, "Sverige kommer att möta utmaningarna: Gemensamma grunder (grundsyn) för en sammanhängande planering för totalförsvaret (translation: Sweden will meet the challenges: A common foundation for a cohesive planning of total defense)", June 2016, available at https://www.msb.se/contentassets/f1298afdc0b1489eb4262d8ccbb63c86/sverige-kommer-att-mota-utmaningarna-2016-06-10.pdf.

[6] Swedish Government Offices, Ministry of Justice, "Struktur för ökad motståndskraft (translation: Structure for increased resilience)", April 2021, available at https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/04/sou-202125/.

[7] Swedish Government Offices, Ministry of Justice, "Inrättande av Myndigheten för psykologiskt försvar (translation: Establishment of the Government authority for psychological defense)" March 2021, available at https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2021/03/dir.-202120/.

[8] Swedish Government Offices, "Totalförsvarsproposition 2021-2025: inriktning av Sveriges försvarspolitik (translation: Total defence bill 2021-2025: focus of Swedish defense policy)", accessed on 25th August 2021 https://www.regeringen.se/regeringens-politik/forsvar/totalforsvarsproposition-20212025---inriktning-av-sveriges-forsvarspolitik/.

[9] The term *competitive neutrality* is usually used instead of *competitive equality*, but as the word neutrality might be misunderstood in the context of security and international relations, the word equality has been used instead.

[10] Statistics Sweden, "Befolkning efter födelseland och ursprungsland, 31 december 2020, totalt (translation: Population according to country of birth and origin, 31 december 2020, total)", december 2020, available at https://www.scb.se/hitta-statistik/statistik-efter-amne/befolkning/befolkningens-sammansattning/befolkningsstatistik/.

[11] Jerker Hellström et al, Kinesiska bolagsförvärv i Sverige: en kartläggning (translated: Chinese business acquisitions in Sweden: a survey), Swedish Defense Research Agency, November 2019, available at https://www.foi.se/rapportsammanfattning?reportNo=FOI%20Memo%206903.

[12] Christian Holmström, "Central Government Debt," Economifakta, August 6, 2021, available at <https://www.ekonomifakta.se/fakta/offentlig-ekonomi/statsbudget/statsskulden/>.

[13] This is not so say that a loan based solution is the ideal solution. The optimal solution would probably be for government to cut budget expenditure in other areas in order to enable increased expenditure on total defence without increasing net expenditure. Such austerity particularly desirable in the case of a country like Sweden that already has one of the world's highest tax burdens.

[14] A government commission presented its recommendations relating to the governance and coordination of the civilian side of total defense in March 2021. Among the commission's reccomendations were that the Swedish Civil Contingencies Agency should assume broader responsibilities for total defence, including the overall responsibility for planning civil defense, compiling overall resource requirements, supporting other government authorities in times of crisis and heightened readiness.

[15] A government commission of inquiry it currently looking into a screening mechanism regarding aqusitions of potentially national security related businesses.

"I dreamed about a human being." (Collage By Fran Simó)

Project Governance for Defense Applications of Artificial Intelligence

An Ethics-Based Approach

By Brian T. Molloy

The recent Department of Defense (DOD) Artificial Intelligence (AI) strategy calls for the Joint Artificial Intelligence Center (JAIC) to take the lead in "AI ethics and safety."[1] In line with this directive, the JAIC and the individual services must develop a coherent ethical review process to identify and mitigate potential ethical risks during project development. To date, the U.S. Defense Innovation Board (DIB) has handled much of the DOD emphasis on AI ethics culminating in the publication of its AI principles report.[2] Although it provides guideposts, it does not necessarily generate actionable controls to limit ethical risk on individual projects. The challenge for the department is to generate a project governance architecture that adequately addresses these ethical risks while also reaping the considerable benefits of AI. This article provides recommendations for implementing project governance controls based on an ethical framework while providing tailorable solutions to tightly control those projects with high ethical risk and speeding the implementation of those with low risk. In this way, a tiered approach to project governance will allow the Department to more closely balance the ethical challenges with the need for efficiency in the development of this technology.

Not all AI projects carry the same ethical risk, yet DOD currently lacks a formalized process to delineate and separate projects by ethical risk or consequences or both. Currently, the Department draws a distinction between Lethal Autonomous or semi-autonomous Weapons Systems (LAWS)[3] and those that are not autonomous weapons systems, yet there is more distinction that needs to be made in order to adequately identify the risks associated with the technology. In tiering out risk categories, the Department can focus resources to review and limit ethical risk on those projects most likely to cause ethical dilemmas while accelerating those identified as low consequence. It should be noted that all projects pose their own unique ethical concerns and that there is no one-size-fits-all policy that can be applied to limit all potential ethical challenges across the broad array of projects being pursued. To address such a fundamentally important issue, this article proposes a business process that can identify ethical risks and then mitigate them appropriately, according to their relative risk.

The Defense Innovation Board AI principles report detailed 12 specific recommendations for DOD to focus on to manage ethics in AI.[4] This article focuses on two of these recommendations and proposes

MAJ Brian Molloy is the Deputy Director of Engineering at Joint Task Force - Bravo in Soto Cano Air Base, Honduras. He is a graduate of the U.S. Naval War College where he studied the Ethics of Emerging Military Technology and other defense issues.

project governance solutions to address these challenges and translate them into concrete project governance controls. First, in line with the DIB's recommendation to create a risk-based management methodology (DIB recommendation #9), this article proposes using risk-based screening criteria to separate and tier projects based on their ethical risk. This approach allows for more stringent controls on projects of high risk, while speeding through projects of low risk. Second, the article builds on the risk management tiering framework and uses this framework to provide recommendations on AI reliability benchmarks (DIB recommendation #7).

AI as a Unique System Enabler

Artificial Intelligence, as an enabler to weapons systems, is unique in its ethical concerns and considerations and warrants a new screening approach outside of those in normal acquisition channels. Unlike other weapon systems, in AI/Machine Learning (ML) projects the end use and development of the product are more closely linked. That is to say, when using AI in a weapon system, the developer will, by design, make some choices that under conventional applications would be left to the end-user. These choices are not necessarily self-evident but are emergent based on the decisions made by developers about the boundaries and rules developed within a particular algorithm. Much has been discussed regarding potential ethical issues with ceding decision-making to AI algorithms.[5,6,7] The question becomes, can we control those decisions and bound them appropriately so that we can control the ultimate end use of the system?

Traditionally, ethical controls on technology were inserted through policy constraints on end-use. However, the relationship between developer and end-user is shifting the ethical burden backwards towards the developers. This shift necessitates a new approach to managing ethical issues. It is simply not sufficient to place policy constraints on end-use. In order to adequately mitigate ethical risks with this technology, policy controls to adjudicate ethical challenges must be applied at the outset, during the design phase, and then continued during development.

This relationship between end-user and developer will be further strained by the movement from narrow AI towards more complex adaptive systems. In the traditional designer-user relationship, the design engineers allowed themselves a certain level of plausible deniability as to the intent of the end product. In effect, the engineers could pass off the ethical dilemmas to the end-users and force them to make the hard decisions. As systems become more automated, however, it will force engineers and therefore policymakers to be more upfront with the potential ethical challenges of end-use. This problem emerges from the fact that the actions of the system will be bounded by the parameters of the design engineers. In simple mechanical systems, all decisions regarding use are made by a human operator, thereby all moral decisions regarding use or non-use are pushed to the user based on context and surroundings. In highly automated systems, however, those decisions must be made by the engineers on the front end. Therefore, during the development of each system, a program of identifying risks and consequences must be developed and then implemented through both internal controls in the algorithm and external controls through policy constraints.

AI-enabled systems must be viewed through the lens of a moral agent. That is, a system that on the one hand, does "not necessarily exhibit…free will, mental states or responsibility," but on the other hand is an entity that performs actions.[8] It is these *actions*, that have ethical ramifications. The moral decisions are not made by the machine, they are made by the design engineers, and the machine is merely the agent that carries out the action expected of it. Therefore, it is here, in the development stage, that the focus of project controls and

U.S. drone attack on the convoy of the Iranian general Qassem Soleimani, 3d render. Baghdad airport, Iraq.

project governance must lie in order to effectively manage ethical risks. The most effective way to achieve ethical behavior by a moral or ethical agent would be to ensure that the outputs of the machine are constrained to avoid unethical outcomes. This could be accomplished by creating the boundary states that implicitly support the ethical behavior of the machine by not allowing the system to conduct actions that are outside of the ethical framework.[9]

An AI Ethical Risk Management Methodology

From a policy perspective, the focus of ethically applying artificial intelligence to weapon systems needs to focus on defining the boundaries for the given technologies. This article relies heavily on the utilitarian approach to ethical issues, or the view that the morally correct action is one that produces the greatest good. There is a practical reason for this. The utilitarian approach focuses on weighing risks with consequences and tends to be the approach that is most easily quantified and measured.[10] Using this approach allows program managers and policymakers the ability to make rational decisions regarding the potential risks of the technology and to make informed mitigation decisions. It is important to note that this does not foreclose the use of other applicable ethical lenses, yet it provides a clear way ahead for providing policy guidance to the development of these technologies.

The two major recommendations for consideration in risk management are discussed below. First, project acceptance criteria must be adopted in order

to initially identify the initial ethical risk and determine boundary conditions for development. Second, projects cannot be evaluated in a one-size-fits-all approach; a consequence-based project tiering must be developed which separates projects based on potential consequences and applies additional controls to those of higher consequence while allowing those of lower consequence to be moved through more quickly.

Tiering of Projects Based on Ethical Risk

The process of tiering projects for ethical risk must begin with an initial screen for ethical issues in development. Applying a utilitarian perspective, if the project's expected benefits outweigh the potential risks within the proposed boundaries, the project then may be continued for development. If the project fails to meet this test, the Department can choose to limit the boundaries of the project to a more tightly controlled problem set until the ethical balance is achieved or until the project is deemed to be irreconcilably unbalanced and discarded. Importantly the output of this initial screen should be codified in an official document such as an "Ethical Issues Report" which would determine initial bounds for development, and this report would then be updated during project execution with additional controls based on more in-depth analysis explained below.

This initial screen of projects is likely already occurring in an informal fashion, yet a formalized procedure would force the Department to codify and document guidance to program managers within the services and to continue in an institutionalized fashion the ongoing identification and mitigation of emergent risks throughout the lifecycle of projects.

Only once the risks are identified can controls be applied within the identified boundary states in order to ensure that ethical risks are effectively managed. Each project must be tiered out based on its consequence level, then scored against its potential risks. Because some risks are more relevant than others based on project consequences, a risk relevancy matrix has been developed to assist with screening project risks. The matrix presented below can be used to ensure that ethical risk management strategies are being applied appropriately based on the type of project associated.

Table 1: Risk relevancy matrix

	Consequence Tiering Level	Ethical Risk Relevancy Matrix				
Tier 1	Lethal Autonomous or Semi-Autonomous Weapons System	High	High	High	High	Low
Tier 2	Targeting information Systems	Moderate	Moderate	Moderate	High	Low
	Safety-Critical Systems	High	High	Moderate	High	Low
Tier 3	Privacy concern systems	Moderate	Moderate	Moderate	Moderate	High
	Business Process systems	Low	Moderate	Low	Low	Low
		Technical Safety	Malicious-Unintended Use case	Algorithmic Bias in data set	Algorithm training Risk	Excessive collection risk

The recommended consequence categories to be developed are: lethal autonomous or semi-autonomous weapons systems, targeting information systems, safety-critical systems, privacy concern systems, and business process systems. Those categories are then tiered to determine additional controls on projects. Tier one projects should already be identified and by Department policy are to be managed in accordance with DODD 3000.09 Autonomy in Weapon Systems.[11] Tier two projects include all projects that result in targeting information and projects that have a significant safety risk. These projects must be screened for ethical risks based on the risk categories in the table and outlined below. The risks should then be formalized and mitigated through a formal risk management procedure overseen by the AI Ethics Committee.

The recommended risk categories to be scored against are technical safety risks, malicious/unintended use case risks, algorithmic bias in data set, algorithm training risks, and excessive collection risks.[12]

1. Technical Safety: The first question for any application is whether it works as intended over time and in various expected applications. The question of the reliability of the system in context is a significant issue in AI systems. This technical safety risk is especially acute in that in a contextually sub-optimal state a system may perform an unexpected action resulting in an unethical consequence. This problem is generally mitigated through a rigorous test and evaluation process; however, for AI/ML or other complex adaptive systems, this process is challenged as discussed below. These technical safety/reliability risks pose a significant ethical concern, in that the system can only be ethically employed if its output is sufficiently known by the operator. The limitations of this technology must be well communicated to the operator in advance of the decision to employ it. Unreliable systems pose a challenge to this dynamic in that the operator may believe it to be operating normally when it is not.
2. Malicious/Unintended Use Case Risks:[13] The second risk to be analyzed is the unintended use case risk. This risk applies to a properly functioning system that is used in a way outside of the expected or approved usage. In this case, an ethically responsible application could be co-opted by end-users for potentially unethical consequences. A detailed review of possible use cases should be conducted to identify and mitigate the possible unintended uses.
3. Algorithmic Bias in Data Set: One challenging aspect of neural networks is that the data that is used to generate the outputs are generally created and curated by humans who harbor inherent biases. These data sets by their very nature have the possibility to produce unintended results. In this case, it refers to the fact that the algorithm will reflect the implicit values of the person who developed it. This is the one ethicists have focused on the most. These biases are then broken down into three subcategories or more depending on the author; pre-existing bias, technical bias, and emergent bias.[14] These biases have been in place in software engineering well prior to the advent of AI but remain significant in the use of AI.
4. Algorithm Training Risks: One major risk in this category for military applications lies in insufficient datasets to train ML algorithms on. In the case of military applications, there are simply not the number of examples that would provide the necessary context for an AI algorithm to operate in varying environments. The mitigation for this risk has primarily been to create synthetic training environments for the algorithms to operate in. The challenge with this approach is that the synthetic environment will likely not be an exact match for the

operating environment out in the world. This mismatch has the potential for the algorithm to operate outside the bounds intended.

5. Excessive Collection Risk: Algorithms that autonomously collect and analyze data have the potential to excessively collect data beyond the scope of the initial application. This excessive collection has the potential to cause privacy or even legal challenges in the use of the technology. This risk is especially prevalent in the use of AI in the cyber domain, where the data on networks is not well defined in terms of ownership or nationality.[15]

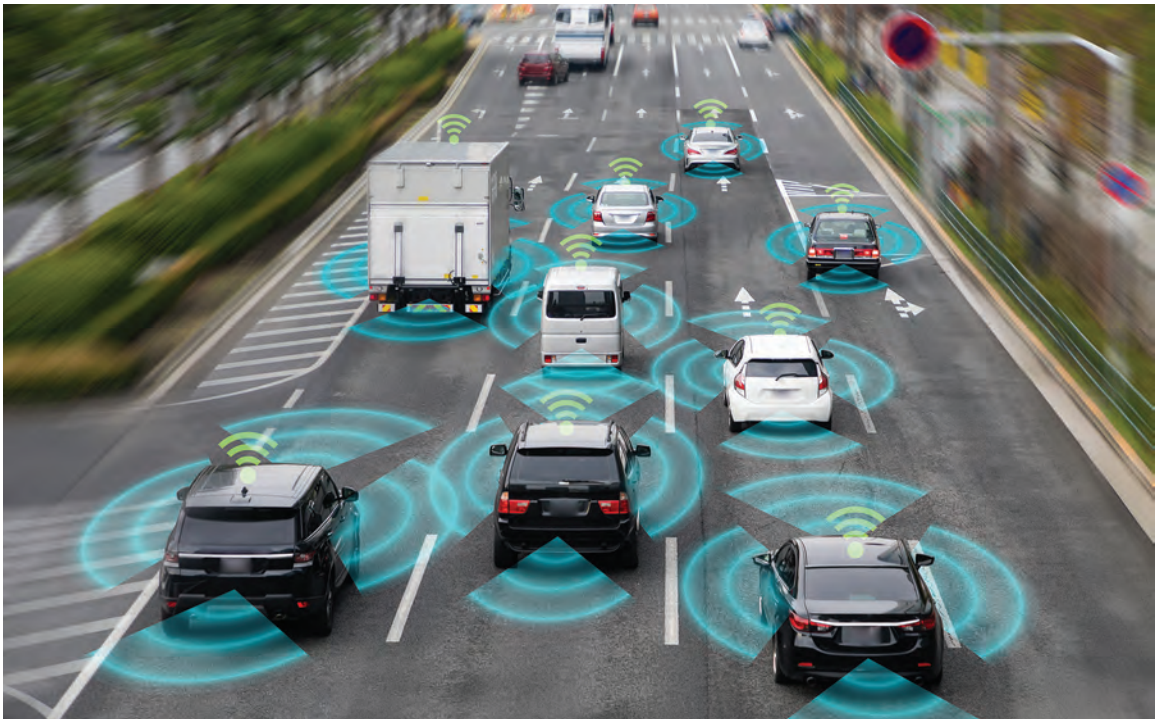
Reliability Benchmarks for Defense AI Applications

Reliability benchmarks remain one of the major unanswered questions for the development of AI-enabled systems within the DOD. AI has the potential to revolutionize the way the Department does business, but as with each new technology, there is risk associated with the adoption and widescale use of the new technology. By codifying hard reliability benchmarks, the Department can formalize the risk acceptance for developers. Likewise, defining reliability will give end-users the opportunity to understand the limits of their respective systems with greater fidelity. With this understanding, the DIB AI report recommended developing AI performance benchmarks relative to human performance.[16] The approach of tying reliability to human performance is not new; the same approach has been taken in many other industries, most notably the self-driving car industry. The DOD, however, has unique challenges that will compound the difficulty of achieving these same standards for benchmarking. For DOD applications, simply addressing whether an AI-enabled system performs better than a human analog is an insufficient approach to manage the risks associated with AI-enabled systems adequately.

Again, a tailored approach should be taken in order to manage the risks appropriately based on the risk for each application. This article proposes the use of three separate benchmarks, aligned against the project consequence tiering criteria introduced previously to more closely align the performance requirements with the potential for unintended consequences. It should also be noted that the research into AI reliability benchmarking is extremely new, and therefore there is a dearth of published industry standards or academic research on which to rely. The self-driving car industry appears to be the furthest along in this effort, but even here, many different approaches are being adopted with no single standard accepted as the norm. Some standards, such as ISO 26262, have developed highly strict standards that state that a car can only make 10 mistakes for each 1 billion hours of operation while humans are expected to make 10,000 mistakes in the same period of time.[17] Yet even this ISO standard has not been widely adopted. In this environment, applying policy ecommendations remains a challenge yet is imperative to ensure the continued viability of this technology.

Technical Challenges in Reliability Benchmarking

The unique environment that the DOD operates in compounds the problem of applying appropriate reliability benchmarks like those in other industries. The DOD environments for which AI-enabled systems are being developed are in many instances high-consequence while at the same time low frequency. The high-consequence nature of the systems will require extremely high reliability, while the low frequency of such events creates a data deficit challenge. This deficit makes it difficult to adequately train algorithms to match, or exceed, human performance. For a moment, let us consider the self-driving car industry as an analog for a high-consequence complex adaptive system. For this industry, human performance is relatively well known, and vehicle



Sensing system and wireless communication network of vehicle. (Metamorworks)

fatality data is readily available. In 2016, for example, there were 1.16 fatalities for every 100 million miles driven. To adequately field test an AI-enabled autonomous driving system to reach 95 percent reliability in comparison to human performance, the vehicle would need to be tested for 255 million miles with no accidents.[18] This standard is extremely difficult to achieve for self-driving cars even in such a data-rich environment. The self-driving car industry is one that is high-consequence but also high frequency. Yet even in this industry, novel approaches are being made in order to ensure reliability that approaches or exceeds human performance. Even in such data-rich environments challenges exist in generating data to match human performance, and the industry has begun to rely on a significant amount of synthetic data, or data that is created in a simulated environment, in addition to real-world test miles. In this industry, the standard approach uses a vast amount of raw data in order to ensure reliability.

Contrast this to a combat environment, where the accumulation of data is incredibly difficult. The environment is extremely data-poor, resulting in a significant challenge for field testing to determine system reliability.[19] Self-driving cars may see hundreds of thousands of examples of stop signs in all manner of environments, orientations, partial obscurations, and defacements during field testing. Combat vehicles will not have such data available. Consider for a moment a Russian T-90 Armada tank. How many examples would it take to achieve human parity with the identification and classification of such a threat enemy combat system? Now let's consider the number of cases where field testing data can be developed. The number of actual meeting engagements with Russian tanks as example data is infinitesimally small compared with the number of stop signs. Many novel training approaches are being developed to address this problem, including synthetic

or simulated training environments, but these approaches engender their own risks.[20]

Applying a human condition as a benchmark is likewise equally challenging. Indeed, for each system, the failure rate of humans must first be measured and then translated into requirements for the machine to be benchmarked against. The measurement of such failure rates could be incredibly difficult and, in some cases, misleading. In many cases, this type of analysis falls victim to what is called the "human filter pitfall."[21] In these cases, using human failure rates as a benchmark against machine performance can be challenging because humans and machines perceive their environment in different ways. Machines and humans operating in the same environment may have wildly different failure rates based on their respective limitations. In many cases, the machine may perform exceptionally in areas that humans routinely fail at and thus meet the reliability benchmark, yet routinely fail at other common tasks that humans do not find difficult.[22]

Additionally, the ability to accurately measure human performance, or even to determine what parameters human performance should be measured against, is difficult. Consider again the same ML algorithm designed to identify T-90 tanks for a ground combat system. How do we determine *human* reliability benchmarks for this relatively narrow task? Since the current physical training environment is data-poor, that is there are very few actual T-90 tanks for soldiers to look at in person, the average soldier is essentially trained on flashcards of T-90 tank photos. We could, therefore, base the reliability standard on the average soldier's ability to accurately identify T-90 tanks in these photos in various environments. Yet when the soldier, or the ML algorithm, encounters this in the field, the reliability changes dramatically. A soldier under the stress of combat will have remarkably different reliability in this task.[23] Indeed, the soldier in the rush of combat may not see the tank at all, an error of omission. Or they may commit errors of commission, that is, misidentify friendly tanks as enemy or enemy tanks as friendly. In other cases, the soldier may identify the tank, but choose not to engage due to some other reason. Perhaps the proximity of non-combatants, perhaps there were other nearby targets or other indications that the tank was not a threat. In these cases, measuring human reliability becomes increasingly challenging. Determining what metric to use as a *human* performance standard must be addressed along with the reliability standards for machines.

Social Acceptability of Reliability Benchmarks

The public's willingness to accept technological change further exacerbates the policy risk that mistakes may impose for the use of this technology. Indeed, any discussion of reliability ultimately can be distilled into a discussion of risk and risk tolerances. Defining a reliability metric that constrains the use of technology in only those cases where it will always outperform a human is one approach to limit risk and manage the risk tolerances of the public. Yet the risk tolerances of the public are not entirely rational. In many cases, the public appears to have a lower risk tolerance for technologies that retain certain characteristics. In some cases, this manifests as technologies that generate visceral emotions.[24] In others, the effect is seen where mistakes cannot be easily explained.[25] In all of these cases, the perceived risk tends to skew much higher than the actual risk.[26] Several heuristics account for the risk perceptions being skewed that are particularly relevant to AI technology. This effect is even more pronounced with new or novel technologies that are not easily explained; this effect has been labeled as "new-risk."[27] This new-risk phenomenon is particularly relevant for AI-enabled systems. A significant perception exists that AI is such a new and untested technology that it simply cannot be trusted, especially in applications with high-consequence. This fear tends to outweigh opinions on the suitability for the application even when presented with

evidence that the technology will ultimately save lives.

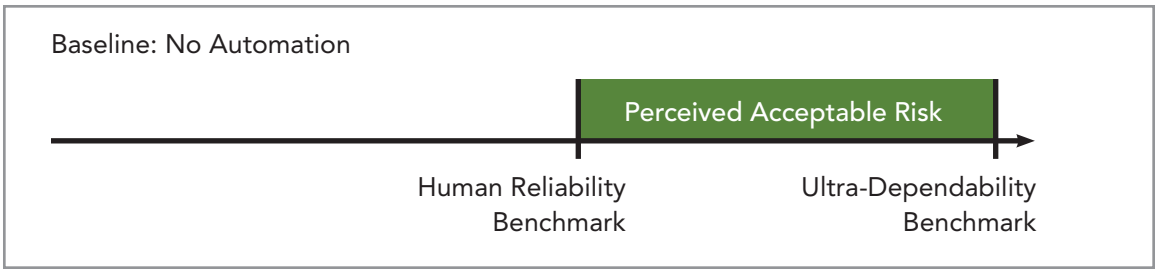
The other relevant heuristic appears to be what is known as "Unnatural or Immoral risk." In other words, technologies that are deemed to have high ethical risk are viewed as riskier than those of other types of risk. This immoral risk phenomenon originated in the nuclear industry,[28] but can easily be extrapolated to other novel military technologies that were ultimately deemed immoral. Many have said that military applications of AI will also fall into this same category. Global movements against autonomous weapons systems are prime examples of the immoral risk perception that accompanies AI in the military sector.[29] It should be noted that the resistance to autonomous weapons systems has followed the reasoning used for the banning of other novel technologies deemed immoral, namely chemical weapons, biological weapons, and landmines. In the case of AI, the question of responsibility and even whether it is morally acceptable or even a violation of human dignity to be killed by a robot are ethical questions that are being hotly debated.[30] Both the newness and the perceived immorality combine to form a *trust gap* that must be overcome in DOD policy.

For most policy documents, the utilitarian approach to develop control mechanisms is generally appropriate. Yet in this case, this approach would lead to a policy mismatch with popular opinion. The utilitarian approach to this problem would be to say that any AI-enabled tech that can outperform a human analog should be allowed to be fielded. In effect, the benefit of the increased performance would outweigh the risks. Yet the perception of this technology does not necessarily follow purely utilitarian perspectives. This mismatch sets up a trust gap that must be overcome in order to achieve public support. The deployment of this technology without public support would put at risk the continued use of the technology and could stymie research and development efforts with wide ranging consequences.

To explain this dynamic, it is important to define some terminology. The first concept is the human reliability benchmark, which represents human analog performance for a tightly controlled task as compared to an AI-enabled system performing the same task. The second concept is the ultra-reliability benchmark. This benchmark, a term borrowed from the airline industry, is a no-fail benchmark since any failure would be considered unacceptable. Essentially, this ultra-reliability benchmark connotes a hypothetical standard where no failures should occur under any circumstances.

The control set for this analysis would be an entirely human-controlled system. This is essentially the system the DOD has operated under since its inception. Under this construct, the population, and DOD policy, understand the limitations of soldiers under the stress of combat and allow for mistakes to be made. The public accepts that human performance will never reach the no-fail ultra-reliability standard. The space between these two systems is defined as the perceived acceptable risk. This acceptable risk can be extrapolated out into perceived *policy* risk.

Figure 1: Baseline Risk Acceptability



However, as the combat environment has continued to become more complex, and weapons systems have become more automated, a new layer of reliability threshold emerges. Here we may define the emergent threshold as an acceptable *machine* reliability benchmark. The space between the human reliability benchmark and the machine reliability benchmark illustrates a trust gap. This gap is somewhat counterintuitive but can be explained by the lack of risk tolerance by the public for "new-risk," or in the case of military technologies, "immoral-risk." In these cases, some mistakes that were acceptable for a human operator are not acceptable for a machine performing the same task. It can be expected, therefore that for technologies with relatively low consequences, the immoral-risk factor will be lower, resulting in a smaller trust gap. This approach explains that benchmarking machine performance to simply match human performance may not be adequate to overcome the perceived acceptable risk of emerging technologies.

An ethical framework analysis can partially explain the emergence of this trust gap. Under a utilitarian model, this trust gap would cease to exist; it should not matter whether a human or a machine was performing the task if the only thing that matters is the result. If a machine with high consequences outperforms a human operator, then by a purely utilitarian logic it would be immoral not to field the system. Yet we do not live in a purely utilitarian world. As noted above, various heuristics are at play. One of the most powerful is the idea of immoral risk. This risk perception relies not on utilitarianism but on virtue ethics.[31] It is understood that humans have virtues; whether machines can have virtues remains an open question. Here, the question becomes whether the public will accept a mistake made by a potentially unvirtuous machine less frequently or by an ostensibly virtuous human more often. For these reasons, it can also be expected that as automation increases, the trust gap will also widen. This phenomenon is largely due to the idea that with a small amount of automation, humans remain largely in control. Yet as the level of automation increases, or the consequences of the task being automated increases, people are more likely to be dubious of the ability of the machine to act as a moral agent.

This scenario becomes even more pronounced when the technology has high consequences. This dynamic can be seen playing out in real-time once again in the self-driving car industry. In this case, the public's acceptance of perceived acceptable risk is exceedingly small. The self-driving car industry, like many DOD programs, is viewed by the public as a technology that is highly automated and high-consequence. In this scenario, both the new-risk and the immoral risk weigh heavily on public opinion and push the acceptable reliability thresholds to reach far beyond human performance. In this case, here defined as automation with high consequences, the trust gap is large and must be overcome by setting a reliability benchmark much higher than human performance. This trust gap is consistent with the

Figure 2: Risk Acceptability in Automation with Low Consequences

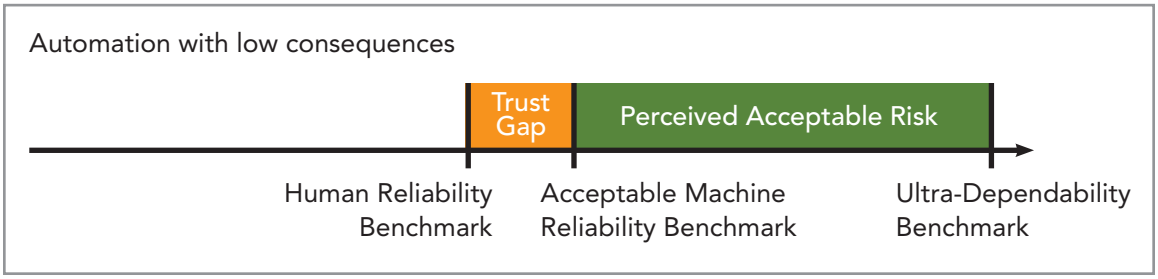
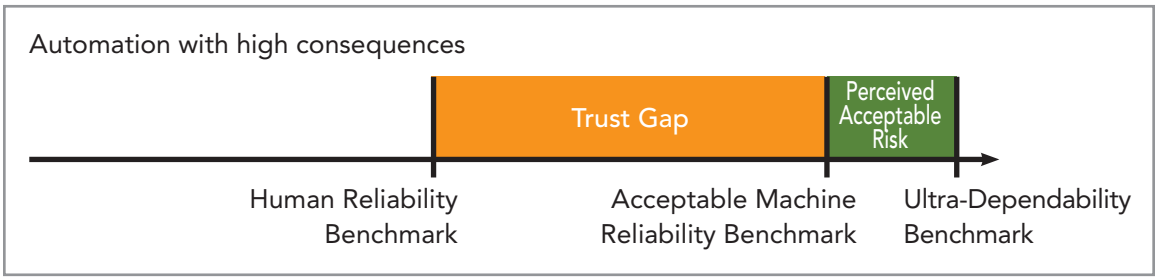


Figure 3: Automation with High-consequences



ethical risk relevancy matrix outlined above. It should be noted that those projects that were identified as having higher ethical risk would also fall victim to the trust gap detailed below.

The DOD must develop reliability benchmarks with these factors in mind. The same consequence tiering levels are recommended in order to adequately allow rapid development of those projects of lower risk while more tightly controlling those of higher risk. In setting these benchmarks, the Department must balance the potentially profound implications that high-consequence mistakes may have on the overall use of the technology with the ability to enjoy the benefits that the technology promises. It has been well documented that the early deployment of this type of technology can lead to exponential increases in overall safety. A recent study by RAND conducted a detailed analysis of this very question for self-driving cars and found that the deployment of self-driving cars at a 10 percent improvement over the human condition would result in significant savings. The report states that "more lives are cumulatively saved under the less stringent … policy than the more stringent … policies in nearly all conditions." The report further compared the benefits of early adoption at 10 percent improvement over human reliability to a 75 percent and 90 percent improvement and found that an early adoption strategy had the result of saving, "tens of thousands to hundreds of thousands of lives."[32] Yet this report also argues that this approach is a purely utilitarian model and cautions against relying on it alone. For the same reasons outlined above, the report recommends policymakers determine a middle ground whereby the policy is acceptable to the public, while still allowing for innovation and rapid adoption.

This article proposes the following reliability benchmarks: Tier 1 projects represent the greatest trust gap that must be overcome in order to enjoy public approval and therefore, must be the most tightly controlled. Therefore, a significant improvement over the human condition is recommended before allowing full fielding. Tier 2 projects engender much less consequence, and therefore would have a lower trust gap, and can, therefore, be less tightly controlled. For these projects, consistent with a rapid advancement model, a 10 percent improvement over human condition should be used. Finally, for Tier three projects where the consequence of failure is low and where there is little to no trust gap, it is not recommended to tie reliability metrics to human performance.

Tier 1 – These project categories have huge consequences as well as high ethical risks. The unique characteristics inherent in autonomous weapons systems mean that a purely utilitarian approach with a rapid adoption model must be avoided. As discussed above, for these projects, a very large trust gap must be overcome before any mistakes are deemed acceptable by the public. Thus, for example, a major backlash against the use of lethal autonomous weapons is likely even for mistakes made that would be easily explained as

Table 2: Benchmarking Projects by Tier

	Consequence Tiering Level	Proposed Reliability Benchmarks
Tier 1	Lethal Autonomous or Semi-Autonomous Weapons System	50%-75% improvement over human performance
Tier 2	Targeting information Systems	10% improvement over human performance
	Safety-Critical Systems	
Tier 3	Privacy concern systems	No human-based reliability benchmark
	Business Process systems	

human error in legacy systems. The potential for this backlash could grind all AI-enabled system development to a halt—resulting in the potential to lose many of the benefits of this technology.

For this tier of project, a 50-75 percent improvement over human performance is recommended. While it is understood that an early adoption methodology that matches, or just slightly improves on, human performance would result in more rapid development, policymakers must work to find an acceptable middle ground that shows a marked improvement over human performance. The early adoption models have been shown to be effective for much more narrowly defined problem sets with a smaller trust gap than can be expected for a lethal autonomous system. At the same time, the policy cannot constrain the technology to a point where the perfect becomes the enemy of the good. As was demonstrated by the RAND report on autonomous vehicles, waiting until a 90 percent improvement over the human benchmark provided marginal gains over a more modest model with a huge tradeoff in time.[33] Policymakers must find a middle ground, and a 50-75 percent increase in performance over human benchmarks will allow the DOD to cover the trust gap while still reaping the long-term benefits of the technology.

Tier 2 – A 10 percent improvement over human performance is recommended for projects with safety critical systems or those that provide targeting data. For these systems, utilitarianism wins out. The benefits gained by early adoption are more important for the DOD than the risks engendered by the potential for mistakes. Logic argues that performance must equal or exceed equivalency to human performance for the technology to make sense to field. Yet this technology still falls victim to the new-risk phenomenon and holds a small trust gap that must be overcome for both the users of the technology and the public. In order to overcome this gap while still retaining the benefits of an early adoption strategy, a modest increase over human performance is prudent.

Tier 3 – For those tier three projects which have low consequence, or those with little ethical risk, it is not recommended to tie reliability metrics to human performance. In these cases, the benefits of early adoption and continued development far outweigh the risk of mistakes. Here, the decision becomes one of functionality and suitability to the task rather than the relative comparisons to human performance in the task. Because of this, it is not recommended to place any restrictions on these applications.

Conclusion

The Department has made significant strides towards the adoption of Artificial Intelligence into critical applications across the force. These technologies have the potential to be game-changers in the way the U.S. military fights its future wars;[34] however, by their very nature, they engender significant ethical challenges. At this early stage of development, the Department has the opportunity to achieve its stated goal of becoming the leader in ethics for military applications. The institutional risks of not getting ahead of the ethical challenges are stark. If the Department runs afoul of industry ethical frameworks, it risks alienating industry, forcing broad policy restrictions from political leaders, or legal challenges to its implementation. Each of these challenges has the potential to grind AI incorporation into the force to a halt. It is, therefore, critical that the Department gains and maintains the strategic messaging that it is pursuing this technology in an ethical fashion and that its use will benefit the United States.

It is time to move past broad ideas of ethical AI in principle and translate these principles into actionable controls that will keep the advancement of this technology inside the bounds of ethical behavior. DOD must create policies which govern the ethical development of this technology. By using a risk management methodology, as detailed above, it will allow the Department to tightly control those projects of high risk while allowing low risk projects to speed through the system. In doing so, the Department can push the boundaries at the technological edge with projects of low consequence while tightly controlling those of high consequence. This risk-based framework lends itself to applying a myriad of controls on projects including the reliability benchmarks and test and evaluation policies detailed in this article. The Department, starting with the JAIC, must institutionalize ethics as part of its ongoing, routine business practices. This focus cannot be viewed as a barrier to development or a bureaucratic process that slows implementation but instead as an essential task to smoothly incorporate AI into the force. The ethical challenges with AI are not insurmountable; they do, however, need to be addressed and mitigated in a formalized fashion for the adoption of this technology to move forward. PRISM

Notes

[1] U.S. Department of Defense, *DOD Records Management Program, Summary of the Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington, DC: DOD 2018).

[2] Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*, Office of the Secretary of Defense (Washington, DC: Defense Innovation Board, 2019).

[3] Department of Defense, *DOD Records Management Program*, Department of Defense Directive (DODD) 3000.09 (Washington, DC: DOD, 11 November 2012).

[4] Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense - Supporting Document*, Office of the Secretary of Defense, (Washington, DC: Defense Innovation Board, Oct 2019), 42-44.

[5] Abigail Beal, "It's Time to Address Artificial Intelligence's Ethical Problems," *Wired*, August 24, 2018, https://www.wired.co.uk/article/artificial-intelligence-ethical-framework.

[6] Future of Life Institute, "Autonomous Weapons: An Open Letter from AI & Robotics Researchers," *Future of Life Institute*, July 28, 2015, https://futureoflife.org/open-letter-autonomous-weapons/.

[7] Brian Green, "Artificial Intelligence and Ethics," *Markkula Center for Applied Ethics*, November 3, 2017, https://www.scu.edu/ethics/all-about-ethics/artificial-intelligence-and-ethics/.

[8] Gianmarco Veruggio and Fiorello Operto, "Roboethics: A Bottom-up Interdisciplinary Discourse in the Field of Applied Ethics in Robotics" in *Machine Ethics and Robot Ethics*, ed. Wendell Wallach and Peter Assaro, (New York: Routledge, 2017), 81.

[9] Ibid, 81.

[10] Lawrence M. Hinman, *Ethics: A Pluralistic Approach to Moral Theory*, 5th ed, (Boston, MA: Wadsworth Publishing 2013) 124.

[11] Department of Defense, *DOD Records Management Program*, Department of Defense Directive (DODD) 3000.09 (Washington, DC: DOD, November 11, 2012), 1.

[12] Brian Green, "Artificial Intelligence and Ethics," *Markkula Center for Applied Ethics*, November 3, 2017, https://www.scu.edu/ethics/all-about-ethics/artificial-intelligence-and-ethics/

[13] Miles Brundage, et al. "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," *Center for New American Security*, February 2018. https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

[14] Batya Friedman and Helen Nissenbaum, "Bias in Computer Systems," *ACM Transactions on Information Systems* 14, no. 3 (July 1996): 330 –347.

[15] Darren Shou, "The Next Big Privacy Hurdle? Teaching AI to Forget," *Wired*, June 12, 2019, https://www.wired.com/story/the-next-big-privacy-hurdle-teaching-ai-to-forget/

[16] Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense - Supporting Document*, Office of the Secretary of Defense (Washington, DC: Defense Innovation Board, October 2019), 43.

[17] Manish Gupta, "Self-Driving Cars: Reliability Challenges, Solutions, and Social Adoption: Strict Reliability Standards are Critical for Human Safety and to Help Drive Social Acceptance of Nascent Self-driving Technology," *Design News*, June 22, 2018, https://www.designnews.com/electronics-test/self-driving-cars-reliability-challenges-solutions-and-social-adoption/87842508158921

[18] Philip Koopman, Aaron Kane, and Jen Black, "Credible Autonomy safety Argumentation," *Published by the Safety-Critical Systems Club*, 2019, 15. https://users.ece.cmu.edu/~koopman/pubs/Koopman19_SSS_CredibleSafetyArgumentation.pdf

[19] Robert Bond, "Artificial Intelligence for National Security Applications" (PowerPoint presentation, Massachusetts Institute of Technology, Lincoln Laboratory, Concord, MA, October 30 ,2019).

[20] Philip Koopman, Aaron Kane and Jen Black, "Credible Autonomy safety Argumentation," *Published by the Safety-Critical Systems Club*, 2019: 19. https://users.ece.cmu.edu/~koopman/pubs/Koopman19_SSS_CredibleSafetyArgumentation.pdf

[21] Ibid, 13.

[22] Ibid, 13.

[23] Ronald Arkin, *Governing Lethal Behavior in Autonomous Robots* (Boca Raton, FL: Chapman and Hall/CRC, 2009), 29-36.

[24] Paul Slovic and Ellen Peters, "Risk Perception and Affect," *Current Directions in Psychological Science* 15, no. 6 (December 2006): 323.

[25] Berkely Dietvorst and Massey Simmons, "Algorithm Aversion: People Erroneously Avoid Algorithms after Seeing Them Err," *Journal of Experimental Psychology* 144, no.1 (February 2015): 5

[26] Lennart Sjöberg, "Factors in Risk Perception," *Risk Analysis* 20, no. 1 (2000): 1.

[27] Ibid, 4.

[28] Ibid, 4.

[29] "Autonomous Weapons: An Open Letter from AI & Robotics Researchers," *Future of Life Institute*, July 28, 2015, https://futureoflife.org/open-letter-autonomous-weapons/

[30] Patrick Lin, "Do Killer Robots Violate Human Rights?: When Machines are Anthropomorphized, We Risk Applying a Human Standard that Should not Apply to Mere Tools," *The Atlantic*, April 20, 2015, https://www.theatlantic.com/technology/archive/2015/04/do-killer-robots-violate-human-rights/390033/

[31] Virtue ethics is an ethical framework which is rooted in the human condition. Essentially it requires a human to have the right moral virtues, and to then be able to use intelligent judgement to conform those virtues to a given situation, and then to ensure that the proper means are used to carry out actions. For more on virtue ethics see: Alasdair Macintyre, "Virtue Ethics," in *Encyclopedia of Ethics*, ed. Lawrence C. Becker and Charlotte B. Becker, 2nd ed. (City: Routledge, 2001), 1276-1281.

[32] Nidhi Kalra and David G. Groves, *The Enemy of the Good: Estimating the Cost of Waiting for Nearly Perfect Automated Vehicles* (Santa Monica, CA: RAND Corporation, 2017), 25.

[33] Ibid, 19.

[34] Shawn Brimley, Ben FitzGerald and Kelley Sayler. "Game Changers: Disruptive Technology and US Defense Strategy, "in *Disruptive Defense Papers*, ed. Thomas P. Hughes and Agatha Hughes (Washington, D.C.: Center for a New American Security, 2013), 3–24.

THE FOREIGN SERVICE JOURNAL

Covering the intersection of diplomacy and defense for a century, *The Foreign Service Journal* provides an insider's perspective for foreign affairs professionals.

Published by the American Foreign Service Association.

Visit us online at **www.afsa.org/fsj**

Subscribe at **www.afsa.org/subscribe-fsj**

Now online:
The full 100-year archive of *The Foreign Service Journal*
www.afsa.org/fsj-archive

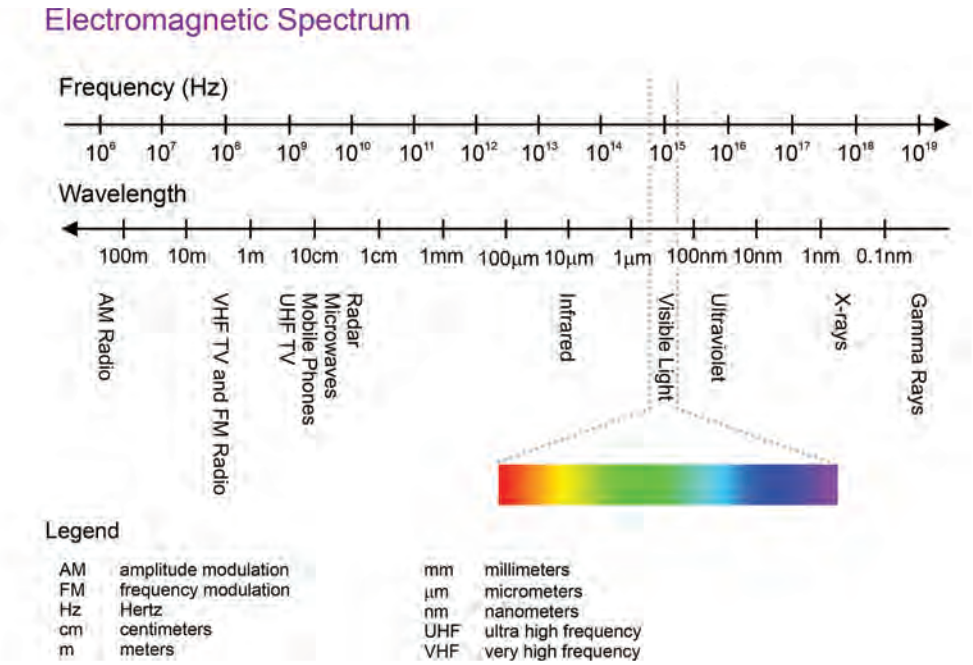
Considered today as a strategic domain in its own right, EMS is at the heart of modern military operations and is the essential link between the land, air, naval, space, and even cyber domains.

Modern Electromagnetic Spectrum Battlefield

From EMS Global Supremacy to Local Superiority

By Major Stéphane Ricciardi and Major Cédric Souque*

As defined in the Joint Doctrine Note 3-16, the electromagnetic spectrum (EMS) is "the range of all frequencies of electromagnetic radiation. The electromagnetic radiation consists of oscillating electric and magnetic fields characterized by frequency and wavelength."[1] This radiation has fascinating properties: it can be visible or invisible, move at speeds approaching that of light, cross certain obstacles or, on the contrary, bounce off them (thus indicating their presence), transport energy or data.



Electromagnetic Spectrum (Joint Doctrine Note 3-16)

Stephane Ricciardi is a Major in the French Army. Cedric Souque is a Major in the French Armament Corps. The views expressed are those of the authors and do not necessarily reflect the official policy or position of the French Ministry of Armed Forces or the French Government.

Considered today as a strategic domain in its own right, EMS is at the heart of modern military operations and is the essential link between the land, air, naval, space, and even cyber domains. At the base of all operational functions (remote sensing telecommunications, navigation, etc.), it also enables the delivery of offensive or defensive effects through electronic warfare (EW) or signal intelligence (SIGINT).

Since the end of the Cold War, Western armed forces, exploiting a comfortable technological lead, managed to achieve almost total electromagnetic supremacy. In other words, they have been able to use all their electromagnetic transmission and/or reception means without major constraints. They had real freedom of action in the field of frequencies during the whole duration and over all the geographical zones of the operation. This undisputed domination was notably decisive in the success of military operations in the Persian Gulf, the former Yugoslavia, Afghanistan, Libya, and Mali.

Unfortunately, the increasing complexity and congestion of the electromagnetic environment (EME), as well as the emergence or return of competitors who have made great efforts regarding EMS capabilities, seem today to call into question Western domination in this area. Indeed, civilian applications are multiplying and the commercial stakes around EMS, such as 5G networks and internet of things (IoT), are constantly growing. In the military domain, hyper-connectivity and increasing digitization have also led to an exponential growth in frequency requirements. Moreover, during the two last decades, many competitors have caught up technologically and developed means of contesting our supremacy in EMS. This evolution concerns both near-peer competitors,[2] such as Russia or China, and intermediate powers, such as Iran. Even non-state actors (insurgents and terrorist groups) have benefited from the democratization of "low cost" EW equipment, most often based on dual-use technology.

Given this increasingly congested and contested EMS, it seems appropriate to ask what strategy the Western forces should adopt in order to maintain their freedom of action. Is it still reasonable to seek to regain global supremacy in EMS through a headlong technological rush?

The answer is no, because while research and development funding will of course be essential to develop disruptive technology over the long term, it will not be sufficient in the short- and medium-term to regain the initiative.

A more pragmatic and affordable approach must therefore be considered. It must be based on a more agile and intelligent management of the spectrum, but mostly on the concentration of effects and the subsidiarity at the tactical level in order to regain electromagnetic local superiority. In other words, it will be a question of establishing an EMS domination limited to the space-time framework of the current operational maneuver and strictly necessary for its achievement.

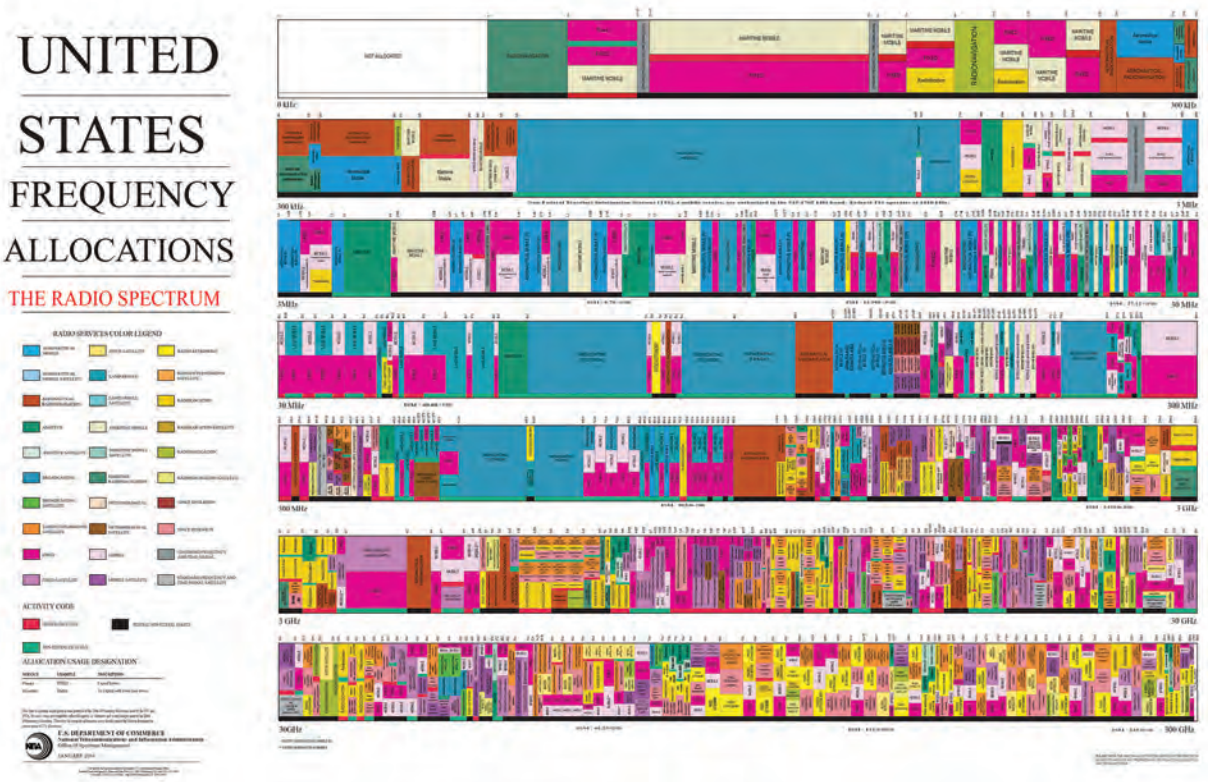
A Complex and Congested Environment

> *"The spectrum has become increasingly complex. More players are accessing and leveraging sections of bandwidth, making it congested."*
>
> Major. General Lance Landrum, U.S. Air Force, 2020[3]

The multiplication of civil and military systems using the electromagnetic spectrum leads to an increasingly congested environment and is the source of unintentional disturbances and a reduction of the operational margins of maneuver in the field of the EMS operations (EMSO).

Competition and Interferences with Civilian and Commercial Use

One of the main sources of congestion in EMS is its widescale use for commercial and non-commercial civilian applications. This general interest



US Frequency Allocations - 2016 (U.S. Department of Commerce NTIA)

in the exploitation of EMS has led to an increased densification of transmitting systems, particularly in the frequency bands between 500MHz and 10GHz. Some bands, such as the 2 to 4GHz band, are particularly congested with the development of technologies such as Bluetooth, Wifi, WiMax, 4G networks and tomorrow's 5G.

This situation leads to many problems that affect military systems: competition between private companies and state agencies, inter-system interference, and increasingly complex management of this resource. Moreover, faced with the economic and social stakes of these civilian needs, the political authorities are increasingly asking military authorities to accept compromises (reduction or abandonment of frequency bands) or to find technical solutions to enable these developments for the public.

Among all civilian applications using EMS, the advent of the 5th generation networks (5G) will have the greatest impact on military systems in the coming years. The civil applications are quite numerous: high-speed communications, internet of things (IoT), and machine-to-machine (M2M) communications[4] including autonomous vehicles. These developments and the use of new frequency bands (e.g. around 3.5GHz and 26GHz) will inevitably be a source of disturbance for military systems. That will affect many operational functions, such as:

- Tactical Radio communications: 5G characteristics (higher data rate, higher number of connected objects and higher number of frequency bands) will induce an overall increase in the level of electromagnetic radiation. This will inevitably lead to problems of electromagnetic

compatibility (EMC) and interference on military radio systems;

- Satellite communications: The use by 5G of the 26GHz band (24.25-27.5GHz) could disturb many Ka-band (27-31GHz) satellite telecommunications systems and cause degradations of the associated military capabilities.
- Weather forecasts: The use of the 26GHz band could also disrupt space weather systems operating between 23.6 and 24GHz. Specialists estimate that this could degrade by approximately 30 percent the reliability of weather forecasts[5] that are critical to military operations.
- Radar and SIGINT systems: 5G technologies will make increasing use of the 3.5 GHz band, which is also used by many S-band (2 to 4 GHz) radars.[6] This could affect the detection capabilities of air traffic control and air defense radars in these bands. Signals intelligence systems could also be impacted in their detection and discrimination capabilities.
- GPS systems: Initiatives by companies such as Ligado Networks[7] in the United States to deploy a low-power national 5G network in close proximity to the GPS frequency band could lead to interference with this critical positioning system for multiple military systems.

This issue will be much more complex than the frequency allocation as 5G applications are not exactly the same in all countries. Indeed, the standard identifies different frequency bands that can be used. Then, each country chooses which one will be used, taking into account its own constraints. For example, in France or the United States, 5G is deployed in the 3.5 GHz band while in China it is also deployed in the immediate vicinity of 5 GHz. In the future, these differences in frequency allocations could be an additional source of interference for the military EMS capabilities.

Of course, the interference related to 5G could increase and be even more complex to manage, since military capabilities should also exploit this technology in many fields of application[8] such as command and control (C2) and intelligence, surveillance, and reconnaissance (ISR) areas. Beyond the risk of interference, 5G-based military systems may be more vulnerable to cyber-attacks and espionage.[9] So far, most 5G equipment comes from China and it is difficult to control its security level.[10] Specific measures[11] will have to be taken to mitigate this risk, such as giving preference to Western suppliers or imposing stricter security rules on Chinese equipment.[12]

Finally, in addition to the problems related to civil transmitting systems, other very specific sources of disturbance can unintentionally constrain EMSO. These include, for example, the topography (mountain, forest, etc.), urban buildings, climatic and meteorological conditions, and certain industrial activities such as wind turbine farms that have a negative impact on radar systems.[13]

Risk of Interference with all Deployed Systems

Civilian systems are not the only sources of EMS congestion. Indeed, modern military operations, such as those conducted by Western armed forces, require increased capabilities using electromagnetic energy;[14] communication systems (for coordinating, navigation and C2 systems), active (radars and LASERs) and passive detection systems (electromagnetic and optical sensors), and electronic attack systems (including directed effect weapons and jammers). These systems are distributed over the entire EMS.[15]

Consequently, frequency bands and data rate requirements[16] have never been more important for military applications. At the same time, the increasing number and complexity of military transmitters on land, naval, and air platforms creates significant electromagnetic radiation that multiplies the risk of intra-system interference (auto-jamming, and even damage on front-end electronic components).

While the level of emission from each weapons system is already a big electromagnetic compatibility (EMC) issue, it becomes much more important in the case of a military force deployment. The multiplication of weapon systems in a small area increases the risk of disturbances. This will be the case in all domains; for example, in a naval deployment with aircraft carrier, destroyers and fighter aircraft or within a deployed battle group with many different types of ground vehicles and helicopters. As an indication, in 2015, the U.S. armed forces were a victim of more than 261 satellite communications jamming events. According to General John Hyten,[17] Head of Air Force Space Command in 2015, the majority, indeed perhaps all, were caused by self-jamming.

And what about the risk of interference in a coalition operation or exercise? The majority of Western armed forces have chosen to improve their connectivity and resilience in EMS, and most have highly radiant communications and weapon systems, not to mention their own EW capabilities. As the different actors do not use the same types of equipment or even the same standards, the constraints on the EME worsen because of significant emissions in conflicting frequency bands.

Dealing with this Environment Without Adapted EMS Management Tools?

As previously demonstrated, the increased use of EMS by civilians and the military is likely to disrupt many operational functions, such as tactical communications or connected C2. Even ISR systems and navigation capabilities could see their effectiveness reduced due to the blinding generated by this congested EMS. These disturbances, if they do not irremediably call into question the capacity for action in the spectrum, are nevertheless likely to degrade and constrain it from time to time.

Most of this interference could be reduced or even avoided if Western forces had agile and interoperable electromagnetic battle management (EMBM) tools.[18] Unfortunately, current tools are not adapted to this congested and complex environment because they were developed before the advent of 5G and the rise of military connectivity. This limitation will be all the more significant as the majority of the transmitting and receiving systems used by Western forces do not have the flexibility to adapt to this environment. Their ability to change frequency bands or waveforms to face interference brought on by other civilian or military systems remains too weak.

In the short term, these limitations will require more and more circumvention measures, such as prohibiting the use of certain frequency bands, limiting the power of emissions, or taking into account minimum distances between systems. If nothing is done, the accumulation of these measures will tend to reduce the maneuver margins of armed forces. However, some actions can be envisaged to mitigate this growing risk:

- Improving collaboration with civil and political actors to defend military interests directly within the decision-making board in charge of frequency band allocation and management;
- Adapting existing EMS military systems by implementing waveforms that allow coexistence with civilian systems using the same frequency bands;
- Fostering the development of future capabilities increasingly flexible in terms of frequency band and waveform;
- Reviewing the EMBM tools[19] to ensure compatibility with this modern environment. This will require better interoperability between systems.

Pending the implementation of these solutions, Western forces will continue to be constrained by this modern EME. While it will be difficult enough to deal with this complex and saturated spectrum, the main challenge ahead in this area for Western forces will most likely be the EMS contestation coming from their competitors.

Electromagnetic Spectrum: a Contested Battlefield

> *"The next war will be won by the side that best exploits the electromagnetic spectrum."*
>
> Soviet Admiral Sergei G. Gorshkov, Commander of the Soviet Navy, 1973

Recent strategic and technological developments have resulted in an increase in contestation in the electromagnetic field.[20] Indeed, the threat has developed on three levels: leading actors in the EMS field who would like to acquire total domination; the probable rise in range of regional powers wishing to increase their capacity to deny access; but also the entry into the race of non-state actors relying most often on dual-use technology.

Growing EW Capabilities of our Near-Peer Competitors

Whether as an enabler of operational functions, for SIGINT, or more directly for EW, EMS quickly emerged as a means of compensating for conventional power asymmetry in military confrontations. Russia was first to realize the advantage this could provide and throughout the twentieth century made the Red Army a reference in this field.

With the fall of the USSR, the young Russian Republic was unable to capitalize on its expertise and gradually lost its lead in EMS. However, Russia, but also China and other intermediate powers, took advantage of this turning point in history to pose as observers during the 1990s and 2000s and learn from the Western camp. Thus, the Gulf War, NATO's involvement in the Balkans, but also more recently, in Afghanistan, gave them the opportunity to monitor and analyze Western C2, ISR, and EW systems and, moreover, build a tailored capability response to counter them.

In parallel with this technical and operational monitoring conducted in Western theaters of operations, China and Russia have also faced challenges in their own spheres of interest that have made them aware of the relative advantage they could gain from mastering EMS.

Russia

During the Georgian conflict of 2008, the first post-Soviet symmetrical conflict, the Russian army became suddenly aware of its lack of preparedness, even its decline, in the field of EW. This "electro-shock" was one of the triggers of the Seridioukov reform of 2008,[21] which notably aimed at a complete overhaul of the EW Soviet model to make it the cornerstone of the Russian defense system.

Above all, this reform involved a structural reorganization aimed at restoring general consistency to EW capabilities by integrating all resources under a single command.[22] Land forces today have five independent brigades to conduct EMS actions at the operational or strategic level, and each combat brigade has its own EW company. Naval forces have five centers dedicated to EW, two of which are exclusively for the Pacific fleet. Finally, the Air Force has five battalions directly integrated into the air defense divisions, 14 helicopter detachments, and one specifically dedicated to combat aircraft.

However, beyond a simple reorganization, the Russian electromagnetic reform has above all brought about a doctrinal rupture. Whereas the traditional Russian approach was essentially based on escort jamming, the new policy aims to be much more offensive and to move from the blockade of electronic information to the usurpation and destruction of opposing systems.

Moreover, it seems that this new, more agile doctrine was not devised in isolation but, on the contrary, to deliver its full potential within a more comprehensive strategy, that of hybrid warfare. Mastery of EMS can indeed be a particularly decisive asset to blind, deceive, or demoralize an adversary in a context of unclear engagement, where

actions are difficult to attribute and remain permanently below the threshold of a declared war. The Ukrainian Donbass conflict of 2014-2015 demonstrated this effectiveness.[23]

Regarding the capability aspect, without going into exhaustive detail, it is interesting to take a quick overview of the most disruptive equipment.[24] Within the Army, the heaviest investments have been made in jammers and SIGINT capabilities. Deployed in Syria and Ukraine, these systems have proved particularly effective in gaining full control of GSM networks,[25] giving an offensive jamming and self-protection capability at the lowest tactical level, but also in countering the ground-to-air threat by distorting aircraft location data, even when encrypted.

The Russian Navy also has a wide range of modern means dedicated to self-protection, jamming, and decoying. Its most modern frigates are equipped with electro-optical countermeasure systems using low frequencies to disorient and blind enemy pilots. The Air Force, already at the forefront in the field, has supplemented its capabilities, especially via the development of new electronic countermeasure systems aiming to break through NATO's interdiction bubbles.

Finally, in addition to the modernization of its conventional electromagnetic capabilities, the Russian Armed Forces seem to have reinvested, in recent years, in research on directed energy weapons (A60 aircraft and the Peresvet gun project), as well as in weapons and ammunition using high-power microwaves to remotely neutralize the hardware of enemy aircraft up to 40km away.

China

Following in Russia's footsteps, China quickly came to understand that EW will be a tool to be developed as a priority in order to deny its main competitors access to and control of the Western Pacific. This realization led to an accelerated modernization of its organization, doctrine, and equipment which began with the concept of Integrated Network Electronic Warfare in the early 2000s.[26] This integrative logic has led organizationally to the creation of a Strategic Support Force (SSF) that controls all information warfare units, including cyber, space, and EW.

In parallel with this structural reorganization, the People's Liberation Army (PLA) has also evolved its doctrine to ensure dominance over the entire EMS. The new strategy focuses particularly on removing, degrading, disrupting, or deceiving enemy electronic equipment.

Regarding its capabilities, it is particularly difficult to obtain precise information on the PLA's level of EW equipment. However, the latest annual report to the U.S. Congress on the Military and Security Developments Involving the People's Republic of China[27] suggests that the PRC has a fairly complete spectrum of capabilities.

The Air Force, for example, might have a large fleet of SIGINT aircraft, and a special effort seems to be made regarding space capabilities: jamming of Western satellites' data and SATCOM using rendezvous and proximity operations (RPO).[28]

Finally, there is now no doubt that in the context of a major conflict the Chinese government is also preparing to use high altitude electromagnetic pulse weapons (HEMP).[29] By producing a powerful electromagnetic pulse, these weapons have an immediate, irreversible, and devastating effect on electrical facilities, computer equipment, and, more generally, all communication systems within a certain perimeter.

For the Chinese government, HEMP could therefore be the ultimate building block in the so-called total information war. In a 2016 article by the Chinese National Security Policy Committee, HEMP is presented as a disruptive technology capable of recalibrating the balance of power. Embedded in hypersonic missiles or, even worse, in satellites, it could constitute a formidable "strategic surprise." Some experts now talk about a potential 21st century Pearl Harbor.

Democratization and Proliferation of EMS among Intermediate Powers and Non-state Actors

While the last 20 years have seen strong resurgence of China and Russia in the race for dominance of EMS, there has been a parallel proliferation and democratization of EW means among both regional, intermediate powers and non-state actors.

Indeed, the market for electromagnetic equipment has been largely restructured and diversified in recent years, favoring a drop in prices[30] and allowing intermediate powers to gain access to an "off-the-shelf" range of equipment. In the Russian-centered market, for instance, a streamlining effort has been undertaken. Of the 120 companies listed in 2010, only 13 have survived and the two largest groups, KRET and Sozvezdie, share most of the domestic market as well as the export market.

Finally, in parallel with the expansion of supply, the market for EW equipment has also been boosted by an increase in demand. The proliferation of ISR and anti-access area denial (A2AD) means, particularly in Asia and the Middle East, is likely the main factor.

Thus, this concomitant increase in supply and demand has contributed to the proliferation of EW equipment among regional powers, whether they are allies or potential competitors. For instance, in the Middle East's so called "arc of crisis," Israel is undoubtedly the regional power with the most comprehensive EW capabilities. Its ground forces have a full range of capabilities in signals intelligence, influence, and communications jamming, as well as explosive device disposal.[31] Neighboring nations such as Iran, although less advanced in the field, might still have GSM, SATCOM, and GNSS jamming capabilities, as well as integrated EW systems, probably purchased from Russian companies.

The widening of the circle of states equipped with EW means is therefore a reality that will have to be dealt with in the years to come. However, while the threat from the main competitors will inevitably be the most serious, it will not be the only one in the field. Indeed, many non-state actors (insurgent movements, pirates, terrorist organizations, or even proto-states) favoring asymmetrical confrontation can today more easily gain access to equipment that can disrupt the use of EMS in a more or less significant way. The latter, by using dual-use equipment or more simply by hijacking the use of purely civilian systems, will probably be able to bypass international arms trade legislation.

While their presence has not yet been officially observed, it is highly likely that we will soon find some of the following equipment or capabilities deployed in theaters of operation:

- Software Defined Radio (SDR), which leverages intrusion capabilities into GSM, Wifi and Tetra networks,[32]
- The jamming or even spoofing of unprotected GNSS equipment.[33]

Impact on the Western Forces' Freedom of Action

The strengthening of contestation in EMS and the spread of threats are not without consequences for the freedom of action of Western forces. Indeed, these may challenge their ability to carry out both offensive and defensive actions by depriving them of an enabler, which has become essential.

First, at the strategic level, this vulnerability might concern satellite telecommunications, which are today the keystone of an info-centric operations model (SATCOM, data transmission, GNSS).

Secondly, at the operational level, the democratization of A2AD equipment incorporating new-generation, barely detectable radars could directly threaten the ability of Western armed forces to get in first. And with regard to the defensive aspect, the threat might result in the use of low-technological means that, if used in significant quantities, could saturate even the most sophisticated defense systems.

It is perhaps at the tactical level that the loss of control of EMS could have the most critical consequences. Actions on GNSS services, for example, in addition to the effects on positioning and navigation, might hamper the use of Blue Force Tracking (BFT) or even lead to friendly fire in case of signal spoofing.

In the end, it seems that in parallel with the ever-increasing congestion of EMS we are also witnessing an insidious and widespread increase in the threat level in this strategic domain. Based on this observation, an effective strategy to deal with this has yet to be defined.

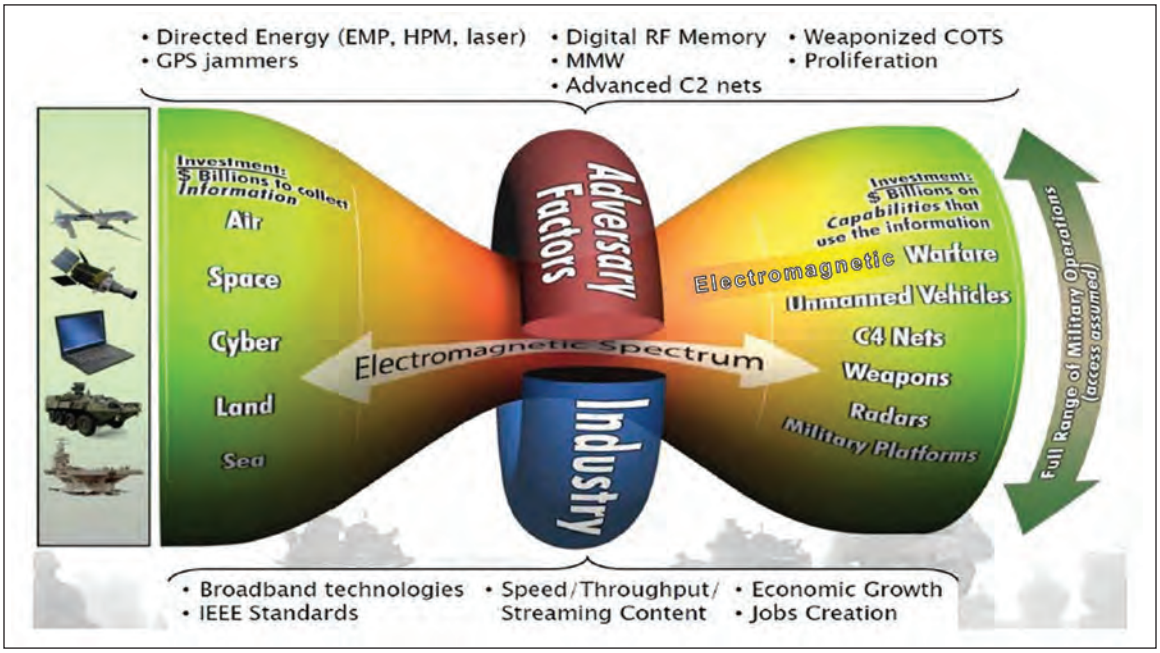
The Utopian Notion of Regaining EMS Supremacy

> *"We have lost the electromagnetic spectrum."*
>
> Alan Shaffer, Pentagon's research and engineering chief, 2014[34]

Taking into account this increasing congestion and contestation of EMS, the first option for Western countries could naturally be to try to regain global supremacy in this environment. To assess whether such a reconquest is possible, it is necessary for Western countries to ask themselves three key questions. The first one is about the current state of EMS and EW capabilities of the Western armed forces, i.e. the starting point. The second concerns the new technologies needed to regain global supremacy and their level of maturity, i.e. the means to achieve it. The last question is the ability of Western countries to win this future arms race, i.e. the credibility of this approach.

The Current State of Western EMS and EW Capabilities

After the end of the Cold War, Western Forces (especially American, French and English) intervened mainly in theaters where the electromagnetic field was barely contested. Thus, during operations in Afghanistan or the Sahel, EMS supremacy was achieved from the outset, and during the Iraq, Balkan, and Libyan campaigns, it was won relatively quickly thanks to kinetic and EW means outperforming opposing forces.



Challenges of regaining a congested and contested EME (US Air Force AFDP 3-51)

However, from the early 2000s, insurgents from Afghanistan, Iraq, or the Sahel region began to challenge this supremacy by conducting operations in EMS: RC-IED attacks, coordination in the context of ambushes, communication jamming or even GPS jamming, and more recently attacks using mini-drones or even interception of tactical data links. Unfortunately, as shown, these weak signals were only the tip of the iceberg constituted by the massive rearming of intermediate and upper-spectrum powers in EW. Western powers failed to take the measure of this evolving conflict, which was a form of strategic myopia.[35]

Since their lesser endowed opponents did not fundamentally succeed in challenging the freedom of maneuver of Allied Forces in these theaters of operation, Western countries were not driven to innovate in the field of EMS,[36] particularly in the area of EW. On the contrary, Western countries have concentrated their investments in the acquisition of existing systems and in the adaptation of these means to threats or local specificities (RC-IED threat or resistance to GPS jamming), without taking into account developments underway in competitor countries. As the Western countries have not invested, at least not sufficiently, in new EW technologies and in new concepts of EMSO, the delay suffered by their armed forces in this area is significant today.

New Technologies Needed and their Maturity Level

Considering the current state of EMS capabilities, regaining global supremacy in this area will require the development of new and innovative systems. The goal is to be able to deal with multi-domain strategies and systems (cyber, EW, A2AD) developed to reduce our capacity of action. Several orientations are being studied to find long-term solutions:

- Low Probability of Interception and Detection (LPI/ LPD) communication systems[37] that minimize the emission level and "dilute" the signal in order to complicate its detection for intelligence or jamming purposes;
- Cognitive EW systems[38] and other intelligent systems[39] with deep-learning capabilities;
- Quantum-based systems[40] such as quantum sensors[41] (for enhanced radar or navigation systems), quantum communications (allowing highly secure exchange against SIGINT systems), and quantum computing (to speed up certain calculations such as EW data processing).

These solutions will rely on disruptive technologies (quantum or artificial intelligence) whose level of maturity must be developed before any operational deployment is possible. These advances should secure supremacy regained over time by reversing the technological value chain and making it more complex for future adversaries to implement effective countermeasures.

Unfortunately, the development of these new technologies will require significant financial commitment, likely several billion euros over the coming decade. Beyond that, it is above all the quantity and diversity of weapon systems to be realized that will complicate this choice. In a particularly constrained economic context due to the consequences and aftermath of the COVID-19 crisis, the sustainability of such a financial commitment is not guaranteed in the short term. It will require prioritization and trade-offs with other capabilities and will raise the inevitable question of abandoning other operational means.

Another fundamental issue is the time required to develop these new technologies. Thus, regardless of cost, it would likely take more than a decade[42] to bring them to maturity and to develop and produce all the necessary weapon systems. Moreover, it is necessary to consider the additional time allowing for the operational ramp-up (recruitment and training of experts) in the use and maintenance of these new technologies.

In conclusion, the time and money needed to regain global supremacy in EMS would leave Western armed forces vulnerable to EMS threats in the short- and medium-term.

Can the West Win this New Arms Race?

The previous considerations do not take into account the likely reactions of the Western forces' competitors. It is illusory to think they will passively wait for us to surpass them again. They will more likely continue their investments (until at least 2025 for Russia[43]) and adapt their systems and strategies accordingly. Meanwhile, the intermediate powers and non-state actors will continue investing in EW.

The choice to invest massively in new technologies for EW, telecommunications, or guidance and navigation in order to regain supremacy over EMS will inevitably lead to a new arms race. In fact, the race seems already to have begun, judging by how Beijing communicates frequently on their new military EMS technologies;[44] anti-satellite weapons, directed effect weapons, artificial intelligence, or quantum technologies. This competition would be profoundly different from the one that took place during the Cold War. Indeed, Western allies will not have just one major competitor to contain but two, Russia and China, not to mention intermediate powers. This situation will make the management of this arms race much more complex and its outcome uncertain.

Another major issue is that the China of the 2020s is not comparable to the Cold War USSR. China's economic power[45] today is far greater than that of the former Soviet Union. Whereas the USSR's GDP never reached 50 percent of the U.S. GDP[46] during the Cold War, China's GDP has never stopped growing and today exceeds 66 percent of that of the United States. Moreover, with an annual growth rate more than twice as high,[47] China's economy could surpass that of the United States by the end of the decade.[48] On the other hand, although the Russian economy is more fragile,[49] Russia has abundant energy resources and a positive trade balance with a public debt lower than that of the Western powers. Russia should therefore be able to continue their efforts in the EMS field so as to be a credible competitor in this arms race.

The situation regarding military spending could be misleading. While the United States remains largely in the lead in this area, it is necessary to pay attention to underlying trends. The gap that existed with China and Russia at the end of the Cold War has been inexorably narrowing. This can be explained by a greater increase in military spending in both countries in recent decades. By comparing the average level of military spending during the 2000s with the 2010s,[50] it appears that U.S. military spending increased by 14 percent while it increased by more than 150 percent in China and 85 percent in Russia.

Moreover, this narrowing gap can also be qualified by the way the different competitors have invested. As demonstrated, Western countries have spread their investments over all capability sectors while Russia and China have focused their financial efforts specifically on EMS, which they consider the main axis of vulnerability of Western armed forces.

This economic and military context makes the situation less favorable for Westerners striving to regain EMS supremacy. With their favorable economic indicators, a reorganized military industry, a large labor force, and unfettered political freedom of action, the Chinese and Russian regimes have significant advantages in this future arms race. Moreover, it is not necessary for them to achieve total supremacy: they need only maintain their ability to challenge it. Therefore, the technological and financial effort required of them will be less than that required of the Western powers.

In conclusion, the success of such a purely technological and capability-based approach seems utopian in the short and medium term. This should force Western forces to consider another option,

more progressive and based on adapted investments and new doctrines: regaining a localized superiority, in time and space, one sufficient enough to carry out any future operation.

Local EMS Superiority Instead of Global Supremacy

Whereas the restoration of global supremacy in EMS no longer seems attainable in the short- or medium-term for Western countries, this does not mean that they must completely change their concept of operations, which is primarily based on the mastery of information from the tactical to the strategic level. However, preserving freedom of action in future conflicts will require an adaptation of this model via a more agile and intelligent management of the frequential resource but, above all, by concentrating the electronic effects in a well-defined space-time framework.

Local Superiority, or the Art of Concentrating Effects and Means

As is already the case in other fields, the principle of concentration of effort, applied to EMS, would make it possible to compensate for the loss of global supremacy. The principle of concentration of effort is one of the three principles of war attributed to Marshal Foch and which have since constituted the fundamental basis of Western doctrinal thought. Conceptually, it is a matter of concentrating in the same place and at a particular time all the power vectors in order to tilt or re-establish a favorable balance of power. Thus, in a situation where the overall domination of the adversary would not be attainable by qualitative or quantitative overmatch, the partition of the enemy by maneuver can allow for their sequential defeat.

Yet in EMS, what would this local superiority correspond to? As we have seen previously, it now seems to be illusory to want to dispose of the entire EMS at will and, at the same time, deny the enemy access to it for their own use. The conquest of electromagnetic superiority limited in time and space would aim at providing the strictly necessary and sufficient EMS resources to carry out a given mission within a well-defined space-time context. In other words, it would be a matter of concentrating EMS efforts on a particular point of application and during a chosen time period in order to guarantee the use of an effector deemed essential to the accomplishment of the mission, or conversely, to deprive the enemy of a key capability.

For instance, it could be a question of preventing the enemy from local use of its communications and its EW means by massive and indiscriminate jamming, accepting if necessary and as a counterpart, the deprivation of one's own EMS means. This could also result in increasing the use of decoys and deception in making the adversary doubt the effectiveness of its EW and A2AD systems.

Strictly Necessary and Sufficient Capabilities to Open a Window into Enemy Defenses (available and cost-effective technologies)

The preference for local EMS superiority rather than global supremacy is justified in part by a rejection of a new, potentially ruinous and uncertain arms race. However, this does not imply the complete banishment of technology from future orientations, but rather integrating into weapons systems technology that already exists, potentially dual-use and available in sufficient quantities. Such technology would notably allow for greater agility and resilience while also being cost-effective. Indeed, the conquest of local electromagnetic superiority will require strong autonomy of the most advanced units and consequent adaptability of their systems using EMS. In particular, the aim would be to deploy offensive EW systems down to the lowest tactical level, offering jamming, interception and electromagnetic deception capabilities.

In addition, a transition to increasingly software-defined types of equipment will also bring more physical agility and better system survivability by

transitioning from heavy systems to potentially lighter (with equivalent capacities) and redundant ones.

Moreover, in order to confer local EMS superiority, it is essential that these future systems be saturating owing to their "mass effect," and inexpensive with regard to their efficiency. Therefore, in addition to the above-mentioned directions it will also be necessary to have low-cost, low-tech equipment, capable of deceiving or momentarily saturating the enemy's sensors owing to weapons or EW payloads.

For example, in the air domain, this approach could be based on the use of swarms of air-launched mini-UAVs, or decoy systems with a reasonable cost (lower than that of a cruise missile), equivalent to the U.S. ADM-160 MALDs.[51] Inert, or equipped with adapted decoy capabilities, or even powerful jammers, these effectors could locally and temporarily incapacitate the most sophisticated enemy defense systems by saturating their sensors and information processing capabilities and depleting their ammunition stocks. Moreover, they could also be highly effective in conducting deception operations, by stunning enemy C4ISR systems.

During their various deployments in the Syrian, Libyan, and more recently in the Nagorno-Karabakh regions, the Turkish Armed Forces have demonstrated the effectiveness of this strategy. With the massive use of UAVs equipped with destructive capabilities and EW payloads, they have succeeded in saturating enemy defenses and inflicting significant losses at a relatively limited cost.[52]

This strategy can also be applied to land operations, and many projects are underway to provide local saturation capabilities in EMS. In particular, the United States is reportedly developing a concept called the Modular Electromagnetic Spectrum Deception Suite (MEDS).[53] This system should eventually enable electromagnetic deception operations by reproducing the electromagnetic signatures of friendly units, but also creating electromagnetic noise capable of saturating enemy detection and command systems.

Finally, one of the keys to regaining local electromagnetic superiority could lie in integrating into EW, at the tactical level, the cyber component. Indeed, due to an ever-increasing part of the logical and application layers in all systems using EMS, it seems that the boundary between EW and cyber warfare is disappearing, such that it is now appropriate to refer to it as cyber-electronic[54] warfare. The perspective of local electromagnetic dominance would thus imply the emergence of some degree of autonomy in cyber combat down to the tactical level.

This evolution will largely rely on the development of individual human skills but will also require an increasing integration of artificial intelligence to overcome the technical barriers between the cyber and EMS fields. In particular, it will make it possible to place cyber actions in the tighter tempo of EW actions by automating the phases of acquisition and analysis of cyber intelligence, as well as the development of ad hoc malware to attack enemy systems.

Fighting in a degraded EME by Decision-making Autonomy at the Lowest Level of Command

While achieving local EMS superiority will not be possible without the help of technological tools, it will also call for a doctrinal paradigm shift in order to promote decision-making autonomy down to the lowest level of command. This change will concern tactical and operational actions, command systems, and procedures, but also the collective and individual ability to fight in a contested and congested EME.

The undisputed dominance of EMS over the last twenty years in expeditionary conflicts has gradually led Western armed forces to an increasingly centralized command and control system for operations. Indeed, the ability to access information relatively consistently and instantaneously down to the lowest level of command has contributed to the overwhelming of decision-making levels and encouraged a strong dependence of our command architectures on information and communication systems.

Conducting operations in a contested EME will inevitably imply getting used to intermittently losing the link with the most forward units, giving more space for subsidiarity. Actually, it would mean adapting the concept of the "conducted battle," where the subordinate iteratively performs a series of tasks (or sub-missions) in order to achieve an overall objective, in line with the concept of "mission command." The latter cedes more initiative to the subordinate to choose the course of action best suited to the success of the mission.

In addition to a potential loss of connectivity to the rear, a highly contested EME could disrupt or even disable the overall consistency of the most advanced weapons systems, whose strength relies heavily on the hyper-connectivity of their various components. Therefore, on the one hand Western armed forces will need to ensure that these new systems are as resilient as possible to the threat (in particular by using highly directional beams, such as FH, which are difficult to jam and intercept), but also, on the other hand, must prepare for the worst-case scenario by considering the eventuality of temporarily operating in degraded mode.

Moreover, beyond the doctrinal and technological evolution, the ability to win in a contested EME will depend on how well troops have prepared for it through training and drilling.

It should be noted that Western armed forces, excepting perhaps the Americans, no longer train or do very much in these degraded electromagnetic conditions and, above all, no longer have the capabilities and structures that would allow them to do so. It might be appropriate, for example, to develop a larger center in Europe allowing for the use of longer-range weapons and using more modern ground-to-air threat simulation systems.

With regard to land forces, a small joint mobile red team-type unit could be created to systematically test the cyber vulnerabilities and capabilities of units. This type of approach has, for example, been undertaken by the U.S. Army, which is testing its new network architecture with its Network Integrated Evaluation (NIE). In addition, it is essential that specific training be provided within each operational unit. In particular, it is important to re-educate tactical operators on electromagnetic discretion: whether for communications or data transmission, each soldier must learn how to choose the most suitable means of transmission and, above all, its transmission power, according to this factor.

Finally, it seems obvious that the ability to fight and gain superiority in a contested EME will also require a change of mindset and education within the armed forces, to instill an EMS "culture."

This change of outlook will aim in particular to minimize the weaknesses caused by the fighter's individual behavior and, on the contrary, exploit those of the enemy. As an illustration, local wi-fi networks deployed on forward bases in theaters of operation are potentially vulnerable to short-range adversary attacks.

Moreover, these networks constitute a further vulnerability since they are also used for the soldiers' well-being and personal communications. By simply monitoring social networks, but also by conducting influence actions through them, the enemy could weaken the morale and cohesion of the force or, worse still, compromise the execution of ongoing operations.

In addition, fighters' personal devices also constitute a vulnerability due to their technical characteristics. Smartphones are now ubiquitous in operations, and it is increasingly rare for soldiers to consent to part with them, even when engaged on the front line. However, beyond the source of information they represent, these devices are first and foremost transmitters that can betray the nature, volume and, above all, position of a unit through their electromagnetic signature.

In 2014, during the Donbass conflict, a Ukrainian artillery battalion was decimated within fifteen minutes by Russian counter-battery fire after its position was betrayed by an application installed

on the personal smartphones of the unit's soldiers.[55] Protection against electromagnetic attacks is therefore not just a matter for specialists. It concerns each soldier and requires individual awareness and discipline to reduce collective vulnerabilities.

Conclusion

Finally, it seems that an increasingly congested and contested EMS is a problem serious enough to challenge the dominance of Western armed forces in this field. More broadly, this loss of supremacy could jeopardize their freedom of action and their ability to conduct operations in an operating environment where information mastery has become a key issue. This new situation calls for an immediate response, or a strategic downgrading will be unavoidable. First of all, it seems obvious that a financial and capability effort must be made; in the long term, only research and development will provide equipment disruptive enough to bridge the accumulated gap in the electromagnetic field and restore a favorable balance of power. However, this strategy will not be sufficient; indeed, it may not prove successful for several decades and could lead to a new, potentially ruinous technology race. Other options must therefore be considered in the short- and medium-term to maintain the initiative.

Congestion of the spectrum might be overcome by more agile and smarter management of the frequency resource. This will be possible in the future through better coordination with civilian organizations, but above all by the development of new tools allowing for dynamic control of EMS. Regarding EMS contestation, a more pragmatic approach must be envisioned, one favoring the conquest of local electromagnetic superiority. The objective would be to regain the necessary and sufficient freedom of action to carry out any mission in a reduced space-time framework. The creation of this "window" in the enemy defense will require the development of cost-effective saturation and decoying capabilities, greater agility, and more decision-making autonomy, but also learning to fight in a degraded EME.

Beyond a simple organizational and capability overhaul in EMS, it will as well be necessary to adopt an even broader approach in the longer-term. Indeed, the borders between the different domains related to information management are becoming increasingly thin. Communication, influence, cyber, and electromagnetic actions all tend today to form a technological and operational continuum, and it would be a mistake to keep considering them separately. PRISM

NOTES

[1] "Joint Doctrine Note 3-16 - Joint Electromagnetic Spectrum Operations," Joint Doctrine (Joint Chief of Staff, October 20, 2016), I–2, https://fas.org/irp/doddir/dod/jdn3_16.pdf.

[2] "Strategic Update 2021" (French Ministry for the Armed Forces, 2021), 16, https://www.defense.gouv.fr/content/download/605304/10175711/file/Strategic%20update%202021.pdf.

[3] C. Todd Lopez, "As in Other Domains, U.S. Use of Electromagnetic Spectrum Is Contested," May 20, 2020, https://www.defense.gov/Explore/News/Article/Article/2193532/as-in-other-domains-us-use-of-electromagnetic-spectrum-is-contested/.

[4] "Vodafone M2M Barometer Report: Internet of Things," July 2015, https://www.vodafone.com/business/news-and-insights/press-release/vodafone-m2m-barometer-report-reveals-rapid-growth-in-internet-of-things.

[5] Jason Samenow, "Head of NOAA Says 5G Deployment Could Set Weather Forecasts Back 40 Years. The Wireless Industry Denies It. - The Washington Post," March 23, 2019, https://www.washingtonpost.com/weather/2019/05/23/head-noaa-says-g-deployment-could-set-weather-forecasts-back-years-wireless-industry-denies-it/.

[6] Hugh Griffiths et al., "Radar Spectrum Engineering and Management: Technical and Regulatory Issues," *Proceedings of the IEEE* 103, no. 1 (January 2015): 85–102, https://doi.org/10.1109/JPROC.2014.2365517.

[7] Jill C Gallagher, Alyssa K King, and Clare Y Cho, "Spectrum Interference Issues: Ligado, the L-Band, and GPS" (Congressional Research Service, May 8, 2020).

[8] John R Hoehn, Jill C Gallagher, and Kelley M Sayler, "Overview of Department of Defense Use of the Electromagnetic Spectrum" (Congressional Research Service, October 8, 2020).

[9] John R Hoehn and Kelley M Sayler, "National Security Implications of Fifth Generation (5G) Mobile Technologies" (Congressional Research Service, October 8, 2020).

[10] Andrea Gilli and Francesco Bechis, "NATO and the 5G Challenge," NATO Review, September 30, 2020, https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html.

[11] 5G Working Group - INSA Cyber Council, "The National Security Challenges of Fifth Generation (5G) Wireless Communications - Winning the Race to 5G, Securely" (Intelligence and National Security Alliance (INSA), June 2019), https://www.insaonline.org/wp-content/uploads/2019/06/INSA_WP_5G_v5_Pgs.pdf.

[12] Andy Purdy et al., "Don't Trust Anyone - The ABCs of Building Resilient Telecommunications Networks," *PRISM* 9, no. 1 (October 2020): 115–29.

[13] ANFr, "Perturbations du fonctionnement des radars fixes de l'aviation civile et de la défense par les éoliennes," May 2, 2006, https://www.anfr.fr/fileadmin/mediatheque/documents/etudes/Rapport%20perturbations%20fonctionnement%20radars%20fixes%20Aviation%20Civile%20et%20Defense%20par%20eoliennes.pdf.10,12]]},"issued":{"date-parts":[["2006",5,2]]}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"} which covered the question of static Civil aviation and Defence radars (static air monitoring radars).

[14] US Joint Chiefs of Staff, "Joint Publication 3-85 - Joint Electromagnetic Spectrum Operations," Joint Publication, May 22, 2020, https://fas.org/irp/doddir/dod/jp3_85.pdf.

[15] Department of Defense, "DoD Strategic Spectrum Plan" (US DoD, February 2008), https://www.ntia.doc.gov/files/ntia/publications/dod_strategic_spectrum_plan_nov2007.pdf.

[16] "Electromagnetic Spectrum Superiority Strategy" (US DoD, October 2020), https://archive.defense.gov/news/dodspectrumstrategy.pdf.

[17] Sydney J. Freedberg Jr., "US Jammed Own Satellites 261 Times; What If Enemy Did?" Breaking Defense, December 2, 2015, https://breakingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-an-enemy-tried/.

[18] Curtis E. Lemay Center, "AFDP 3-51 Electromagnetic Warfare and Electromagnetic Spectrum Operation," Air Force Doctrine Publication 3-51 (US Air Force, July 30, 2019), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-51/3-51-Annex-EW-EMSO.pdf.

[19] "Electromagnetic Spectrum Superiority Strategy" (USA Department of Defense, 10/20), https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.

[20] Olivier Letertre et al., "Regards croisés sur la guerre électronique," *Etudes de l'Ifri* Focus stratégique, no. 90 (July 2019): 54.

[21] Roger N McDermott, "Russia's Electronic Warfare Capabilities to 2025" (International Center For Defense And Security (ICDS), September 2017).

[22] Jean-Jacques Mercier, "L'organisation de La Guerre Électronique Russe," *DSI*, no. 143 (October 2019).

[23] Aurélien Duchêne, "Guerre Électronique : Comment Les Capacités Russes Pourraient Fragiliser Les Forces Occidentales," Aurélien Duchêne, September 2020, https://aurelien-duchene.fr/guerre-electronique-russie/.

[24] Yannick Genty-Boudry, "Guerre Électronique, Le Multiplicateur de Force Russe," *DSI*, September 2019.

[25] Unknown, "In Syria Spotted New Russian RB-341V «Leer-3» Electronic Warfare System," *Defense News* (blog), 3, accessed January 14, 2021, http://defensenews-alert.blogspot.com/2016/03/in-syria-spotted-new-russian-rb-341v_14.html.

[26] Roger Cliff, "Anti-Access Measures in Chinese Defense Strategy" (RAND CORPORATION, 2011).

[27] Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China, Annual Report to Congress," 2020.

[28] Prepared Statment of Mr David Chen, Independent Analyst, "China's Advanced Weapons" (U.S.-China Economic and Security Review Commission, February 2017).

[29] Peter Vincent Dr. Pry, "CHINA EMP THREAT - The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack" (EMP Task Force on National and Homeland Security, June 10, 2020), https://securethegrid.com/wp-content/uploads/2020/06/CHINAempTHREAT2020logo.pdf.

[30] Brendan I. Koerner, "Inside the New Arms Race to Control Bandwidth on the Battlefield," *WIRED*, February 18, 2014, https://www.wired.com/2014/02/spectrum-warfare/.

[31] "IDF's Electronic Warfare Battalion: The Enemy's Headache," iHLS Israel Homeland Security, 2014, https://i-hls.tumblr.com/post/106593530750/idfs-electronic-warfare-battalion-the-enemys.

[32] Simon Ballantyne, "Wireless Communication Security: Software Defined Radio-Based Threat Assessment.," 2016, 72.

[33] Philippe Gros, "Les Opérations En Environnement Électromagnétique Dégradé" (IFRI, Observatoire des conflits futurs, May 2018), 10.

[34] Sydney J. Freedberg, "US Has Lost 'Dominance In Electromagnetic Spectrum,'" Breaking Defense, September 3, 2014, https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/.

[35] Brendan l. KOERNER, "Inside the New Arms Race to Control Bandwidth on the Battlefield," *WIRED*, n.d., file:///C:/Users/steph/Zotero/storage/36IQQGWH/spectrum-warfare.html.

[36] Bryan Clarck, Whitney Morgan Mc Namara, and Timothy A. Walton, "Winning the Invisible War - Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum" (Center for Strategic and Budgetary Assesments (CSBA), 2019), 3, https://csbaonline.org/uploads/documents/Winning_the_Invisible_War_WEB.pdf.

[37] Clarck, Mc Namara, and Walton, "Winning the Invisible War - Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum," 2019, 25.

[38] John G. Casey, "Cognitive Electronic Warfare: A Move Towards EMS Maneuver Warfare," *Over The Horizon (OTH)*, July 3, 2020, https://othjournal.com/2020/07/03/cognitive-electronic-warfare-a-move-towards-ems-maneuver-warfare/.

[39] Matthew J Florenzen, "Unmasking the Spectrum with Artificial Intelligence," *JFQ Quarterly* 95 (October 2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-95/jfq-95_116-123_Florenzen-Skulkitas-Bair.pdf?ver=2019-11-22-151711-083.

[40] Rajesh Uppal, "With China Rapidly Militarizing Quantum Technologies, U.S. Army Funding Assessment of Military Potential of Quantum/Electronic Warfare (EW) Based Threats | International Defense Security & Technology Inc.," May 29, 2019, https://idstch.com/threats/china-rapidly-militarizing-quantum-technologies-u-s-army-funding-assessment-military-potential-quantumelectronic-warfare-ew-based-threats/.

[41] Patrick Tucker, "Army Creates Quantum Sensor That Detects Entire Radio-Frequency Spectrum," Defense one, February 8, 2021, https://www.defenseone.com/technology/2021/02/army-creates-quantum-sensor-detects-entire-radio-frequency-spectrum/171939/.2,9]]},"issued":{"date-parts":[["2021",2,8]]}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}.

[42] Clarck, Mc Namara, and Walton, "Winning the Invisible War - Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum," 2019, 39.

[43] Roger N McDermott, "Russia's Electronic Warfare Capabilities to 2025" (International Center for Defence and Security - Republic of Estonia Ministry of Defence, September 2017), https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

[44] Dr. Pry, "CHINA EMP THREAT - The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack."

[45] World Bank, "World Development Indicators," n.d., https://datatopics.worldbank.org/world-development-indicators/.

[46] Angus Maddison, *The World Economy: Historical Statistics*, OECD Publications, 2003, https://www.oecd-ilibrary.org/development/the-world-economy_9789264104143-en.

[47] World Bank, "World Development Indicators."

[48] CEBR, "World Economic League Table 2021," December 2020, 231, https://cebr.com/wp-content/uploads/2020/12/WELT-2021-final-23.12.pdf.

[49] Maddison, *The World Economy: Historical Statistics*.

[50] SIPRI, "Military Expenditure Database," 2020, https://www.sipri.org/databases/milex.

[51] "MALD Decoy | Raytheon Missiles & Defense," www.raytheonmissilesanddefense.com, accessed January 16, 2021, https://www.raytheonmissilesanddefense.com/capabilities/products/mald-decoy.

[52] Scott Ritter, "'Like Horse-Mounted Cavalry against Tanks': Turkey Has Perfected New, Deadly Way to Wage War, Using Militarized 'Drone Swarms' — RT Op-Ed," www.rt.com, November 2020, https://www.rt.com/op-ed/508000-turkey-drone-swarms-war/.

[53] Mark Pomerleau, "US Army Working on New Electromagnetic Deception Tool," C4ISRNET, November 23, 2020, https://www.c4isrnet.com/electronic-warfare/2020/11/23/us-army-working-on-new-electromagnetic-deception-tool/.

[54] Aymeric Bonnemaison and Stéphane Dossé, *Attention : Cyber ! Vers le combat cyber-électronique*, 1re édition (Paris: Economica, 2014).

[55] Laurent Lagneau, "Les positions de l'artillerie ukrainienne trahies par une application pour téléphone mobile," www.opex360.com, *Zone Militaire* (blog), December 23, 2016, http://www.opex360.com/2016/12/23/les-positions-de-lartillerie-ukrainienne-trahies-par-application-pour-telephone-mobile/.

Insurrection at the U.S. Capitol: QAnon Shaman, Jake Angeli" (Johnny Silvercloud At Shutterstock)

Pride of Place

Reconceptualizing Disinformation as the United States' Greatest National Security Challenge

By David V. Gioe, Margaret Smith, Joe Littell, and Jessica Dawson

On January 6, 2021, long held assumptions about the meaning of American national security were challenged when insurrectionists stormed the United States Capitol, attempting to overturn the results of the 2020 Presidential election. Largely fueled by a toxic combination of mis- and disinformation about American democratic institutions, processes, and elections, the insurrection highlights how misguided mob power—energized by false information—can have devastating results. Interestingly, the attackers were not social outliers and recent polls indicate that nearly 20 percent of Americans approved of the insurrection.[1] What the attack on the Capitol suggests, is that America's civil society is struggling to function. Social norms are being challenged and morphed by the current contested information environment, which poses an urgent and existential threat to democracy—namely, a declining respect for government and institutional norms, a diminishing trust in foundational democratic processes, and a growing aversion to the rule of law. In the contested information environment, both domestic and foreign actors use mis- and disinformation for malign and malicious purposes and, if left unchecked, the information environment presents adversaries with an attack surface that conventional national security measures fail to secure.[2] Ultimately, the speed and scale at which mis- and disinformation penetrate and disrupt civil society is America's most urgent national security challenge.

Surprisingly, "fake news" only entered the American lexicon in 2016,[3] but mis- and disinformation—and America's increasing receptivity to it[4]—have been eroding American democratic norms for decades.[5,6] Mis- and disinformation generate domestic chaos by championing falsehoods couched in seemingly legitimate sources of information designed to chip away at social cleavages. Additionally, mis- and disinformation undermine public trust in democratic institutions, denigrating public esteem in science, journalism, higher education, and health systems, among others. Yet, the domestic strife resulting from foreign and domestic mis- and disinformation campaigns was not identified as a threat in any U.S. national security strategy until very recently.

All authors are researchers affiliated with the Army Cyber Institute at West Point. Additionally, David V. Gioe is Visiting Professor of Intelligence and International Security in the Department of War Studies at King's College London. Jessica Dawson is a sociologist who focuses on extremism, morality, narratives, and social change that comes from the digital disruption of social processes. Joe Littell is a U.S. Army officer and graduate of Duke University, and Margaret Smith is a U.S. Army officer and assistant professor in the West Point department of social sciences. This analysis is solely that of the authors and does not reflect any official position of the U.S. Military Academy, the Department of Defense or the United States Government.

This article is written in response to the Capitol insurrection and is motivated by the thesis that democracy cannot exist without a shared reality. Additionally, threats to a nation-state's shared reality are threats to the state's continued existence and should be prioritized accordingly. We argue that the national security concerns resulting from mis- and disinformation mandate a coordinated and well-resourced government response. In the following sections we first address the development of mis- and disinformation to identify the roots of the current crisis. We then explain why the threat from mis- and disinformation represents a national security crisis, and finally, we identify potential solutions to mitigate mis- and disinformation's ability to deepen societal divisions in America. Potential policy solutions include increasing awareness and attention from national security leaders, raising public concern about the deleterious effects of mis- and disinformation, and fostering a proactive and educated public to assist in curbing the spread of mis- and disinformation.

The Curious Absence of Disinformation in U.S. National Security Strategies

The first National Security Strategy of the George W. Bush Administration contains a striking omission: the document fails to mention the threat of mis- or disinformation.[7] President Bush's second National Security Strategy suffers from the same oversight and only briefly discusses threats emanating from "sub-cultures of conspiracy and misinformation"[8] in the context of Salafi jihadism. "Terrorists," the Bush Administration explains,

> recruit more effectively from populations whose information about the world is contaminated by falsehoods and corrupted by conspiracy theories. The distortions keep alive grievances and filter out facts that would challenge popular prejudices and self-serving propaganda.[9]

Yet, over the past decade, it is increasingly apparent that mis- and disinformation, and the security threats they pose, are not limited to the likes of al-Qaeda, the Islamic State, or fringe conspiracy groups.

Making only minor improvements to the Bush Administration's strategy, the Barack Obama Administration included a passing reference to "Moscow's deceptive propaganda" on page 25, of a 29-page document.[10] It was not until the Donald Trump Administration that mis- and disinformation were given more attention, noting that "America's competitors weaponize information [and] disseminate misinformation and propaganda."[11] Striking a markedly different tone than previous administrations, the Trump White House determined the threat was not from divergent and disparate terrorist groups, but instead from "America's competitors," elevating the threat from nonstate actors to state-supported activities.

Despite their destructiveness, mis- and disinformation campaigns have failed to garner much attention from the national security community. Naturally, every administration's National Security Strategy reprioritizes all security threats based on the current operational context and their governing agenda. But, even the most recent strategies have fallen short by failing to identify the domestic and foreign variants of mis- and disinformation as a primary national security threat. To be precise, the threat is not the malign information, but is instead the American public's inability to manage and mitigate mis- and disinformation that poses the urgent threat. The effect is an undermining of America's shared reality and a fracturing of the framework through which Americans understand global developments as well as domestic issues.

The Joe Biden Administration has an opportunity to remedy past national security oversights by

including a robust discussion of threats from mis- and disinformation as it crafts its own National Security Strategy. The Biden Administration claims, "this moment is an inflection point," and we agree, believing that a shared reality is necessary for membership in the community of values that defines America. America cannot act with unity or purpose, globally or domestically, if it is a "house divided" against itself, to borrow Abraham Lincoln's famous metaphor.

In early March 2021, President Biden released an Interim National Security Strategic Guidance, outlining the administration's security posture as a final version is produced.[12] Promisingly, disinformation is covered in detail as a threat to American and global democracy:

> Anti-democratic forces use misinformation, disinformation, and weaponized corruption to exploit perceived weaknesses and sow division within and among free nations, erode existing international rules, and promote alternative models of authoritarian governance.[13]

Unlike past administrations, the interim guidance clearly identifies disinformation as a threat and insists that if global democratic values are to survive, America must regain the trust of its allies and rejuvenate the public's trust in its domestic institutions. However, despite outlining the threat of disinformation and the dangers posed by it, the interim guidance does not discuss mitigation efforts as prescriptive and substantive policy solutions are not included in the report. We therefore see this article as an opportunity to contribute in a specific manner toward crafting a forthcoming Biden administration National Security Strategy document that contains a strategy to appropriately deal with mis- and disinformation.

Reimagining and Reordering Threats

Because the Biden Administration has emphasized that it wishes to chart a new course in national security, we propose an update to how national security challenges are imagined and defined. Our reimagining will undoubtedly make America's national security apparatus uncomfortable but, throughout history, technological advancements and innovations have changed the character of warfare with corresponding re-conceptions of threat, purpose, and national defense. Examples include heavy armored vehicles, air power, nuclear technology, the internet, and militarized space to name but a few. Despite hiccups in implementation, American doctrine and theory have routinely adapted to account for substantial changes in technology, adversary competence, and intent. We therefore argue that acknowledging the widespread and hostile dissemination of disinformation as a top national security concern—and adjusting the U.S. national security posture to reflect the change—is necessary and achievable in the near term.

Unlike other security threats, mis- and disinformation are an epistemic threat—a threat to what people believe is *real*. Knowledge should be understood not as an individual attribute but rather, as "socially distributed."[14] Over the last forty years, the civic institutions that help define what is real and what is true have been steadily eroded,[15] giving malign actors a vector to distort and undermine the American public's shared reality. For the purposes of this article, we endorse the articulation of "shared reality" described by Gerald Echterhoff and E. Troy Higgins:

> the experience of having in common with others inner states about the world. Inner states include the perceived relevance of something, as well as feelings, beliefs, or evaluations of something. The experience of having such inner states in common with others fosters the perceived truth of those inner states.[16]

Humans are motivated to create shared realities because they establish a grounding truth about

the world around us. Religious affiliations are a good example: shared beliefs create a rooted sense of identity among a congregation and a common way of understanding the world and explaining its mysteries. By developing shared realities, Echterhoff and Higgins claim, people can fulfill a basic need by establishing valid beliefs about the world. People with a shared reality are bound by common values and a common understanding of the world and their place in it. As a result, shared realities enable people to interpret events and underlying facts in a similar manner or from a common place of understanding. To extend the claim, we argue that a common construct underpins the way a polity interacts with—and acts within—a nation-state. To continue the parallel with organized religion, many church denominations have splintered through divergent understandings of Biblical teachings. In the same way, societies can also fracture along lines of interpreted reality.

The most recent example of fissures to an American shared reality is the January 6 insurrection. As the mob breached the Capitol, it became clear that Americans do not live in a common, fact-based, shared reality. Perhaps more controversial than acknowledging that Americans are not rooted in a shared reality, is our assessment that the public's appetite for confirmational and explanatory disinformation over fact-based sources far exceeds the conventional national security threats, like belligerent foreign powers, nuclear proliferation, and Salafi-jihadist terrorism. Without a shared reality, truth becomes negotiable, existing on a spectrum and leaving a confused and agitated American public without a common understanding of current events. After January 6, and despite the negative impact of leaving Washington D.C. in an extended military lockdown, many leaders agreed that mis- and disinformation surrounding the election, voting systems, and the Biden administration's legitimacy mandated the deployment of over 20,000 National Guard troops to safeguard the Capital. The United

Voter Fraud' rally marches to Supreme Court in support of Donald Trump, who refused to concede election. (Bob Korn at Shutterstock: 186799326

States has not experienced a similar domestic security posture since the days immediately following the September 11, 2001 (9/11) attacks.

The American military response to 9/11 also provides a useful foil in the disinformation fight. During the Cold War, "hard" applications of conventional military power (and their deterrent effect) were enough to maintain the superpower standoff. In contrast, the disinformation challenge has more in common with terrorism or climate change because the root problems are complex and applications of conventional power are ill-suited to manage the problem, much less claim a victorious end-state. In this case, America's formidable military might has little application to countering false and misleading narratives, but the Pentagon has been slow to apprehend this development. Unlike the Cold War, the response to mis- and disinformation must include a "whole of society" approach, as we will explore in greater detail after a brief overview of America's historically skeptical relationship to centralized authority and an identification of how foreign actors have sought to exploit this inherently American trait.

Evolution of a Disinformation-Driven Security Crisis

Nearly two hundred years ago, sociologist Harriette Martineau argued that America had done the impossible: it had demonstrated that self-rule was possible.[17] Contrary to oversimplified accounts of early American harmony, Martineau's investigation of society in America in the first post-Revolution generation also underscores how democracy in America has always been contested and shaped by public debate. Martineau would have recognized many of contemporary America's political traditions in which elected officials routinely apply a partisan spin to social issue framing, leading to disparate narratives, confusion over facts, and two distinct shared realities based on political persuasion.

Of course, different viewpoints and perspectives have always existed to some degree; indeed, these are the basis of political ideologies and parties, but Reuben E. Brigety II argues that the 2020 presidential campaign may have been a watershed tipping point because it exposed societal cleavages and how party identity is linked to a foundational identity, like race or religion.[18] Moreover, when foundational identities become the organizing principle of a country's political life, tribal conflict becomes more likely. Brigety emphasizes that "the [2020] campaign looked less like a contest of ideas and more like a battle between tribes, with voters racing to their partisan corners based on identity, not concerns about policy."[19]

While American political parties have long-running stereotypes associated with their respective constituents, party affiliation was heretofore less public and more private, leaving people more inclined to build communities and friendships based on more robust, less divisive civic identities unattached to politics. As these diffuse civic organizations have declined over the last 40 years,[20] they combined with neighborhood sorting that moved Americans into more and more homogenous neighborhoods,[21] perhaps a proto-filter bubble presaging the type of sorting done by and through social media. As we will explore, filter bubbles and echo-chambers threaten shared reality, which we identify as a prerequisite for productive policy deliberation. When this common operating picture becomes unrecognizable to a large number of voters, it is almost foreordained that civil chaos should follow. America's culture wars, coupled with declining trust in American institutions, have helped harden the ideological and foundational identities affixed to political parties. If things become brittle once hardened, the trajectory of such tribalism in American political and civic life is alarming, and the canaries are already in the coalmine.

For those paying attention to the steady erosion of confidence in American norms and institutions

over the past few decades, the events of January 6 did not come as a surprise. For several years, a systematic influence campaign aimed at undermining public trust has occurred, directed at institutions like the courts, elections, and the broader mechanisms inherent to democracy, although the erosion of trust and the January 6 attack on the U.S. Capitol was *not* solely caused by conspiratorial fiction about democratic institutions spread via mis- and disinformation campaigns. Some of the recent decline in public trust is warranted and expected, as societal norms have changed in response to increasing access to information and rapid globalization brought about by the internet. In fact, some antecedents to January 6 are *real* events and *real* public concerns, but influencers, media personalities, and charlatans have taken fact-based threads and twisted them together with falsehoods, weaving tales and drawing connections between stories and events to create a pseudo-reality that no longer resembles the facts, but instead supports their specific political and social agendas. We now provide a brief historical overview to illuminate the conspiratorial threads that, when woven together, help explain the troubling events at the Capitol.

Distrusting government is not new and the experiences of the past two generations justify a healthy criticism of government and raise the legitimate question of whether the government is worthy of the public's trust. The Watergate scandal, the Pentagon Papers, and the Vietnam War all tested public trust in government. Those examples left the Baby Boomer generation with a lingering skepticism of their leaders and institutions. Trust has not improved in younger generations because of the September 11, 2001, attacks and the "forever wars" in Iraq and Afghanistan. Operation Iraqi Freedom began with an intelligence failure and nearly every official who used the word "progress" to describe America's ongoing presence in Afghanistan was being dishonest with the American people.[22] Ultimately, the already low trust in government created a fertile field for conspiracy theories crafted from mis- and disinformation to take root. Mis- and disinformation do not circulate in isolated information systems – instead, they intersect with, and shape, society's natural information flow guided by social media. Into that complex ecosystem entered the Russians.

Enter the Russians

In 2015, conspiracies about Jade Helm, a routine military training exercise that takes place across Texas and the greater American west, rose to prominence on social media, bringing previously fringe ideas to the news feeds of a large, mainstream audience.[23] Russian cyber actors, mimicking American social media users online, propagated radical theories about Jade Helm, claiming that the military exercise was really being used by the Obama Administration as a ruse to round up its political opponents.[24] Analysis of the Jade Helm conspiracy tends to focus on the success of the Russian influence and how the campaign even led the Texas Governor to publicly question the true purpose of the training exercise. However, less emphasized is the strain of deep-seeded anti-government sentiment that the Jade Helm conspiracy reveals, and it justifies the Russian approach in that vein.[25] Legitimate concerns about armed government overreach at incidents like Ruby Ridge, Idaho, in 1993 and Waco, Texas, in 1994 fed into the suspicion fueling the anti-government militia movement.[26] These fringe concerns about the military exercise entered the mainstream political sphere as politicians sought to capitalize on the public's outrage for political advantage.[27] Such distortions from reality provided fertile soil for a Russian disinformation campaign.

If the 2015 Jade Helm exercise was a proof of concept for Russian meddling via social media, operating in the American information environment became a full scope operation by 2016. Even though most Americans likely became aware of Russian influence operations following documented

Russian interference in the 2016 presidential election,[28] Russia has meddled in U.S. media and social narratives for decades before the advent of social media.[29] The legacy of Russian interference dates back to the fall of tsarist Russia and was a hallmark of the Cold War, and we can credit Russia, China and other foreign actors (all adept at information operations) with exposing how vulnerable American society is to mis- and disinformation and, more importantly, how inept Americans are at mitigating it. The Russians did not create American suspicion of the federal government but, the Russian influence campaign surrounding Jade Helm skewed, weaponized, and amplified long-standing American narratives, harkening back to President Ronald Reagan's claim that "government is the problem,"[30] twisting a conservative skepticism of government overreach into outright distrust. To make matters worse, as the Jade Helm conspiracy gained momentum, it was not quashed but was instead humored by Texas state officials, giving the conspiracies and false narratives an air of legitimacy.[31]

It is hard to overstate this fork in the road for the Russian approach to American audiences.[32] Russia's Jade Helm-related active measures worked, and the ease with which the Jade Helm disinformation campaign took over the mainstream narrative proved just how easily the American public could be swayed via digital means, ultimately paving the way for Russia's (and others') digital influence activities during the 2016 election and beyond.[33]

Foreign Disinformation Flourishes Amid Domestic Social Discontent Amplified by Social Media

It is critical to note that foreign adversary influence operations have not created nor invented the schisms in American society; instead, they identify,

Facebook launches PR campaign as public backlash after Cambridge Analytica scandal and Russian interference in 2016 elections. (NYCStock)

exploit, and exacerbate them. Domestically generated discontent is what brought protestors to the Capitol on January 6 and the most extreme of them arrived with pipe bombs, zip ties for handcuffing hostages, and calls for executions.[34] This is a rich environment for foreign and domestic malevolent actors to ply their trade. In a sense, even if the seeds are foreign, the fertile field is American, and this blurring of the lines between foreign and domestic disinformation leaves American national security mandarins and agencies in uncomfortable territory in terms of legal authorities, lanes of the road, and responsibilities for combatting a polluted information environment that does not recognize national boundaries.

Above we identified factors like the erosion of trust in government that make citizens more receptive to mis- and disinformation. According to multiple academic studies, one in four Americans believes in at least one conspiracy theory, and, perhaps unsurprisingly, belief in one is strongly predictive of belief in other conspiracies.[35] Research also shows that conspiracy theories are often partisan and that one of the strongest predictors of a person's receptivity to specific conspiratorial ideas is their political orientation.[36] On January 6, the attacking mob was joined in spirit by millions of Americans watching from home, representing a variety of backgrounds, and spread across social strata. Many passive supporters agreed with the mob and had also lost trust in the American government, believing oft-repeated claims of a stolen election.[37] Based on the close 2020 election and scholarly evidence linking political affiliation to a person's susceptibility to specific conspiratorial narratives that align with their political beliefs, America's lack of a shared reality for electoral outcomes is hardly surprising—realities diverge as partisan polarization increases.[38] Tying several strands together, a recent Pew survey found striking differences along party lines regarding the impact of the COVID-19 pandemic, election legitimacy, willingness to accept the vaccines, and other critical elements necessary to coexist in society.[39] It seems clear that diverging shared realities appear to be largely driven by partisan politics, and it is therefore understandable that foreign influence operations would wish to join domestic actors and focus their attention on that civically-vulnerable area.

Just as deceitful government activity such as Watergate or hyped up intelligence over the justification for the Iraq war seemed to justify or warrant popular skepticism, the most successful mis- and disinformation campaigns are often rooted in fact or closely mimic actual events. Most of the public reacted in horror to the 2016 "Pizzagate" tragedy, when a man traveled from his home in North Carolina to Washington, D.C., and fired a rifle into a pizza restaurant. The man was there to investigate the alt-right (loosely connected online white supremacist groups) claim that the pizza restaurant was really a cover for a child sex-trafficking ring run by wealthy and socially well-connected Americans. On the surface, the claim sounds ridiculous, but not long after the pizza parlor shooting, wealthy socialites, Jeffrey Epstein and Ghislaine Maxwell[40] were charged with a similar crime, leading many to believe the alt-right was correct in its suspicions. The "Pizzagate" event highlights how extreme narratives are often validated by actual events and how conspiracy theories are often underwritten by historical events or prior incidents.[41]

Digital Technology and Social Media Amplify and Enable Foreign Disinformation Operations

The social media ecosystem has expanded and accelerated the propagation of mis- and disinformation.[42] Acting like a megaphone, social media has incited violence and allowed foreign trolls, domestic politicians, cable news hosts and other influencers to spread falsehoods, place blame, and target opposition groups. While conspiracy theories and alternative realities have long histories,

digital information technology—particularly social media—has enabled their spread, allowed believers to easily connect, and developed a cadre of vocal leaders to coordinate attacks in virtual and physical spaces.[43] The mix of legitimate grievances, mis- and disinformation, and unchecked social media algorithmic amplification is both driving and providing the soil for this national security crisis.[44]

Various geopolitical adversaries have identified this gap in the U.S. national security posture and have begun exploiting it, even down to the local level where hostile foreign actors have sought to exacerbate American suspicions about electoral integrity. For instance, the past few American elections have seen the increasingly populous state of Florida act as a swing state with each political party competing doggedly for every vote. In October 2020, weeks before the November election, many Floridians received menacing emails from an address associated with alt-right group, the "Proud Boys," threatening harm if they did not vote for President Donald Trump and change their voter registration to Republican. Proud Boys leadership denied any involvement and U.S. authorities were hasty to pin the blame on Iranian actors using overseas servers to spoof Proud Boys emails. U.S. intelligence officials also noted a video, apparently sponsored by Iran, that suggested ways to fraudulently cast ballots.[45]

These efforts at stoking voter skepticism were predicted in advance as early as August 2020 by the U.S. National Counterintelligence and Security Center, which issued an assessment that "Iran seeks to undermine U.S. democratic institutions, President Trump, and to divide the country in advance of the 2020 elections." Further, "[their efforts] probably will focus on online influence, such as spreading disinformation on social media and recirculating anti-U.S. content."[46] It seems reasonable that Iran would choose to act to undermine voter confidence when leading American politicians were preemptively doing the same thing. Iran, however, was far from the only foreign actor to appreciate the vulnerable American attack surface.

If Iran's rather ham-handed approach to election meddling seemed opportunistic, Russia's concept of Hybrid Warfare[47] and Chinese Three Warfares[48] have thoughtfully considered the power of influence operations at the strategic level, and, in turn, have drastically restructured their vision for how malevolent influence operations against the United States should be conducted. Both strategic approaches subordinate conventional kinetic warfare to overarching information campaigns, drastically reducing U.S. military capabilities to intervene or muster the political will to contest the outcome.

Russian actions within the Ukraine mirrored similar operations domestically in the United States. Sowing distrust and instability[49] within a region allows for a contested information environment in which further disinformation campaigns can thrive. Russian forces regularly harassed and attacked racial minorities such as the Roma, Jews, and Hungarians within Crimea, attempting to blame the actions on Ukrainian forces.[50] Direct harassment and psychological warfare was conducted against Ukrainian soldiers on the front lines through phone calls and text messages to them and their families to torment them.[51] This closely mirrors efforts by Russia in the United States to cause racial division amongst African Americans and the population at large, playing to both pro- and anti-police narratives.[52] Russia furthermore pushes transnational white supremacist extremism in both the United States and Russia.[53] Numerous controversial American white supremacists like David Duke and Richard Spencer have praised Russia for their efforts in promoting white supremacy.[54] Spencer's ties run even deeper, as he was married to Nina Kouprianova,[55] a Russian national, long-time adherent of Russian nationalist icon Aleksander Dugin,[56] and Kremlin mouthpiece.

China's efforts have also ramped up to exploit vulnerable flanks in East Asia and beyond.

Previously these methods were predominately focused on regional adversaries, such as Taiwan or Vietnam,[57] and China's maritime ambition for complete control over the South China Sea. Operations utilized a myriad of approaches to include aggressive seaborne expansion and fortification, use of ambiguous naval militias, and use of non-internationally recognized maps of territorial waters to sway the narrative.[58] More ambitious Chinese efforts included informational forays against academia,[59] professional sports,[60] and Hollywood.[61] Chinese academic espionage resulted in numerous arrests in 2020 and the investigation of 189 more grant recipients, 54 of which had undisclosed foreign ties to China.[62] Both the NBA,[63] and American video game developer Blizzard-Activision[64] found themselves censoring employees in response to anti-democratic crackdowns in Hong Kong, showing further how China can influence large numbers of Americans through its leverage of multinational corporations. Chinese media markets are heavily regulated by the government, requiring all Western movies entering the market to show China in a positive light.[65] Considering Hollywood's reach into the American movie goer audience, many citizens only know of China through its portrayal in films, thus muddying the waters. Increasingly, following the global COVID-19 pandemic, China has shifted heavily into online social media channels, particularly anglophone ones to contest the narrative that it was to blame for the outbreak and insufficient initial response. To argue in favor of its role in combating the pandemic China has attempted to discredit U.S. and other Western democratic responses, as well as shift their culpability in the outbreak's origins.[66]

Solutions for Malign Digital Interference

As the above sections illustrate, the threat is urgent, complex, and non-traditional. Any whole-of-nation response to malign manipulation of the information environment requires both government and private sector responses, cooperative public-private partnerships, and tasks and responsibilities down to the level of the individual citizen. The balance of this article will explore some necessary steps and adjustments toward addressing the disinformation threat.

Technical responses are often the first ones proposed when addressing digital threats, yet consensus on a technical response has yet to emerge. As Jon Bateman and Craig Newmark have complained, "Social media disinformation discussions are going in circles."[67] Currently many filtering algorithms and methodologies are being tested by large social media platforms. Twitter has attempted to use warnings and forms of soft moderation surrounding COVID-19 and the results of the 2020 U.S. Presidential election,[68] with varying results.[69] Other platforms, such as Reddit, have attempted to de-platform individuals and groups in order to meet the same ends.[70] Often these de-platforming methods have merely slowed the movement of information temporarily, as users migrate to more salient platforms.[71] However, many argue that such filters encroach on First Amendment rights and limit user capacity to practice thinking critically about the information they ingest.[72] This has caused a schism politically where platforms like Voat, Gab, and Parler, among others, have marketed themselves as platforms of free speech.[73]

These methods are reactive and do not account for emergent technologies such as generative adversarial networks, or GANs, algorithmic confounding, and data poisoning. GANs have already gained traction through their use in Deepfakes,[74] a technology so democratized that a mother in Pennsylvania used it against her daughter's teenage rivals.[75] Algorithmic confounding and data poisoning can be used to circumvent previously mentioned attempts at filtering, forcing additional users to see false or misleading content at a greater rate than typical of an average user.

However, most recommendation engines and content filtering technologies actually push users to more extreme viewpoints by surrounding them with media and content that reaffirms prior beliefs, reinforces already formed opinions, and connects them to similarly extreme users.[76] For example, 64 percent of Facebook users who join extremist groups do so because of algorithmic recommendations.[77] Essentially, filtering algorithms create echo chambers that normalize radical ideas and extreme opinions, amplifying bias and dangerous behaviors,[78] working within existing societal schisms, offering justifications for existing fears or prejudices.[79] For example, research from the University of Warwick demonstrates a correlation between increased Facebook usage and violence against immigrants.[80]

Social media has many benefits, such as playing a critical role in keeping socially distant loved ones connected during the COVID-19 lockdown, but the filtering of society into isolated media and content bubbles has created multiple shared realities instead of unifying citizens under a single shared reality. If social media is hard to police, it is also still largely unfiltered, allowing prominent voices, however extreme, to spread mis- and disinformation.[81] The result is a far more complicated world, with multiple realities existing in an information nightmare that is difficult to dissect, understand, or combat.[82]

The terms "alternative facts" and "fake news" became popular vernacular in the "post-truth" era of the Trump Administration, but these are just the newest iterations of mis- and disinformation tactics.[83] What is different today is how social media platforms and technology amplify the problem to a scale without historical precedent.[84] Winston Churchill's quip, "a lie is half-way around the world before the truth has a chance to put its pants on," is now woefully outdated as recent studies confirm that mis- and disinformation travel, on average, 6 times faster than fact.[85] As algorithms are designed for amplification of engagement, verified truth and legitimate news sources do not stand a chance against computational propaganda.[86] Yet there are promising developments. NewsGuard, for example, is a technology popularized when Microsoft implemented it into its Edge browser, that gives trust ratings to users as they browse websites.

To mitigate the risks associated with mis- and disinformation, America should reintroduce civic education into elementary education and, continue it through a child's entire academic career to grow a robust, active, and engaged public. Civic engagement is an investment in democracy and students need to understand how their involvement is critical to the health of their country. Modern civic education should be directed towards media and information consumption to help raise a public capable of coping with a saturated information environment flush with mis- and disinformation. Curricula should encourage active engagement with trusted media sources, teaching students to tease out facts, identify bias, and draw informed conclusions. Finland provides a good example and currently leads the world in digital media education,[87] scoring among the very highest of countries in indices relating to the strength of its democracy[88] and the digital literacy of its population.[89] With targeted civic education aimed at civic institutional knowledge and digital literacy, America can build a more robust society that is less susceptible to mis- and disinformation.

Educational efforts must also encourage students to engage in civil discourse with people who have conflicting opinions. One effort, Millions of Conversations,[90] is a civic campaign founded by Samar Ali, a former White House Fellow and attorney. Ali's initiative encourages dialogue across parties, fostering conversation with the intent of healing social divisions. The effort encourages people to non-judgmentally exchange narratives—an activity that Joshua L. Kalla and David E. Broockman recently found can reduce exclusionary attitudes. Kalla and Broockman

conducted three experiments targeting exclusionary attitudes towards unauthorized immigrants and transgender people. They found that dialogue and interpersonal exchanges reduced exclusionary attitudes towards the marginalized out-groups. However, the key to Millions of Conversations and Kalla and Broockman's study is the *exchange* of narratives—one-sided, face-to-face conversations that deliver arguments produced no effect on exclusionary attitudes. To reinforce good civic behavior, America's leaders must set the example and reach across the aisle, giving citizens behavior to emulate. Leaders across the country should establish forums for narrative exchanges and encourage more grass-roots organizations like Millions of Conversations.

Additionally, elected officials should counter mis- and disinformation publicly, acting as a whistle-blower when they identify false narratives and as educator when they publicly correct a false or misleading story. Government agencies must get involved too—like the Cybersecurity and Infrastructure Security Agency (CISA), which took proactive steps—even developing the hashtag #protect2020 to support its campaign—to dispel election rumors by setting up a public website[91] to debunk popular myths about voting security and fraud. In a democracy, retribution for correcting falsehoods is dangerous and will discourage shared understanding—as when former CISA Director Christopher Krebs was fired[92] for coming out publicly against claims that the 2020 election was rigged. Because elected officials are beholden to the public, debate and civil discourse among citizens is critical to democracy.

Another cornerstone of digital literacy is the ability to detect false and misleading information—education, as discussed above, can grow a public less susceptible to conspiratorial thinking. However, simple detection is not enough, and detecting and removing mis- and disinformation on social media, at speed and scale, is not easy. Social media platforms are currently drawing their own lines between legitimate and illegitimate online speech with the help of sophisticated yet non-transparent detection algorithms and extensive human involvement. It is impossible to catch and verify all false and misleading information, but the U.S. government should consider mandating greater transparency surrounding what content is moderated by private social media companies.

Additionally, social media firms should be held accountable on several fronts, most notably being how quickly they respond to fraudulent accounts, how thoroughly they respond to government oversight requests, how transparent they are with data usage and privacy policies, and the transparency of their content filtering mechanisms. Government regulation may be required, but ultimately, technology companies cannot solve the mis- and disinformation crisis and it remains the responsibility of every citizen to engage in critical thinking and try to distinguish between news and "fake" news.

Yet, despite being the responsibility of every citizen to educate themselves on the threat of mis- and disinformation, the erosion of a shared reality makes people across all social strata[93] highly susceptible to mis- and disinformation or "fake" news. Interventions that target information nodes, like public figures with large social media followings or message board moderators, can influence previously isolated sectors of the internet. In a local or closed network, small amounts of information are shared and constantly reinforced by group members. Exacerbating the cycle of a closed information loop are social media and search engine algorithms. Injecting additional and diverse information sources into insular online communities may challenge the group's ideological status quo.

A team of researchers recently demonstrated that professional norms in journalism like fact checking, published corrections, and retractions

work to insulate people from conspiratorial thinking by providing oversight and reducing the incentive to print whatever will go viral.[94] Additionally, "lateral" reading (or reading more sources but less in-depth) as defined by Sam Wineburg and Sarah McGrew, emphasizes that people are more likely to believe something is true, even if it contradicts their own opinions, if they are exposed to multiple sources of contrary information instead of simply being told that they are wrong.[95] Ideological nudges, akin to Richard H. Thaler and Cass R. Sunstein's behavioral economic nudge concept, may therefore help break the extremist cycle by introducing new material and ideas into a digital thought bubble. It may be necessary to consider requiring social media companies to adjust their algorithms to ensure users view a variety of legitimate professional news sources.[96]

Finally, research suggests[97] that the rapid flow of online information discourages rational thinking and favors emotional and heuristic reasoning. Social media companies can decelerate the spread of between mis- and disinformation by slowing down or altering how information is shared on their platforms. Further, functionality could be changed to amplify verifiable information and bury spurious sources. However, social media companies are not incentivized to develop technology to retard information flow, which counters their business model, or to change functionality as changes may push people off their platform. Pressure, if not regulation, from government is required.

Despite the initiatives and efforts discussed above, a major gap remains—no single agency or department is responsible for developing or deploying technology to identify and combat mis- and disinformation. The U.S. government needs to identify a central organization with the mandate of countering mis- and disinformation, developing tools to protect and defend users, and building social information resiliency through coordinated education programs.

Conclusion

Conventionally understood national security threats do not require the American public or private sector to be actively involved in their management because the Pentagon, the FBI, DHS, and the Intelligence Community are charged to defend the nation and have historically managed national defense and security issues. But, as we have argued in this article, mis- and disinformation, reimagined as a national security threat, are qualitatively different from traditional conceptions of security threats; as the Capitol insurrection laid bare, perhaps they are even more urgent, thus requiring a reordering of U.S. national security priorities. Further, this vulnerable flank is well known to America's foreign adversaries, and they continue to assault it with seeming impunity.

Because political and civic discourse are increasingly taking place in the information space we have attempted to offer some fruitful avenues of approach for the Biden administration as it crafts its own national security strategy. This is but the tip of the iceberg, however, given the complexity of the challenge. While our recommendations cannot be considered comprehensive in a short article, we emphasize that public, private, and individual aspects are necessary for any truly comprehensive approach.

Despite the instrumental role technology has in amplifying and spreading mis- and disinformation, there is not a technical or government-provided solution to its threat. Instead, it is a whole-of-society threat and *everyone* has a role to play: the private sector, the government, and the public. Understanding and countering the threat of mis- and disinformation is critical to identifying additional interventions to increase the public's awareness of, and resiliency to, mis- and disinformation. Societal cohesion bolstered by information resiliency is an urgent matter of national security and we urge the Biden Administration to give pride of place in their national security agenda to the complex and urgent threat posed by mis- and disinformation. PRISM

Notes

[1] Craig Kafura, "What Americans Make of the January 6 Chaos at the Capitol", The Chicago Council on Global Affairs, 7 January 2021, https://www.thechicagocouncil.org/commentary-and-analysis/blogs/what-americans-make-january-6-chaos-capitol.

[2] Jeffrey M. Berry and Sarah Sobieraj, *The Outrage Industry: Political Opinion Media and the New Incivility*, Reprint Edition (Oxford: Oxford University Press, 2016); Benkler, Faris, and Roberts, *Network Propaganda*.

[3] Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics* (New York, NY: Oxford University Press, 2018).

[4] Hart, J. & Graether, M. (2018). "Something's going on here: Psychological predictors of belief in conspiracy theories. *Journal of Individual Differences 39*(4): 229-237.

[5] The impact of mis- and disinformation campaigns are not limited to America. For instance, Estonia, Georgia, Ukraine, the Philippines, Britain, and Turkey have all watched as their foundational identities, beliefs, and assumptions about their societies unraveled. See Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War against Reality*, 2019; Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (I.B. Tauris, 2020); Benkler, Faris, and Roberts, *Network Propaganda*.

[6] Conversely, China enforces a policy of tight information control to artificially ensure domestic tranquility and, most importantly, the continued control of the Chines Communist Party. See Kai Strittmatter, *We Have Been Harmonized: Life in China's Surveillance State* (Custom House, 2020).

[7] "The National Security Strategy of the United States of America", September 2002, accessed at https://2009-2017.state.gov/documents/organization/63562.pdf.

[8] "The National Security Strategy of the United States of America", March 2006, accessed at https://www.comw.org/qdr/fulltext/nss2006.pdf.

[9] Ibid, p. 10.

[10] "National Security Strategy", February 2015, accessed at https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf.

[11] "National Security Strategy of the United States of America", December 2017, p. 34, accessed at https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[12] "Interim National Security Guidance", March 2021, accessed at https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[13] Ibid, p. 7.

[14] Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, 10 (Penguin UK, 1991), 21.

[15] Robert Bellah et al., *Habits of the Heart: Individualism and Commitment in American Life*, First Edition, With a New Preface edition (University of California Press, 2007).

[16] Gerald Echterhoff and E. Tory Higgins (2018), "Shared reality: Construct and mechanisms", *Current Opinion in Psychology*, pp. 4-6. https://doi.org/10.1016/j.copsyc.2018.09.003.

[17] Harriet Martineau, *Society in America Volume 1* (Hard Press, 1837).

[18] Reuben E. Brigety II, "The Fractured Power: How to Overcome Tribalism", *Foreign Affairs,* March/April 2021, accessed at https://www.foreignaffairs.com/articles/united-states/2021-02-16/fractured-power.

[19] Brigety II, "The Fractured Power."

[20] Robert D. Putnam, *Bowling Alone: The Collapse and Revival of American Community*, 1st edition (New York, NY: Touchstone Books by Simon & Schuster, 2001).

[21] Bill Bishop and Robert G Cushing, *The Big Sort Why the Clustering of Like-Minded America Is Tearing Us Apart* (Boston, MA: Mariner Books, 2009); Charles A Murray, *Coming Apart: The State of White America, 1960-2010*, 2013.

[22] David V. Gioe, "The Afghanistan Papers and the Perils of Historical Analogy", *Lawfare*, 21 January 2020, accessed at https://www.lawfareblog.com/afghanistan-papers-and-perils-historical-analogy.

[23] Patrick Svitek, "Jade Helm 15: The Black Helicopters Are Coming. Well, Maybe Not," The Texas Tribune, May 1, 2015, https://www.texastribune.org/2015/04/30/abbotts-letter-puts-jade-helm-national-stage/.

[24] Cassandra Pollock and Alex Samuels, "Hysteria over Jade Helm Exercise in Texas Was Fueled by Russians, Former CIA Director Says," The Texas Tribune, May 3, 2018, https://www.texastribune.org/2018/05/03/hysteria-over-jade-helm-exercise-texas-was-fueled-russians-former-cia-/.

[25] Lane Crothers, *Rage on the Right: The American Militia Movement from Ruby Ridge to Homeland Security*, 0224th edition (Lanham, Md: Rowman & Littlefield Publishers, 2003); Jessica Dawson and DB Weinberg, "These Honored Dead: Sacrifice Narratives in the NRA's American Rifleman Magazine," *American Journal of Cultural Sociology*, 2020, https://doi.org/10.1057/s41290-020-00114-x; Jessica Dawson, "Shall Not Be Infringed: How the NRA Used Religious Language to Transform the Meaning of the Second Amendment," *Palgrave Communications* 5, no. 1 (July 2, 2019): 58, https://doi.org/10.1057/s41599-019-0276-z.

[26] Jess Walter, *Ruby Ridge: The Truth and Tragedy of the Randy Weaver Family*, Reprint edition (New York: Harper Perennial, 2002); Kenneth S. Stern, *A Force Upon the Plain: The American Militia Movement and the Politics of Hate*, First Edition edition (New York: Simon & Schuster, 1996); Dick Reavis, *Ashes of Waco: An Investigation* (New York: Syracuse University Press, 1998); Kathleen Belew, *Bring the War Home: The White Power Movement and Paramilitary America* (Cambridge, Mass: Harvard University Press, 2018), http://www.hup.harvard.edu/catalog.php?isbn=9780674286078.

[27] Leonard Zeskind, *Blood and Politics: The History of the White Nationalist Movement from the Margins to the Mainstream*, First Edition edition (New York: Farrar, Straus and Giroux, 2009).

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

[29] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (Farrar, Straus and Giroux, 2020); Timur Chabuk and Adam Jonas, "Understanding Russian Information Operations", *Signal*, 1 September 2018, accessed at https://www.afcea.org/content/understanding-russian-information-operations.

[30] Philip S. Gorski, *American Covenant: A History of Civil Religion from the Puritans to the Present* (Princeton: Princeton University Press, 2017).

[31] W. Gardiner Selby, "Doonesbury Says Greg Abbott Activated Texas State Guard in Case of Federal Martial Law and More," @politifact, June 19, 2015, https://www.politifact.com/texas/statements/2015/jun/19/doonesbury/doonesbury-says-greg-abbott-activated-texas-state-/. See also Matthew Yglesias, "The amazing Jade Helm conspiracy theory, explained", *Vox*, 6 May 2015, accessed at https://www.vox.com/2015/5/6/8559577/jade-helm-conspiracy.

[32] David V. Gioe (2018), "The Cyber operations and useful fools: the approach of Russian hybrid intelligence", *Intelligence and National Security*, 33/7, pp. 954-973. https://doi.org/10.1080/02684527.2018.1479345.

[33] Russia was not the only one who noticed America's social fragility and susceptibility to conspiratorial thinking, domestic fringe movements also took note.

[34] Elaine Godfrey, "It Was Supposed to Be So Much Worse", *The Atlantic*, 9 January 2021, accessed at https://www.theatlantic.com/politics/archive/2021/01/trump-rioters-wanted-more-violence-worse/617614/.

[35] S. Clarke, "Conspiracy Theories and Conspiracy Theorizing," *Philosophy of the Social Sciences* 32, no. 2 (June 1, 2002): 131–50, https://doi.org/10.1177/004931032002001; Michael Barkun, "Conspiracy Theories as Stigmatized Knowledge," *Diogenes*, October 25, 2016, 039219211666928, https://doi.org/10.1177/0392192116669288.

[36] J Hart and M Graether (2018). "Something's going on here: Psychological predictors of belief in conspiracy theories. *Journal of Individual Differences* 39(4): 229-237.

[37] Kafura, "What Americans Make…"

[38] Hart and Graether "Something's going on here."

[39] John Gramlich, "20 Striking Findings from 2020," *Pew Research Center* (blog), December 11, 2020, https://www.pewresearch.org/fact-tank/2020/12/11/20-striking-findings-from-2020/.

[40] Gordon Pennycook et al., "Understanding and Reducing the Spread of Misinformation Online," preprint (PsyArXiv, November 13, 2019), https://doi.org/10.31234/osf.io/3n9u8.and what can be done about it? In a first survey experiment (N=1,015.

[41] Barkun, "Conspiracy Theories as Stigmatized Knowledge."

[42] Renee DiResta, "Computational Propaganda: If You Make It Trend, You Make It True," *The Yale Review*, October 9, 2018, https://yalereview.yale.edu/computational-propaganda. See also David V. Gioe, Michael S. Goodman and Alicia Wanless (2019), "Rebalancing cybersecurity imperatives: patching the social layer", *Journal of Cyber Policy*, 4:1, 117-137, DOI: 10.1080/23738871.2019.1604780, and Daniel Dobrowolski, David V. Gioe and Alicia Wanless (2020) "How Threat Actors are Manipulating the British Information Environment", *The RUSI Journal*, 165:3, 22-38, DOI: 10.1080/03071847.2020.1772674.

[43] Christine Geeng, Savanna Yee, and Franziska Roesner, "Fake News on Facebook and Twitter: Investigating How People (Don't) Investigate," 2020, 14; Karen Hao, "He Got Facebook Hooked on AI. Now He Can't Fix Its Misinformation Addiction," *MIT Technology Review*, March 11, 2021, https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation/.

[44] Jessica Dawson, "Microtargeting as Information Warfare," *Cyber Defense Review*, December 7, 2020, https://doi.org/10.31235/osf.io/5wzuq.

[45] Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker, and Craig Timberg, "U.S. government concludes Iran was behind threatening emails sent to Democrats", *Washington Post*, 22 October 2020, accessed at https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida/.

[46] As quoted in Nakashima, et al.

[47] Mason Clark, "Russian Hybrid Warfare," *Institute For the Study of War,* Military Learning and The Future of War Series, September 2020, http://www.understandingwar.org/report/russian-hybrid-warfare.

[48] Doug Livermore, "China's "Three Warfares" In Theory and Practice in The South China See" *Georgetown Security Studies Review,* March 25, 2018, https://georgetownsecuritystudiesreview.org/2018/03/25/chinas-three-warfares-in-theory-and-practice-in-the-south-china-sea/.

[49] Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare": The Case of Ukraine," *Center For European Policy Analysis,* January 29, 2021, https://cepa.org/the-evolution-of-russian-hybrid-warfare-ukraine/.

[50] Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare": The Case of Ukraine."

[51] Kateryna Zarembo and Sergiy Solodkyy, "The Evolution of Russian Hybrid Warfare": The Case of Ukraine."

[52] Zilvinas Svedkaukas, Chonlawit Sirikupt, and Michel Salzer, "Russia's disinformation campaign are targeting African Americans," *The Washington Post,* July 24, 2020, https://www.washingtonpost.com/politics/2020/07/24/russias-disinformation-campaigns-are-targeting-african-americans/.

[53] Elizabeth Grimm Aresnault and Joseph Stabile, "Confronting Russias Role in Transnational White Supremacist Extremism." *Just Security,* February 6, 2020, https://www.justsecurity.org/68420/confronting-russias-role-in-transnational-white-supremacist-extremism/.

[54] Natasha Bertrand, "'A Model for Civilization': Putin's Russia Emerges As 'A Beacon for Nationalists' and the American Alt-Right", *Business Insider,* December 10, 2016, " https://www.businessinsider.com/russia-connections-to-the-alt-right-2016-11.

[55] Natasha Bertrand, "A Model for Civilization."

[56] Alan Ingram, "Alexander Dugin: Geopolitics and neo-fascism in post-Soviet Russia," *Political Geography,* November 2001, Volume 20, Issue 8, https://www.sciencedirect.com/science/article/pii/S0962629801000439.

[57] Doug Livermore, "China's 'Three Warfares.'"

[58] Doug Livermore, "China's 'Three Warfares.'"

[59] David Bowdich, "The Importance of Partnership in Responding to the Chinese Economic Espionage Threat to Academia" *Academic Security and Counter Exploitation Annual Seminar,* Texas A&M University, March,4 2020 https://www.fbi.gov/news/speeches/the-importance-of-partnerships-in-responding-to-the-chinese-economic-espionage-threat-to-academia.

[60] Johan Blank, "China Bends Another American Institution to Its Will," *The Atlantic*, October 10, 2019, https://www.theatlantic.com/international/archive/2019/10/nba-victim-china-economic-might/599773/.

[61] Douglas Larson, "China's Emerging Soft Power Strategy in Hollywood," *Naval Postgraduate School,* September 2019, https://www.hsdl.org/?view&did=831031.

[62] Jeffrey Mervis, "'Has it Peaked? I don't know.' NIH officials details foreign influence probed." *Science Magazine*, June 22, 2020, https://www.sciencemag.org/news/2020/06/has-it-peaked-i-don-t-know-nih-official-details-foreign-influence-probe.

[63] Johan Blank, "China Bends Another American Institution to Its Will."

[64] Zack Beauchamp, "One of America's Biggest Game Companies is acting as a Chinese Censor," *Vox*, October 8, 2019, https://www.vox.com/2019/10/8/20904433/blizzard-hong-kong-hearthstone-blitzchung.

[65] Douglas Larson, "China's Emerging Soft Power Strategy in Hollywood."

[66] Elizabeth Chen, "Chinese COVID-19 Misinformation a Year Later," *The Jamestown Foundation,* February 4, 2021, https://jamestown.org/program/chinese-covid-19-misinformation-a-year-later/.

[67] Jon Bateman and Craig Newmark, "Social Media Disinformation Discussions Are Going in Circles. Here's How to Change That", *Slate*, 24 March 2021, https://slate.com/technology/2021/03/online-disinformation-congressional-hearing-amazon-google-twitter-ceos.html.

[68] Yoel Roth and Nick Pickels, "Updating our approach to misleading information," *Twitter,* May 11, 2020, https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html.

[69] Savvas Zannettou, "I Won the Election! An Empirical Analysis of Soft Moderation Interventions on Twitter," *Cornell University ArXivm* January 18, 2021, https://arxiv.org/abs/2101.07183.

[70] Ben Collins and Brandy Zanrozny, "Reddit Bans Qanon Subreddit after months of violent threats," *NBC News,* September 12, 2018, https://www.nbcnews.com/tech/tech-news/reddit-bans-qanon-subreddits-after-months-violent-threats-n909061.

[71] Manoel Horta Ribeiro et all, "Does Platform Migration Compromise Content Moderation," *Cornell University Arxiv,* October 21, 2020, https://arxiv.org/abs/2010.10397.

[72] David V. Gioe, "The History of Fake News", *The National Interest*, 1 July 2017, https://nationalinterest.org/feature/the-history-fake-news-21386.

[73] Arielle Pardes, "Parler Games: Inside the Right's Favorite 'Free Speech' App," *Wired Magazine*, November 12, 2020, https://www.wired.com/story/parler-app-free-speech-influencers/.

[74] Joseph Littell, "Don't Believe Your Eyes or Ears: The Weaponization of Artificial Intelligence, Machine Learning, and Deepfakes," *War on the Rocks,* October 7, 2019, https://warontherocks.com/2019/10/dont-believe-your-eyes-or-ears-the-weaponization-of-artificial-intelligence-machine-learning-and-deepfakes/.

[75] Associated Press, "Cheerleader's mom accused of making 'deepfakes' of rivals," *Associated Press News,* March 15, 2021, https://apnews.com/article/pennsylvania-doylestown-cheerleading-0953a60ab3e3452b87753e81e0e77d7f.

[76] Kevin Roose, "The Making of a YouTube Radical", *The New York Times*, 8 June 2019, https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html.

[77] Hao, "He Got Facebook Hooked on AI. Now He Can't Fix Its Misinformation Addiction."

[78] Ibid.

[79] Barkun, "Conspiracy Theories as Stigmatized Knowledge"; Clarke, "Conspiracy Theories and Conspiracy Theorizing."

[80] Karsten Muller and Carlo Schwarz. (2018). "Fanning the Flames of Hate: Social Media and Hate Crime." *Centre for Competitive Advantage in the Global Economy.*

[81] Dana Weinberg and Jessica Dawson, "From Anti-Vaxxer Moms to Militia Men: Influence Operations, Narrative Weaponization, and the Fracturing of American Identity," *Brookings*, 2021, https://doi.org/10.31235/osf.io/87zmk.

[82] Zeynep Tufekci, "View of Engineering the Public: Big Data, Surveillance and Computational Politics | First Monday," *First Monday* 19, no. 7 (2014), https://firstmonday.org/ojs/index.php/fm/article/view/4901/4097.

[83] Gabriele Cosentino, *Social Media and the Post-Truth World Order: The Global Dynamics of Disinformation* (Cham: Springer International Publishing, 2020), https://doi.org/10.1007/978-3-030-43005-4.

[84] Renee Diresta and Tobias Rose-Stockwell, "How to Stop Misinformation Before It Gets Shared," *Wired*, March 26, 2021, https://www.wired.com/story/how-to-stop-misinformation-before-it-gets-shared/.

[85] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–51, https://doi.org/10.1126/science.aap9559.

[86] DiResta, "Computational Propaganda: If You Make It Trend, You Make It True."

[87] Saara Salomaa and Lauri Palsa, "Media Literacy in Finland: National Media Education Policy," *Publications of the Minsitry of Education and Culture,* 2019, https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf.

[88] Intelligence Unit, "Democracy Index 2018: Me too? Political Participation, Protest and Democracy" *The Economist,* 2018, https://www.eiu.com/public/topical_report.aspx?campaignid=democracy2018.

[89] Nic Newman et al, "Reuters Institute Digital News Report 2018," *Reuters Institute for the Study of Journalism. 2018*, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/digital-news-report-2018.pdf.

[90] Samar Ali, "Millions of Conversations," https://millionsofconversations.com/team.html.

[91] Cybersecurity and Infrastructure Security Agency, "#Protect 2020: Rumor Vs. Reality," https://www.cisa.gov/rumorcontrol.

[92] Christopher Krebs "Opinion: Trump fired me for saying this, but I will say it again: The election wasn't rigged," *The Washington Post,* December 1, 2020, https://www.washingtonpost.com/opinions/christopher-krebs-trump-election-wasnt-hacked/2020/12/01/88da94a0-340f-11eb-8d38-6aea1adb3839_story.html.

[93] David Gioe, "The History of Fake News," *The National Interest,* July 1, 2017, https://nationalinterest.org/feature/the-history-fake-news-21386.

[94] Benkler, Faris, and Roberts, *Network Propaganda*.

[95] Sam Wineburg and Sarah McGrew, "Lateral Reading: Reading Less and Learning More When Evaluating Digital Information," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, October 6, 2017).

[96] We acknowledge the difficulty in securing universal agreement on what constitutes "legitimate" news sites.

[97] Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," *Oxford Handbook of Cyber Security*, August 11, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680.

Interview with the Honorable Michèle Flournoy

Co-Founder and Managing Partner of Westexec Advisors, and former Under Secretary of Defense for Policy

President Biden has pledged to withdraw U.S. troops from Afghanistan by September 11th. Are the circumstances right to be leaving Afghanistan now?

I understand that President Biden made an assessment that the Afghanistan situation cannot be resolved to anybody's satisfaction by military means alone at this point. I do understand his impetus for withdrawal. He has been wanting to reduce our commitment to Afghanistan for a very long time, dating back to when he was Vice President. I do wish that he had approached it in a somewhat different way. What do I mean by that? The small U.S. force presence that was left there by President Trump—who also wanted to withdraw all of our troops—has been in the position of the boy with his finger in the dyke.

As we removed U.S. forces, it unleashed a whole set of events. I wish we had taken more time to try to set and bound the conditions around the President's decision. For example, I would have liked to have seen one last push diplomatically with the United States in the lead, bringing our international partners together to really push the Taliban to fully meet the commitments made in the agreement that was signed with the Trump administration—a full break with al-Qaeda, the implementation of a national ceasefire, and their commitment to Afghan-to-Afghan negotiations for a political settlement, among others.

I would have liked to have seen that final diplomatic push to see if we could use the leverage of future assistance, future recognition, the willingness of the international community to stay engaged in Afghanistan to try to get some kind of political framework in place. I am not saying that would have been easy, but I would have liked to have seen us try harder than appears to have been the case.

This interview was conducted by Michael Miklaucic on July 14, 2021, and has been updated based on recent developments.

Second, I would like to have seen more time given to managing the risks associated with withdrawal in terms of an accelerated plan upfront for taking care of the Afghans who assisted us and their families, as opposed to a belated and chaotic scramble to do that. Also, a plan for how exactly we are going to prosecute continued counterterrorism operations against al-Qaeda if it reconstitutes, or against ISIS-K which has stated its aspiration to attack not just in the region but U.S. interests more broadly. How are we actually going to execute that? What does that look like and how do we set the theater for that?

And then finally, I would like to have seen extensive planning to help the Afghan government and particularly the Afghan security forces, to keep them from collapsing under the pressure of the Taliban offensive. What kind of assistance might we have provided to keep them viable? These are all questions that will be debated in after-action reviews. I would like to have seen more time and effort put into setting the conditions for withdrawal to try to mitigate the risk of a rapid Taliban takeover of the country.

Do you think our departure from Afghanistan will benefit our adversaries Russia and China and if so, how can we prevent or mitigate the consequences of their attempts to capitalize on our departure from Afghanistan?

While we've met certain narrow objectives in Afghanistan related to counterterrorism, the broader ambitions that several administrations have had for Afghanistan clearly have not been met. Our adversaries will use that to question our leadership, our credibility, our staying power, and our ability to get things done. We should expect that kind of propaganda, that kind of messaging from them.

I don't think there are huge gains for Russia or China. Russia can't be thrilled about the Taliban's return to power in Afghanistan; they are concerned about ripple effects in their near abroad. But I do think they'll use this to bludgeon us from a reputational perspective, and that's just an opportunistic approach that we should expect.

In terms of more concrete benefits, when things settle down China stands to gain the most economically. China has wanted to make serious investments in Afghanistan's mining and mineral sectors. Without the United States there to reinforce the rule of law they stand a good chance to get in there with contracts that will exploit Afghanistan. Obviously, their alliance with Pakistan will be affected by this as well.

Moving away from Afghanistan towards the larger geo-strategic situation, in what ways does China threaten the national security of the United States? How would you characterize the threat?

China is emerging as our principal competitor. In economic terms they may soon overtake the United States economy in size. Technologically they are seeking dominance or advantage in key areas such as semiconductors, 5G, synthetic biology; you can go through a long list. These are the technologies that will define the future both economically and from a national security perspective. China has been at that for at least a decade, really going after the advantage in those areas, though with mixed results.

Militarily, China has become the pacing threat; not only in terms of their technological investments and Anti Access/Area Denial systems designed to counter our power projection, but also in areas like cyber and space, and even in some aspects of the maritime domain.

Ideologically the big narrative in Beijing is: "Look at the United States! It's a mess. It's in decline. Our system is superior to democracy. We are performing better vis-a-vis COVID-19, etc." They are now competing ideologically from a systems perspective.

There are key areas where it is very much in our interests to compete with China but also, areas to cooperate with China. For example, climate; there is no solution without getting China on board.

Non-proliferation, same thing. We must work together toward preventing the next pandemic.

The name of the game is managing the competition, which is multi-dimensional, and trying to keep it from erupting in an open conflict between two nuclear-armed powers. So, very challenging, but if you asked me—would you rather have the U.S. hand to play or the China hand to play, there is no question; I would rather have the U.S. hand. We just need to be playing it better and with greater urgency than we have been so far.

We and our allies wish to preserve what we call the liberal, rules-based system. How would a China-dominated world order differ from that? What would it look like?

We have seen from China's actions that, first of all, their autocratic system has been harnessing emerging digital technologies to create a true surveillance state. We have seen them start to export that model to other states around the world. It is not just that the Chinese people are being denied certain human rights and freedoms; it's that the Chinese are actually trying to export that model to other countries that they invest in or work with.

Something else we should expect to see—that we are already in fact seeing—is a might-makes-right approach. The Chinese have demonstrated that they are willing to throw their weight around, certainly in the region but also more broadly. They believe that a big power like China should be able to intimidate, coerce, and dictate to smaller powers in the region—for example, some of the smaller members of ASEAN. They are not going to treat those countries as equals and take disputes to international arbitration or negotiation. They are going to say, "We are the big power. We are the empire. Our will should stand as defining the status quo or the new status quo." That is what worries me; selective respect for international law, a tendency to use coercive and even aggressive measures to impose their will on weaker states, and an embrace of technology for the purposes of state control and surveillance. That is a very different world than the one we have been living in that has given us tremendous security and prosperity since World War II, and it is certainly not one that I would want to live in.

Can you imagine or describe a scenario in which military conflict with China would be justified?

I have two big concerns; one is the risk of miscalculation and accident. In the Cold War period we and the Soviet Union negotiated rules of the road, with the Incidents at Sea Agreement, the hotline, and various approaches to de-escalation should there be some interaction of our forces at the tactical level, to keep it from spinning out of control. Some of that, of course, was put in place years after the Cuban Missile Crisis, which was probably the best example of things spinning out of control. But we do not have that with China today. They really have not engaged with us seriously on that kind of de-escalation or confidence building measures. That's one concern.

But the other scenario is that China believes its own rhetoric. They think the United States is in decline and not coming back. They believe that they are on the rise and this is their moment, and they might decide to enforce their will using military means, whether it is an offensive against Taiwan or some disputed territory in the South China Sea. If they underestimate U.S. resolve and capability to respond, suddenly, we could be in a situation where our militaries are confronting one another. The only way that might happen is if China miscalculates.

That is the reason I have argued that the name of the game right now militarily is to shore up and reinvigorate deterrence and demonstrate to China that we do have resolve; and clarify for them what we are willing to defend. Then we must demonstrate the capabilities and concepts we possess to either deny or roll back the success of any aggression and/or to

be able to impose such costs that they understand it is really not in their interest to pursue the aggression in the first place. That is the name of the game in this next period.

Many Americans are hostile to the idea of sending U.S. forces to fight in faraway places. How would you convince them that Taiwan is a partner worth protecting militarily, or do you believe that it is?

If China were to attack Taiwan unprovoked—in the absence of any unilateral independence declaration or any other action by Taiwan—we would be defending a democracy in the region. The way to explain it is to say that if the United States and the international community were to ignore such aggression, we are giving China a green light to steamroll across the region as it sees fit. Not necessarily in strictly military occupation terms but in terms of being a bully, using coercive measures and using its military, its law enforcement capabilities, and its economic clout to routinely violate the sovereignty of smaller countries. You would be opening the door to the future we talked about earlier which is a very different future than we hope for, with Chinese rules rather than the existing international rules that have served us so well.

Is our policy of strategic ambiguity with respect to Taiwan the right policy now or should we be more explicit in saying that we are prepared to defend Taiwan militarily if need be?

The combination of the One-China Policy and the Taiwan Relations Act has always maintained that ambiguity. There is a certain inherent tension, but U.S. policy has generally gotten that right. At this time though, when China is doubting our resolve, they are unclear about how we see our interests and are becoming overconfident in their own military capabilities, it is very important to clarify the message that if Taiwan were attacked unprovoked, China should expect a U.S. and more importantly an international response.

Moving to the economic domain, in 2013 China initiated the Belt and Road Initiative which is extremely ambitious and seems to be proceeding, though with some hiccups. How do we compete with something like that that is supported by almost a trillion dollars equivalent of investment?

We cannot compete with it dollar for dollar. We have to think asymmetrically and strategically. What I mean by that is, first of all, along the Belt and Road Initiative path there are some places that really matter to us and affect our interests, and others that are not high up on our priority list. We need to focus; we need to make strategic judgments as to where we want to compete. And then, we need to think about what tools we have that play to our advantage.

I would suggest they are things like internet access, ubiquitous wi-fi, broadband, fiber optic cable. Helping to create more free and open economies and societies by connecting them to the world wide web. Rule of law assistance to counter some of the more mercantilistic and often predatory practices China brings with it into these countries. We can offer entrepreneurial coaching, investment, assistance to grow innovation hubs. There is some exciting work being done in Africa in this regard. We have to think strategically—where do we want to compete?—and then asymmetrically in terms of what do we have that other countries really want and need. It may not be the same dollar amount that China offers, but we will get higher impact with targeted areas of investment and assistance.

Speaking of asymmetries, because they are autocratic countries that can command all of the elements of national strength for strategic purposes, China and Russia have certain advantages in terms of mobilizing all of these elements for strategic ends. What can we do to mitigate those advantages?

Where we have real advantage is with our allies; we should not be doing any of this alone. There are so many areas where, whether it's dealing with China

or dealing with Russia, our interests and our values are very similar to those of our allies in Europe and with democracies across Asia. We should be looking to build out coalitions of the willing focused in these different areas so that we can pool our resources and focus them; we are more effective together than if we each try to go it alone.

There is a purported gap between Washington and Silicon Valley with major American companies seeing their commercial interests served by a good relationship with China in ways that sometimes might compromise U.S. national interests. What is the best way for them to balance the competing interests of their shareholders who want maximum profits and access to the Chinese super-large market and our national security interests that may not be identical to the shareholder interests?

The U.S. companies that I work with are U.S.-based but global in footprint and in their business. What they are trying to navigate is, how do I do my part as a responsible U.S. entity to ensure that I am protecting U.S. national interests, but at the same time, continue to compete effectively in the Chinese commercial market where I have to be careful about controls on IP, what I share, what activities I undertake, etc. These companies know they must be mindful of export controls and all of the compliance requirements, and must ensure that their activities in China don't advance Chinese national security; but it is the China market that will give them the revenue that allows them to create and keep American jobs, contribute to the GDP and economic growth, and in many cases, fund the innovation necessary to support their national security customers in the United States.

American companies are walking through this minefield every day trying to figure out how to navigate it. The first thing is to be thoughtful about a risk management framework, so that the right hand knows what the left hand is doing and that they are mindful of the national security concerns that are genuine and real. But they should also help educate their partners across the U.S. government about what kind of work in China does not involve national security risk, is lawful, and is actually generating revenue that plows back into the U.S. economy and into U.S. innovation. This gets it into very detailed questions.

The same is true in terms of accepting Chinese investment in the United States, and this is what the Committee on Foreign Investment in the United States (CFIUS) process gets at. If it is purely passive investment in Silicon Valley— meaning there is no access to non-public intellectual property, and there are no decision rights, no observer status or seat on the board, no ability to influence the decision-making of the company—if it is truly just passive investment looking for a return on investment, that is blood in the bloodstream of our innovation engine. It hurts us to choke that off entirely, and this is how the CFIUS has evolved. CFIUS distinguishes between passive versus active investment and ensures that we are cognizant of that distinction. Because if we get it wrong we have a situation where sensitive IP gets handed to the Peoples Liberation Army and then we have hurt ourselves.

What can the United States government do or should the United States do to encourage better cooperation and collaboration between the national security community and the private sector?

Most of the companies that I talk to are very eager for that and they are trying to figure out how to plug in. More dialogue between senior government officials and their counterparts in the private sector is important, and more mutual education. The companies need to understand what the U.S. government is trying to protect and what they see as a national security danger. For their part, government officials need to understand exactly what these companies are and are not doing in China, how revenue from the Chinese

commercial market actually contributes to the U.S. economy in various ways, and when companies have been responsible by choosing to abstain from certain activities or business opportunities in China.

A lot of mutual education is needed and a lot more transparency in communications. The best companies are already doing this. They are having conversations with their U.S. stakeholders before they make big decisions on China business, in order to make sure that they are getting the balance right and staying within the right lines of activity. A lot more of this is needed if we are going to stay competitive in key sectors while ensuring we don't inadvertently give away precious IP that needs to be protected.

How can we protect our national interests against China without pushing China closer to Russia and vice versa? How can we protect our national interests vis a vis Russia without pushing Russia closer to China?

In the case of China, we have to find ways to engage on those issues that require cooperation. As I mentioned, climate policy, pandemic prevention, non-proliferation, and even in some economic areas where there is not a national security implication. Russia is a harder nut to crack because under Putin I actually do believe Russia is a dedicated adversary. There are a few areas where we can cooperate—such as arms control—but Putin is not really interested in cooperation. That said, there are instances where China and Russia, from a tactical or opportunistic perspective, will see opportunities to cooperate to try to push back against us or counterbalance us.

The big announcements coming out of China-Russia summits are almost always much more lofty than the actual joint activities they are undertaking. There are natural limits to China and Russia cooperation. One limitation is that China does not view Russia as an equal. They see Russia as a declining power and not one they have to pay a lot of attention to. Russia is not a principal market for them. China is interested in Russia's strategic resources and energy resources and minerals, but they are not a top priority.

In Moscow there is a tremendous amount of fear of China. Russia has a depopulated border with China and they are terrified of the prospect of Chinese aggression for which they have no response or capacity to counterbalance. Russia is very careful with China. They are trying to keep it friendly but there is a lot of fear and distrust there. I don't think they are natural allies. We could certainly play our cards poorly and push them together in opportunistic ways, but I do not think it's a natural or strong alliance.

Russia takes every effort to drive wedges between the United States and our European allies. Does it serve our interest to try to, in a Kissinger/Nixon way, drive a wedge between China and Russia?

We should certainly consider that as the opportunities arise but not the way it was done by the Trump administration which was so worried about them coming together that they picked one as the enemy—China—and picked the other—Russia—as a friend. Unfortunately, the Trump administration chose to try to befriend Putin and Russia, which is entirely contrary to our interests. The way they approached China pushed China from competitor to adversary, to outright enemy, then not being interested in exploring cooperation with China.

We need to focus on managing each relationship in its own right, looking for opportunities to prevent things that bring them together, while collaborating with each on issues that we care about. It would be a mistake to pursue a policy where in order to balance China, we cozy up to Putin's Russia; that is not in our interest.

Putin appears to want to establish a sphere of influence in the former Soviet space. Why should or shouldn't we oppose that?

By any objective measure, Russia is in decline economically, demographically, and politically. Putin

is trying to recreate a sphere of influence that will help him keep himself in power. Putin needs to have an external enemy to try to rally and create internal unity. We have seen the protests on the streets of Moscow. We have seen him so threatened by opposition figures like Navalny that he tried to have them assassinated. Failing that he has jailed Navalny and others and persecuted them. What Putin is most threatened by is democracy, actual democracy, true democracy coming to Russia.

He is looking not only to counter democracy at home but to discredit it in the United States and Europe as well, and that is what Russia's social media disinformation campaigns are about. That is what Putin's propaganda is about, and it is what his other covert means are about; creating the perception that we are in chaos, that democracy doesn't work, that it is a failing model, and therefore, you should appreciate the strong hand of an authoritarian leader. It is also about creating an insulating layer of non-democratic states that are in Russia's sphere of influence, that are dependent upon Russia for various things to create a buffer between Russia and the NATO democracies.

Only a few years ago, Russia invaded and occupied Crimea. Is that something that we should allow to stand or do you see any future other than a frozen conflict there?

It was appropriate to impose sanctions with regard to both Crimea and Ukraine. Neither the United States nor NATO define Crimea as a vital interest, so I do not see either of them intervening militarily. Crimea is an example of Putin creating a *fait accompli*. Ukraine is different. Putin faces continued sanctions, international pressure, and continued Western assistance to Ukraine in the support of its defense. He keeps trying to change the parameters of the Minsk Agreements, but the solidarity between the United States and Europe on this issue has been remarkable and will continue. I do not see a resolution anytime soon but I also don't see Putin being able to take further, significant action in Ukraine without very strong international opposition.

Both China and Russia employ tactics of conflict below the threshold of war to achieve strategic effect, and embrace a full spectrum approach to conflict. How do we counter these measures below the threshold of war?

We have to get a lot better in terms of countering Russian and to a lesser extent, Chinese manipulation of our social media platforms. We have to get a lot better with regard to cyber security in terms of trying to prevent and stop attacks not only against our militaries and our governments but also against our societies. There is obviously a lot to be done in light of our recent experiences.

The best counter to propaganda is the truth, and we have to do a lot better at getting our message out. I have talked in the past about trying to figure out what is the digital equivalent of a United States Information Agency in the 21st century.

We have got to do better at getting the truth out in real time to counter Russian propaganda, which is ubiquitous in markets like Europe. It will take a lot of interagency effort because our tools are distributed, and the authorities to use these tools are distributed across multiple agencies; most of them are not within the Department of Defense. This is an area where we have to perform better and we have to try to get our NATO allies to do better as well.

Both China and Russia appear to embrace concepts of conflict that are constant and comprehensive, while we in the west tend to embrace a binary concept of war and peace. Is that a vulnerability on our part?

Not necessarily. People are seized with the notion of competition on a spectrum, and what the Chinese and Russians might see as war, we see appropriately as competition. That does not necessarily put

us at a disadvantage particularly because many of the instruments we have to mobilize and engage in competition are not military in nature. The thing I worry about in Russian doctrine is the notion of "escalate to de-escalate" which is very dangerous in the context of two nuclear powers. I worry about the Chinese doctrine of "systems destruction warfare" which explicitly envisions early massive cyber-attacks on our critical infrastructure to try to prevent U.S. forces from projecting from CONUS into the region, as well as early attacks on space-based assets which are very fundamental to the functioning of the global economy. I think they underestimate the impact that would have on U.S. resolve.

I think they intend to create such cost and chaos that we would give up before a war even started. If critical infrastructure around the eastern seaboard or the western military bases were attacked it would take down power grids that are powering hospitals and medical facilities. American civilians will almost certainly be harmed if not die. What is that going to do to a president's resolve? That's going to increase the president's resolve. That's going to be seen as an act of war.

China is completely miscalculating how we would react to early major cyber and space attacks. This is an area where we need some direct dialogue to say "this is what your doctrine says, but what you think will happen is the opposite of what almost certainly will happen. You will end up bringing the United States in faster with more commitment than if you didn't pursue this approach." That is the kind of candid conversation we need in strategic stability talks going forward.

What specifically are potential existential threats from Russia, China or both acting together that the United States must be able to deter?

In a world of nuclear powers that includes some who see us as an adversary we still have to be concerned about nuclear deterrence. A smart investment in modernizing a nuclear arsenal that is essential to deterrence has to be on our agenda, which is why you see that appearing in the budget not only of past administrations but the current administration's as well. We can debate about particular systems and exactly how many of what is required, but the investment in keeping nuclear deterrence safe, secure, reliable, and effective is a foundational piece of our security.

We need to think in similar terms about cyber and space. Russian and Chinese doctrine are different, but they have this in common; they will both attack us in those domains in order to create *faits accomplis* thus avoiding traditional military conflict. We have a lot of work to do to better defend ourselves in the space and cyber domains and to make our assets there more resilient. And we should create both defensive and offensive capabilities to try to deter or constrain some of their actions or the effectiveness of their actions in these areas.

We really have to think through deterrence from multiple angles. Secretary Austin has coined the phrase "integrated deterrence." He talks about it across multiple domains thinking not only as the United States, but with our allies, not only in military terms but also using other tools of power. We need an intellectual effort to rethink deterrence in this context similar to the intellectual efforts of Tom Schelling, Herman Kahn, and others in the early days of the Cold War when we were conceptually trying to get our heads around what is necessary to deter the Soviet Union. These questions need to be asked in a totally new context particularly with regard to China.

What role might U.S. nuclear-armed allies play in balancing against China and Russia in this two against one deterrence approach?

The NATO alliance remains important particularly from a political solidarity perspective and sending a message to Russia that it is not just the United States alone, but all NATO allies that are a part of

this endeavor of nuclear deterrence. We have an interest in making sure that there is appropriate burden-sharing there. This will be a big question as some of the older dual-capable aircraft systems, for example, age out and need to be modernized. Will countries like Germany and others actually go forward with nuclear-capable systems given the additional cost? Unless and until we can negotiate an arms control regime for non-strategic nuclear forces in and around Europe, we need to make sure that NATO's part of the deterrent remains strong as well.

There are increasing indications that a Biden-Xi summit might be in the cards. How would you advise the president to approach such a summit? Does a personal touch matter in the Biden approach and would such a summit become a headline grabbing event with little to show for it?

There has been a lot of behind the scenes work to set the conditions for such a summit meeting. We should not expect huge momentous breakthroughs. A leader-to-leader meeting of that kind sets the tone for how we will work together, how we will approach areas where we have differences, and how we will approach areas where we need to cooperate. How will we create frameworks for working on some of the differences we're going to try to at least manage if not resolve.

Presidents Biden and Xi will be taking each other's measure but it's more about what kind of working relationship we will have with China even as we continue to compete and invest in the drivers of our own competitiveness and our allies and partnerships that give us such strategic advantage. I don't expect it to be a big breakthrough with many important deliverables or surprises, but I do expect it to unclog the system and allow things to start moving forward.

Will China and Russia attempt to keep conflicts and competition in the gray zone? What is their escalation calculus if conflict crosses into the conventional domain?

I don't think either power seeks to have a direct conventional military confrontation with the United States because I don't think they have parity at scale, not just quantitatively but qualitatively. They will try to manage the competition to keep it below that level using the various hybrid warfare means we have talked about. That said, because we do not have great communication or negotiated rules of the road, and because we lack de-escalation mechanisms in place, we must be prepared for a failure of deterrence and have the ability to quickly re-establish it on terms favorable to us.

That is why I think we need to spend a lot more time thinking through Moscow's and China's respective hierarchies of interests and, also, the different scenarios where we might find ourselves in conflict. How would we protect our interests while also de-escalating before things get to the nuclear level?

Isn't it fair to characterize China's behavior as merely the mirror image of America's effort to achieve global dominance through military, technological, and financial means?

China is competing in a very different way; it is not parallel because of the state's deep involvement in their economy. China is motivated both by the fact that there are areas of technology where they have encountered limits or bans or difficulty getting western technology, which drives them to double down on developing that technology indigenously. But China also seeks to dominate in some areas because they believe these technologies will define the future economically and they want to export their products, whether it's Huawei and 5G or what have you.

They want to export those technologies to fuel their domestic imperative which is bringing millions and millions of Chinese people out of poverty and getting them to buy into the Communist Party and its one-party rule. Ultimately, everything the Chinese leadership

does is about keeping the Party in power. A lot of their international economic activity is designed to create the revenue needed to maintain domestic stability. They have a lot of motivations to compete in these areas, but they don't want fair and open competition on a level playing field. We do. That is where we excel, but that is not what China is interested in.

What recommendations do you have to address the recent spate of hacking and ransomware most notably involving Russia but not exclusive to Russia?

We have to up our game in cyber security and that will require new types of public-private partnerships. I think the best examples have been in the U.S. financial sector. They were targeted early and often. A real collaboration emerged between the U.S. government and the financial sector working as an industry to try to really enhance their protection, and they've had very good results particularly in providing threat intelligence, sharing best practices, etc. Another example that is still a work in progress is the Defense Industrial Base where there is a lot of public-private collaboration happening.

We need to move that kind of model into a number of areas of critical infrastructure, most of which in the United States is owned by and operated in the private sector, as we witnessed with the Colonial Pipeline, with our electrical grid and so forth. There is some technological innovation coming in this area. We have been in a constant offense-defense battle trying to catch intrusions when they occur and shut them down as quickly as possible. There is a lot of discussion about a different approach, and some companies are actually executing a different approach called "runtime security." I would encourage you to look into this. Basically, runtime security goes below the level of apps to the actual monitoring of runtime.

The way it works is by monitoring for any departure from the normal runtime pattern; even a nanosecond deviation indicates something is wrong and you can shut it down in the next nanosecond. There have been hackathon experiments where the best hackers in the United States spent a week launching thousands upon thousands of attacks on a system with this kind of security and they have zero intrusions. That is the wave of the future. It is a fundamentally different approach to cyber technology. If widely adopted, this will dramatically improve cyber security for both the U.S. government and for American companies.

Does it make sense for the United States to have a more robust counter response to these types of attacks and conduct a more aggressive overall response in order to show resolve against such attacks?

We should be able to impose a cost for these attacks. The response does not have to be symmetric, i.e., a cyber response to a cyber-attack. We need to look at all of the instruments that we have and how we can combine them most effectively to impose cost. Again, this is an area where we have some work to do conceptually and in terms of developing a strategy. After the 2016 Russian cyber meddling in our election cycle there was a lot of concern about similar meddling but using novel techniques in the 2018 elections. The White House authorized CYBERCOM to conduct a series of offensive cyber operations against the Russian perpetrators of the 2016 attacks to impose a denial-of-service attack on them; as a result, they were so preoccupied trying to get their own systems back online that they were unable to launch any attacks on us during that period. That is an example of forward defense in cyberspace. When someone—an adversary—has proven their willingness to attack us using cyber means in ways that are strategic and very harmful, we need responses that complicate or even prevent those attacks.

What can we do to improve education on strategic deterrence?

Part of it is going to school on how the Chinese think about this the way we went to school on how the Soviet Union thought about deterrence. We tend too often to project our calculus onto them as opposed to really understanding how they think about things and how they might see things differently. We should be developing a cadre of national security professionals who really understand China, who deeply understand how the Chinese think about these issues.

The second piece is the new big bets and technology investments that the Department of Defense will make. How do we hasten the adoption cycle for innovative capabilities and integrate them into the force more quickly and at scale? Perhaps a key part of this—maybe the key part of this—is concept development.

We are so accustomed to being the dominant force on the field that others adopt asymmetric means against us. Yet we continue to think conventionally. We are now going to be in a situation if we are dealing with crisis in the Indo-Pacific, where we are outnumbered because of China's geographic proximity and its multi-decade investment in anti-access and area denial (A2/AD) capabilities. There are going to be times when we are really challenged, our networks are going to be constantly disrupted and taken down.

We have to do some serious conceptual work about how are we going to operate effectively and achieve our objectives in that very different environment where we won't have domain superiority. We want to have it early and even when we get it, sometimes it won't necessarily be persistent. That is a fundamentally different problem set that requires new concepts, and the best way to get that is not some huge bureaucratic exercise. It is by competing ideas and solutions. The more the war colleges and institutes can set up opportunities, war games, simulations, and concept development exercises to allow people to compete creative new approaches, the greater our chances of success. That is a long-term investment.

There is much speculation surrounding the PLA's strategic support force and its ability to potentially field emerging technologies including artificial intelligence (AI). Should we be anticipating a strategic or operational surprise in this space and if so, how should we best prepare?

We should devote more resources to understanding exactly what the Chinese are doing in AI. I would commend to you the National Security Commission report on AI. It is one of the most consequential commissions we have had since the 9/11 Commission. Hopefully Congress and future administrations will fully implement their recommendations.

If you look at different dimensions of AI, there are several areas in which the Chinese have already gained parity and they're working very hard to catch up in the other areas. We can no longer assume that China is not going to catch up or even surpass us in some areas. The concern I have about China's progress in AI is that I don't believe that they have the same ethical constraints regarding AI as we have. Because we are a democracy the first thing the Department of Defense does is publish a set of ethical principles on how we will govern the use of and integration of AI in our defense. The Chinese do not have such concerns. The risk that they will use AI in ways we deem irresponsible or unacceptable is very real—and if we encounter such uses on the battlefield we might be caught by surprise because we would never think to do those things.

The most important near-term application of AI is enabling a more resilient network of networks; what we are now calling Joint All-Domain Command and Control. Number two is enabling human decision support so that we can sort through the vast amounts of information and intelligence faster and more accurately to make better, faster decisions than our competition. And three, enabling

human-machine teaming so that a single human platform can control many unmanned systems, providing clear command and control with a huge force multiplier and thus being able to send unmanned systems to do really tough missions in contested or lethal environments. Those are three areas of AI where we absolutely have to accelerate our progress and aim to be dominant, just as a start.

Is China's current muscle flexing in Hong Kong just testing the water for Western response? It would seem based on the news media that the Western response to China and Hong Kong has been more bark than bite.

China is always testing the waters and Hong Kong is no exception. There have been strong political and diplomatic sanctions in response to Hong Kong but not more than that. The danger is that China concludes that because it got away with it in Hong Kong it can do the same in Taiwan. I actually think the international response on Taiwan would be different. Again, Chinese leaders are in danger of setting themselves up to miscalculate how the international community will respond.

What should the United States do regarding Chinese activities in the South China Sea?

We should continue to press the issue diplomatically and legally, in the context of international law, and with our military means through freedom of navigation exercises, by refusing to recognize their land grabs as legitimate, and by supporting our allies and partners in the region. We should try to create international diplomatic pushback on China whenever they overstep and violate international law in trying to create a new status quo. We have had some success in doing this in the past that has forced China to recalculate and step back, but if we are not consistent about it, they will keep pushing and pushing, and eventually, change the status quo—which is what they have succeeded in doing so far.

As you just highlighted an outright military confrontation may be an outcome of a miscalculation on the part of China; what, in your view, might be a U.S. miscalculation that could lead to a military confrontation with China?

We are so accustomed to thinking about it as Chinese miscalculation that we rarely give any thought to how the United States might miscalculate, but this is a very good question. The Chinese, particularly in this period, have a lot of bluster about them with their "wolf warrior diplomacy" and some very aggressive rhetoric. There is a risk that we might think it's just rhetoric or bluster when they actually intend to do something. The risk is if we assume China will not take an action and we fail to take preventive measures, we might be forced into a hasty military response, and find ourselves on the escalation ladder that we might have prevented had we been more discerning about what is bluster and what is real. We should give that a lot more thought as we develop concepts for the future.

In 2005, Russia's defense minister stated that Russia is fighting an undeclared war with the West. Sun Tzu says that the state that doesn't recognize that war is being waged against it is at risk of losing the war. How does the United States confront undeclared war against peer adversaries that believe they are already fighting us in the competition space?

Our eyes have opened up on Russia, particularly after the 2016 elections. We may not call it a war but we certainly see the nature of their actions. There should be a concerted effort to counteract that sort of gray zone conflict, if you will. On the Chinese side, people are framing it differently. They are framing it in terms of a multi-dimensional competition with strategic implications. We recognize that we are in a serious competition that risks becoming open conflict in some areas if we're not careful.

The best way to prevent that is to actually do well in the competition by, for example, investing in the drivers of our own economic and technological competitiveness here at home. That includes everything from science and technology funding, research and development funding, proper incentives and investments from the public sector to draw the private sector into the big bet technology areas where we absolutely need to win. We need a smart immigration policy to attract the best and brightest to the United States and encourage them to develop their new ideas and their businesses here as we have been so successful doing in the past. We need 21st century infrastructure.

All of this is part of being able to compete effectively as the United States and then finding areas where we have allies and partners that have particular assets to bring to the table in key technology areas, and combining forces and resources with them more effectively. With China, we need a process of mobilizing at a national level and hopefully, at an international level, to compete effectively and to be able to underwrite deterrence so that we do not go into open conflict.

Legislation needs to move on The Hill and the administration needs to do more. But even in a time when we are very polarized, this is actually one area of remarkable bipartisan consensus.

Is there any final thought you would like to leave with us?

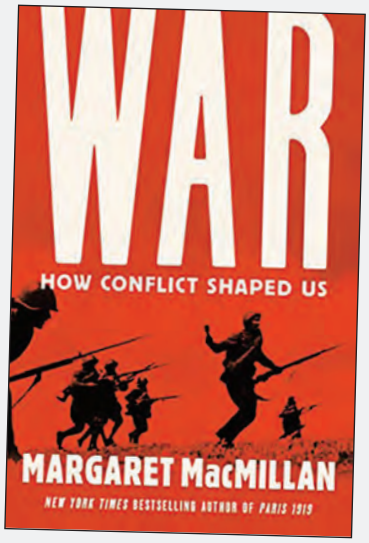
Just a call to action, if you will, to take on this conceptual work, whether it is toward a better understanding of how the Chinese think and how best to deter them, or at the more operational level; we need new concepts. Think in two timeframes. One in the near term, based on what we already have in hand; how do we combine capabilities in new ways and use them in new ways to get better results? And then in the longer term, as investments and new capabilities come online, how do we leverage those in ways that really take full advantage of what they bring to bear and that will require new concepts of operations.

This effort will take many years and require many minds. It needs to be open and competitive. It cannot be done as a deductive bureaucratic exercise like writing a consensus document or policy. We must submit these new concepts and solutions to competition, testing, and experimentation with new approaches if we are to harness our own strength which is real creativity, innovation, and human capital. That is our real source of advantage. PRISM

War: How Conflict Shaped Us

By Margaret MacMillan
Random House, 2020
312 pp $18.19
ISBN: 978-1984856135

Reviewed by Bryon Greenwald



The evolution of human society and its capacity to make war are so intertwined, so symbiotic, as to be inseparable. To study one without the other is an exercise in incomplete scholarship. For, as Margaret MacMillan exclaims early in her insightful study of war and its influence on Western society, "we have to include war in our study of human history if we are to make any sense of it."

War: How Conflict Shaped Us, is an elegantly written examination of the subject, initially delivered by MacMillan as part of BBC Four's Reith Lecture series in 2018. In it, MacMillan delivers on her promise to analyze the evolution of war and society and how one influenced the other. She does so across nine chapters that combine the best of Quincy Wright's *A Study of War*, Clausewitz's *On War,* and Sun Tzu's (or as she notes *Sunzi*) *The Art of War*, along with a healthy dose of war and warfare in the Western World, and incisive chapters on "Making the Warrior," "Fighting," "Civilians," and "Controlling the Uncontrollable." She closes with a crisp chapter on how we remember conflicts, which is a master class in how society has viewed its sacrifices in war over time.

The book is an excellent 270-page summary of war as a phenomenon. Following an opening chapter on the relationship between war and humanity, MacMillan presents the reader with a series of nested expositions on the social, political, technological, and cultural evolution in the conduct of war from the 18th century through the end of the 20th century; how and why men (and some women) and societies fight; the act of fighting or combat as recorded by participants; the expansion of conflict to include attacks on civilians; the largely fruitless efforts to control conflict; and how humans have tried to trivialize, capitalize on, and memorialize war. As such, the book should be mandatory reading for staff and war college students and civilians in security studies programs. Indeed, the bibliography of mostly memoirs and secondary sources represents a reading list worthy of an Oxford professor, which of course, she was.

MacMillan is the author of several best-selling books including *The War that Ended Peace: The Road to 1914* and *Paris, 1919: Six Months that Changed the World.* In *War: How Conflict Shaped Us*, she focuses heavily on Western Europe and those nations' involvement in both world wars. As the great granddaughter of WWI British Prime Minister

Dr. Bryon Greenwald is a Professor of History at the Joint Advanced Warfighting School, Joint Forces Staff College, National Defense University.

David Lloyd George, perhaps that focus is only natural. Still, her historical breadth allows her easy inclusion of examples in the text from Thucydides, Alexander, the Romans, the Thirty Years War, the Age of Napoleon, the American Civil War, and even America's post–1945 wars. Unfortunately, she largely refrains from examining the wars in Iraq or Afghanistan, which witnessed an acceleration of warfare into the digital age and occurred concurrently with the next phase of societal, technological, ethical, and military evolution (possibly revolution). This period offers such rich territory for examination that it seems to be a lost opportunity for someone of MacMillan's caliber. A major exception occurs in chapter 2, "Reasons for War," where she eviscerates the planning for Iraq (2003) as evidence that "those making decisions for war" assumed "that, somehow, victory will magically sort out all the problems," colloquially satirized by security professionals as the "ding-dong the witch is dead" strategy and a direct reference to the Defense Department winning the tactical battle, but losing both the war and the peace to follow, if that condition can realistically be said to exist in Iraq today.

While panoramic in scope, *War: How Conflict Shaped Us* is a book of synthesis and reflection. It is less than half the length of *Paris, 1919* and though peppered with historical examples to illustrate her analysis, it contains none of the detailed treatment of the subject seen in her earlier books. As most historians do, MacMillan looks backward. Only in the conclusion does she attempt to go beyond historical analysis and offer some prognostication on the future, specifically the likely bifurcation of war into two levels: one fought by professional forces with high technology, and another fought by loosely organized forces with low-cost weapons. As history suggests, however, these two levels will not remain separate. Instead, like the modernized British Army that pulverized the much larger, but poorly equipped Mahdi Army at the Battle of Omdurman (September 2, 1898), the forces at MacMillan's two levels will often clash in the same arena with horrific results. Even more ominously, security analysts expect these loosely organized forces to gain ever-increasing access to much of the easily trafficable high technology now used by the militaries of the major and medium-weight powers.

A historian and author of MacMillan's stature is rarely off the mark. She is eminently qualified to lecture and write on virtually any historical topic. Most authors would be happy to achieve a tenth of her acclaim and literary success. That said, readers should remember that *War: How Conflict Shaped Us* is not comprehensive nor foolproof. It relies on secondary sources, some of which are considered classics and others that are "general knowledge" texts (for example, Heuser's *The Evolution of Strategy,* Paret's *Makers of Modern Strategy,* and Parker's *Cambridge History of Warfare*, to name a few). As is common in some publishing circles when producing books in this genre, it lacks the citations to give it the gravitas that elbow patch-wearing academics might desire. This situation creates problems when one runs across sections that seem to disagree with or shortchange the historical record, something that MacMillan's other works rarely do.

For example, the section on Iraq (pp. 46–47) conflates two different historical events and leaves the reader with the impression that they are directly related when they were not. The first event was the planning for the invasion of Iraq in 2003, and the second U.S. Marine Lieutenant General Paul Van Riper's participation in Exercise *Millennium Challenge*, a $250 million joint concept experiment (wargame) run by the U.S. Joint Forces Command in late summer 2002. In the latter event, Van Riper commanded the lesser-equipped opposing Red force, which had seized some disputed islands. But instead of waiting for the Blue force to attack with an overwhelming air and missile bombardment as was done in the Persian Gulf War, Van Riper struck unexpectedly with a

barrage of rockets, missiles, and suicide speedboats as soon as the Blue force was within range. In seizing the initiative, he managed to destroy almost two dozen capital ships and desynchronize the Blue force to the point that the umpires stopped the wargame and "reset" or restored the friendly force to full strength. Van Riper quit in disgust.

Unfortunately, MacMillan's linking of the two events together in her text suggests that Van Riper's decimation of the Blue force (20,000 casualties in 25 minutes—less time than it took to deliver a pizza, according to one account) foreshadowed the asymmetric tactics the U.S. faced in Iraq and Afghanistan and that somehow the military should have known better. In fact, she writes that the experiment's "demonstration of asymmetric war . . . was a warning of what was going to happen to coalition forces in both Afghanistan and Iraq . . . . "

Perhaps she is correct at the conceptual or macro level, *U.S. forces should always know better.* In real life, and at the operational and tactical levels of war, the two events were unrelated; they were two wholly different incidents, separate in time, place, and effect. Millennium Challenge was not a wargame to prepare for the invasion of Iraq; it was mandated by Congress and planned years in advance to test emerging warfighting concepts. In it, Van Riper surprised Blue forces with his unexpected use of regular military forces, conventional tactics (with a nod to WWII history), heavy artillery, and suicide speedboats. In Iraq, religious militias and insurgents backed by Iran fought an unconventional (guerrilla, if you will) campaign, planted improvised explosive devices in roads, and detonated them with garage door openers. While surprise existed in both, there are significant differences between the two events. Finally, in attempting to verify her research, this reviewer searched her chapter and book bibliographies and found only one source on the Iraq war, Tom Ricks' *Fiasco,* which does not mention Millennium Challenge at all.

There are other small examples, such as MacMillan calling British General Bernard Montgomery and General of the Army Douglas MacArthur "great commanders" who had the "ability of great actors to reach out and make their men feel that their commanders knew them, cared about them and were speaking directly to them" that indicate a limited exposure to some of the historical record. Both men had erratic records in World War II and neither were loved by their men. Monty was indeed the "hero of El Alamein" in North Africa in 1942, but a failure when he reached the Continent (for example, Caen, the Falaise Pocket, Antwerp, and Operation *Market Garden*). While Montgomery maintained that his "beret was worth three divisions," his men frequently turned their backs on him as he drove by. If forced to choose a British commander to include in the list, Horatio Nelson (of Trafalgar) or William Slim (of Burma) would have been better choices based on their combat records and ability to motivate their forces.

That MacMillan would succumb to the MacArthur myth, but not include Patton on her list of great actors, is just as puzzling. MacArthur lost the entire Far East Air Force to the Japanese air attack on December 8, 1941, despite the attack occurring 8 hours after the assault on Pearl Harbor. He also ordered the ill-considered movement of supplies and men forward on Luzon to await a Japanese landing only to lose all his supplies as his forces fell back in disarray into Bataan, where they held on for 4 months on starvation rations before surrendering. After not seeing their commander for several months, MacArthur's beleaguered forces on Bataan started calling him "Dugout Doug," a reference to his exodus to the Malinta Tunnel on the fortress island of Corregidor. His record in the Korean War was no better. The Inchon landings were a success, but his pursuit to the Chinese border and casual dismissal of warnings of Chinese intervention sealed his historical fate. As a coda, President Harry

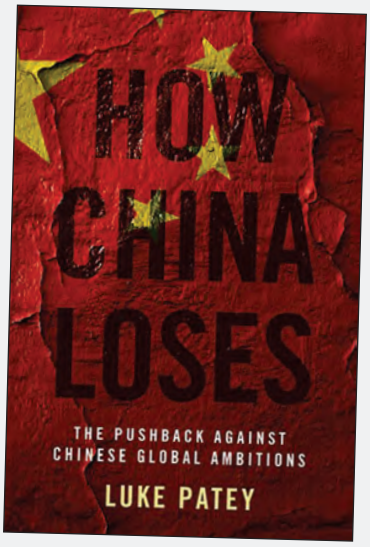
Truman relieved him for insubordination and failure to follow orders the following year.

Despite these minor flaws *War: How Conflict Shaped Us* is a worthwhile read, especially for political leaders, pundits, and that part of the populace for whom military service is a foreign concept and who have no understanding of war's evolution or its impact on those who fight it or lay in its path. As MacMillan accurately notes, "war is perhaps the most organized of all human activities and in turn it has stimulated further organization of society." It is alive with puzzles and paradoxes. We hate it, but employ it, at times with gusto. It wrecks nations, but rebuilds and remakes them as well. It is the final arbiter of arguments between kings and statesmen until the conditions change and the argument is revisited. As MacMillan argues, we must understand ourselves and our interaction with war, conflict, and organized killing if we, as a species, are to arrest our natural tendencies and turn our organizational and technological abilities to solving a host of other maladies that influence the human condition. PRISM

How China Loses: The Pushback Against Chinese Global Ambitions

By Luke Patey
Oxford University Press, 2021
400 pp, $29.95
ISBN: 978-0190061081

Reviewed by Dean Cheng



As the economy of the People's Republic of China (PRC) has grown, its military has modernized, and its global presence has expanded, there has been more and more concern about the prospect of a Chinese century, or even millennium, to replace the American century. Views range from equanimity (Martin Jacques' *When China Rules the World*) to gravely concerned (Michael Pillsbury's *The Hundred-Year Marathon*). Even President Joe Biden is now reportedly concerned with the rise of China—and the possibility that China might prevail in the current great power competition.[1]

The rise of China was almost inevitable, once it recovered from the economic devastation and internal turmoil created by Mao Zedong. Deng Xiaoping's policy of "Reform and Opening," while reestablishing internal political and economic order, also provided an extended period of relative stability (compared with the regular upheavals that marked Mao's reign). Given China's sheer size in various dimensions, including its economy and military, it always has had the potential of being a great power (a status it held for most of its millennia's-long history). Luke Patey's book, *How China Loses*, discusses these issues in detail with his own take.

The challenge posed by the PRC, especially after Deng officially stepped away from power in the early 1990s, lies in how it has leveraged the attributes of a large population, significant natural resources, and a growing economy to attract foreign investment and political partnerships. Beijing has capitalized upon the appeal of its enormous markets and massive educated labor force to integrate into the global supply chains of various products. Meanwhile, over the past decade, the PRC has exploited its huge foreign exchange reserves and relatively low-profile diplomatic position to implement a new form of checkbook diplomacy, exemplified by the Belt and Road Initiative. In a very real sense, China's appeal is multifaceted. Both importers and exporters see their futures tied to China. Both developing countries and developed countries seek to curry favor, or at least avoid alienating Beijing.

Assessing China has been further complicated by the persistent belief that China would reform as its economy expanded. At a minimum, China was expected to adhere to the terms of the World Trade Organization and show greater respect for intellectual property. Ideally, the growth of a Chinese middle class would lead to demands for political reform, whether in terms of greater accountability on

Mr. Dean Cheng is the Heritage Foundation's Senior Research Fellow for Chinese political and security affairs.

the part of the Chinese Communist Party (CCP) or perhaps even a softening of authoritarian tendencies. After all, Chinese officials in the 1990s and 2000s had talked about a "Singapore model" for Chinese development.[2] Leaders like Deng Xiaoping and Xi Jinping both praised Singapore's economic achievements and political evolution. While such optimism has passed, it undeniably delayed reassessments of China's rise as posing more threat than opportunity.

The view of a rising, even dominant, China as inevitable is further reinforced by the apparent lack of pushback. While there are periodic stories about fears of Chinese "debt trap diplomacy," and the U.S. Department of Defense and other government agencies regularly issue reports on the growth and modernization of the Chinese military, there is nowhere near the consensus that characterized the view of the Soviet Union in the 20th century. For example, Vice President Mike Pence's 2018 speech about the threat of China was derided by Peter Beinart in The Atlantic, and attributed to domestic politics by the Brookings Institution.[3] This is seemingly even more true internationally, where China's economic diplomacy is often portrayed as ultimately successful, although at times alienating.

Luke Patey's book, *How China Loses*, looks at many of the same facts, but reaches very different conclusions. Patey highlights many of the same strengths and tactics that others have identified. Because the PRC's economy has grown so substantially, it offers an attractive market for many of the West's conglomerates. That massive explosion in wealth has also provided the CCP with substantial resources to invest both at home and abroad, with financial returns on investment only one of several considerations. Thus, the PRC can develop and implement policies such as "Made in China 2025" and the Belt and Road Initiative.

In certain respects, Patey's book is a continuation and update of both Jacques and Pillsbury. However, with the benefit of an additional 5–10 years of perspective, Patey can also provide details of Chinese missteps and failings. From Argentina to Malaysia to Germany, Chinese investments—and more importantly its broader behavior—have alienated many of the very nations it has courted and invested in. China's asymmetric, unequal approach to economic relations, for example, has not only raised alarms in Europe, but also caused disenchantment in Africa and South America.

Patey also notes that far from exercising a single, integrated operational plan in its efforts abroad, Chinese activities are often as riven by bureaucratic competition and lack of coordination as Western efforts. His description of different Chinese bureaucratic interests and efforts among China's national oil company, foreign ministry, and oil ministry in South Sudan would likely find American, British, and French officials nodding in sympathy.

An interesting insight from the book is that China's willingness to work with local officials behind closed doors, often in ways that sustain local corrupt practices, is alienating not only local populations that would prefer a more transparent system, but also other local interest groups and political parties. In a democratic system, those groups may eventually assume power, and are likely to be much less enamored of working with Beijing.

Patey's discussion of China-Argentina relations, especially the Macri government's investigation of various Chinese investments made under the previous Kirchner administration, demonstrates how the Chinese approach can lose China friends as well as gain them. This is not necessarily grounds for optimism, however. Patey notes that Chinese negotiators included provisions in their contracts with the Kirchner regime that made it almost impossible for the Macri government to completely kill some of the higher profile projects. The twisted story demonstrates how Chinese mastery of legal warfare extends to the political and economic realm and is exercised in contracts and in investments.

With these elements in mind, Patey concludes that, "This is how China loses… because the actions and visions of its leaders elicit cautious reception and push back across the world that undermines its potential as a global superpower."[4] This aspirational conclusion, however, that China somehow alienates, or induces caution, in enough of the rest of the world so that it does not achieve its full potential as a global superpower is emblematic of the shortcomings of the book.

At no point does Patey indicate that China will lose, despite the title of his book. Indeed, he does not demonstrate why China will **not** win. Part of the problem is that Patey is never quite clear how China itself defines *winning*. At one point, Patey suggests that China poses as much an ideological threat as it does an economic or diplomatic one. "China seeks to challenge the core values of the world's liberal democracies: individual liberty, freedom of speech, and rule of law."[5] This would suggest that China defines winning by altering the rules of the international order.

But having stated that China is trying to overturn the rules-based international order (or at least substitute a new set of rules), Patey later suggests that China simply wants "foreign countries to see China's economic and political practices as legitimate and worthy of emulation."[6] This is far less challenging to the West, and given China's history, including the "century of humiliation," appears far less threatening. After all, a China that simply seeks to have its system deemed legitimate need not overthrow the international system in the process.

Patey then characterizes the problem as one of China's approach. China is not proselytizing its system, but,

> is normalizing its state-led, authoritarian economic and political practices and values . . . [China's] activities thus socialize characteristics of China's model into foreign countries by re-enforcing state control over the economy, offering plenty of room for political and corporate elite corruption, limiting public participation, and neglecting social and environmental issues.[7]

Apparently, the Chinese threat is that it plays to the baser instincts of other states and leaders. This undermines the international system, but not necessarily through direct Chinese actions. If this is the case, then China's definition of winning may be far harder to define, and therefore defeat. It is not clear "how China loses." In this light, Patey's treatment of the China challenge, while a welcome counterweight to the various books and articles suggesting that China will inevitably win, remains unsatisfying.

If *How China Loses* doesn't really provide a solid answer to China's definition of winning, its response is equally nebulous. For all the problems that he outlines of China's foreign policy, Patey recognizes that other states are unlikely to defeat China in a bilateral fashion. Yet while he excoriates President Donald Trump for failing to pursue a more multinational effort to confront China, he provides little evidence that other states would follow an American example. At one point, he notes that European states have often refused to cooperate in confronting China on trade and economic issues, providing rhetorical criticism of China even as they "continued to undermine the implementation of policies that advanced these positions."[8]

Much like the political science model of the "Stag Hunt," various individual states, whether African, Asian, or European, are as likely to cut their own deals with Beijing as cooperate in confronting a nation that offers access to a massive market and significant potential investment, no matter how many strings are attached. Patey provides little reason to think that this would change, no matter who is in the White House. Indeed, the book provides as much evidence that "we are not exporting our values to China—we are importing theirs."[9]

If the key to preventing China from winning is to "elicit a cautious reception and push back across the world that undermines its potential as a global superpower," there is little evidence that such caution and pushback, on a global scale in coordinated fashion, are forthcoming any time soon.

Other parts of the book also leave the reader wishing for more. One of the greatest contributions of *How China Loses* is that the volume gathers reports and discussions from a variety of global sources on a range of topics, such as economic, political, and military. Weaving this expanded picture provides the more casual observer of China with a better sense of its comprehensive, global efforts as a coherent whole, both in terms of Chinese strengths and weaknesses.

But Patey does not delve further into the issues. For example, he highlights that there are various bureaucratic weaknesses within the Chinese approach—but ultimately does not provide much insight beyond the observation that not every Chinese bureaucrat sees the world the same way. Are there consistent divides between the diplomats and the state-owned enterprises? Are there regional biases among China's provinces? Does the old "Shanghai faction" or do various princelings have ties to specific state-owned enterprises?

Equally frustrating is that many of the problems he highlights are not primarily due to China. Patey notes, for example, that "many of the problems China's projects suffer from in Africa are also typical for the construction industry worldwide."[10] Similarly, he notes that at least some alleged "debt traps" that China exploits are less the result of Beijing's machinations than the consequences of both lender and borrower behavior. Is China, then, really the problem? One of China's weaknesses is supposed to be that its actions do not counter local corruption. But if local populations and officials are unhappy with Chinese actions that abet local corruption, are they actually unhappy with China or with local corruption? Or are they unhappy because they are unable to share in that corruption?

Along these lines, Patey also seems not to recognize that at least some of the issues he is discussing are endemic to great power competition and are not unique to the 21st century or to China. During the Cold War, various states sought to play the United States and Soviet Union, and their associated blocs, against each other in pursuit of aid. Many of the techniques appear little changed as applied to the World Bank and Chinese lenders, or Western states concerned about growing Chinese influence.

What *How China Loses* does well is bring together both Chinese successes and failures, providing evidence of both its strengths and weaknesses. It also underscores the reality that China is not, in the end, simply a great power seeking a place for itself within the rules-based international order (although that is not nearly as conclusively demonstrated). The volume provides a useful one-stop shop of Chinese actions across a range of locales, including Africa and South America as well as Europe and Southeast Asia.

But it neither demonstrates that China will lose, nor provides much useful guidance on how to achieve that end. Readers hoping for a more concrete assessment of Chinese ends—and therefore methods of deterring or defeating them—will likely be left frustrated. PRISM

Notes

[1] Thomas Wright, "Joe Biden Worries that China Might Win," *The Atlantic* (June 9, 2021) https://www.theatlantic.com/international/archive/2021/06/joe-biden-foreign-policy/619130/.

[2] China to 'Emulate' Singapore's Economic Model," BBC (November 13, 2012) https://www.bbc.com/news/av/world-asia-20307144, Felix Chang, "The Odd Couple: Singapore's Relations with China," FPRI E-Notes (December 3, 2019) https://www.fpri.org/article/2019/12/the-odd-couple-singapores-relations-with-china/.

[3] Peter Beinart, "China Isn't Cheating on Trade," *The Atlantic* (April 21, 2019) https://www.theatlantic.com/ideas/archive/2019/04/us-trade-hawks-exaggerate-chinas-threat/587536/, and Ryan Hass, "Who Was Mike Pence Really Addressing in His Speech on China?" Brookings Institution (October 4, 2018) https://www.brookings.edu/blog/order-from-chaos/2018/10/04/who-was-mike-pence-really-addressing-in-his-speech-on-china/.

[4] Luke Patey, *How China Loses* (NY: Oxford University Press, 2021), p. 253.

[5] Luke Patey, *How China Loses* (NY: Oxford University Press, 2021), p. 11.

[6] Luke Patey, *How China Loses* (NY: Oxford University Press, 2021), p. 91.

[7] Luke Patey, *How China Loses* (NY: Oxford University Press, 2021), p. 92.

[8] Luke Patey, *How China Loses* (NY: Oxford University Press, 2021), p. 134.

[9] Jim Geraghty, "We Are Not Exporting Our Values to China—We Are Importing Theirs," National Review (October 8, 2019) https://www.nationalreview.com/the-morning-jolt/were-not-exporting-our-values-to-china-were-importing-theirs/.

[10] Luke Patey, *How China Loses* (NY: Oxford University Press, 2021), p. 97.

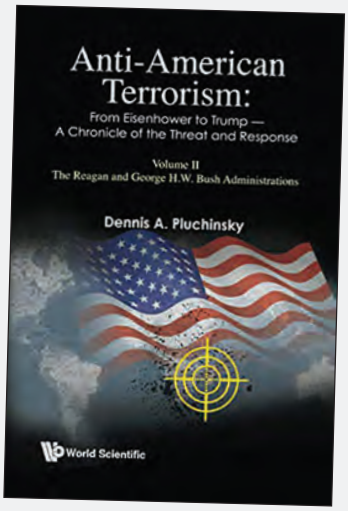
Anti-American Terrorism: From Eisenhower to Trump: A Chronicle of the Threat and Response

Volume I: The Eisenhower Through Carter Administrations

Volume II: The Reagan and George H.W. Bush Administrations

By Dennis A. Pluchinsky
World Scientific Publishing Europe, Ltd., 2020
Vol I 617 pp, $36.00, ISBN: 978-1-78326-872-6
Vol II 630 pp, $38.00, ISBN: 978-1-78634-829-6

Reviewed by Aaron Danis



This year (2021) the counterterrorism campaign that started out as the Global War on Terrorism is 20 years old. It has not ended, but with the death of Osama bin Ladin in 2011, the operational neutralization of the al-Qaeda core in Afghanistan and Pakistan, and the U.S. withdrawal from Afghanistan, it has moved on to other battlefronts. Although the United States is now focusing on state-centric Great Power Competition, the terrorist fights continue at a lower intensity in the Middle East, Africa, parts of Asia, Europe, and on the American home front (it never really left). It is time for a long-term retrospective and reckoning for the counterterrorism fight. The two volumes reviewed here are the start of that process.

To begin, the three main points readers should take away from these two volumes are those that I emphasize in my terrorism and counterterrorism courses. First, in the era of modern terrorism, the United States has a lot of experience countering an ideologically diverse set of terrorism threats, both domestically and internationally, but the lessons get lost over time. Second, U.S. counterterrorism policy is evolutionary, not revolutionary, and has gradually built on previous counterterrorism policies, even if the bloodlines are not obvious to the new generation of counterterrorism policymakers. Third, U.S. counterterrorism policy is reactive, not proactive, and tends to ignore emerging threats until they are knocking on the door. The fact that the threat has been so enduring suggests that the United States should stop worrying about "winning" the Global War on Terrorism, but instead manage it.

Mr. Dennis Pluchinsky was a senior terrorism analyst in the U.S. Department of State's Office of Intelligence and Threat Analysis from 1977 to 2005,[1] and thus was perfectly placed to expound on these three points above.

It is rare that someone points to a book and says it is that author's life work. I can point to Mr. Pluchinsky's first two volumes and confidently state that he is well on his way to completing a life's work on anti-American terrorism threat and counterterrorism policy and operations. There is simply nothing else like it. The first two volumes clock in at over 1,300 pages of text that cover the

Mr. Aaron Danis works for the Office of the Director of National Intelligence as a faculty member with the National Intelligence University.

time periods between the 1950s and 1992, with the introductory chapter in the first volume being 65 pages alone. Certainly, one should ask what would possess Mr. Pluchinsky to attempt such an encyclopaedic project?

Mr. Pluchinsky clearly is no stranger to writing on the theme of terrorism, having co-written two seminal books on left-wing terrorist groups in Europe during the Cold War. As he states in his author's note, his goal for this project is for the volumes to become standard references on the topic for future scholars, analysts, and policymakers. This is no mean feat considering the amount of ink spilled on anti-U.S. terrorism since 9/11 alone.

The depth of Pluchinsky's research and historical knowledge is showcased in these volumes. In addition to mining previous books on the topic, he has interviewed participants, requested thousands of government documents through the Freedom of Information Act, and searched the collection of hard-to-find unclassified historical publications that he retained from his career, most of which can now be found in the Naval Postgraduate School Homeland Security Digital Library.

These volumes examine both the threat to the United States and the U.S. policy response. Mr. Pluchinsky has built on work by others, to include Yonah Alexander and Michael B. Kraft, editors of the three-volume set *Evolution of U.S. Counterterrorism Policy,* which holds nearly 1,500 pages of White House, State Department, Department of Defense, and Congressional documents, speeches, and testimony dating from the Nixon administration and ending before the Obama administration. Pluchinsky goes the extra mile to put government documents into context with analysis using interviews and memoirs.

Finally, it is notable that Pluchinsky does not just focus on foreign terrorism; he gives equal weight to the domestic threat (which he labels the "internal threat") and policy, discussing groups such as the Puerto Rican nationalist groups Armed Forces of National Liberation (FALN) and the Boricua Popular Army (*Los Macheteros*—The Machete Wielders), both of which were active in the 1970s and 1980s when they tried to force the U.S. government to grant independence to Puerto Rico despite contemporaneous evidence that the island's population preferred Commonwealth status or statehood. For the current generation of would-be terrorist experts who act as if domestic terrorism is a new phenomenon, Pluchinksy discusses right-wing groups like The Order and the Covenant, Sword, and the Arm of the Lord, as well as left-wing groups like the Weather Underground, the Symbionese Liberation Army (famed for kidnapping newspaper heiress Patty Hearst), and the Black Liberation Army, among many others. Seeing that almost all Federal Bureau of Investigation (FBI) agents who worked any of these cases are by now retired or close to it, the FBI would do well to buy many copies of these volumes to issue to new agents and analysts to avoid making the mistakes of the 1970s and 1980s over again.

I have a couple of quibbles about the volumes, but they are not showstoppers. The first issue is a result of Pluchinsky's former home agency, the State Department, and future releases in its justifiably slow-moving *Foreign Relations of the United States* (FRUS) historical series. State historians are currently working on writing and declassifying the FRUS volumes for the Reagan administration. The two-part terrorism policy volume will span 12 years from the Jimmy Carter to the George H.W. Bush administrations. It is probable that newly declassified revelations from this era await despite Pluchinsky's herculean research and archival efforts here.

The second issue is the lack of a consolidated bibliography. I assume it was not included because it would take another 50-plus pages and would add to the cost of the book. Because the books are so well footnoted, however, it is possible to find source material without a bibliography. Perhaps publisher World

Scientific will compile and post a consolidated bibliography on its website when the project is completed.

In conclusion, anyone who is going to study, assess, publish on, or teach terrorism cannot be without these first two volumes at arms' reach. All academic libraries should have it stocked. Mr. Pluchinsky is diligently working on the final two volumes, to be finished in 2022 and 2023, respectively. Until those are released, U.S. analysts, law enforcement and defense officials, and policymakers have plenty of lessons to mine from these volumes. PRISM

Notes

[1] I have known Dennis Pluchinsky professionally and personally for over 20 years and have been mentioned in the acknowledgment section of each volume.

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.

INSS

INSTITUTE FOR NATIONAL
STRATEGIC STUDIES