

# PRISM

VOL. 9, NO. 1 | 2020

THE JOURNAL OF COMPLEX OPERATIONS

# PRISM

VOL. 9, NO. 1, 2020

## EDITOR IN CHIEF

Mr. Michael Miklaucic

## ASSOCIATE EDITOR

Mr. Dale Erickson

## EDITORIAL ASSISTANTS

Ms. Lolei Brenot

Ms. Julia Filan

Ms. Julianna Pestretto

## INTERNET PUBLICATIONS EDITOR

Ms. Joanna E. Seich

## DESIGN

Mr. John Mitrione, U.S.

Government Publishing Office

## EDITORIAL BOARD

Dr. Gordon Adams

Dr. Pauline Baker

Ambassador Rick Barton

Dr. Alain Bauer

Dr. Hans Binnendijk

ADM Dennis Blair, USN (ret.)

Ambassador James Dobbins

Dr. Francis Fukuyama

Ambassador Marc Grossman

Ambassador John Herbst

Dr. Laura Junor (ex officio)

Dr. David Kilcullen

Ambassador Jacques Paul Klein

Dr. Roger B. Myerson

Dr. Moisés Naím

Ambassador Thomas Pickering

Dr. William Reno

Lt. Gen. John F. Sattler, USMC  
(ret.)

Dr. James A. Schear

Dr. Joanna Spear

ADM James Stavridis, USN (ret.)

Dr. Ruth Wedgwood

ISSN 2157-0663

## ABOUT

*PRISM*, the quarterly journal of complex operations published at National Defense University (NDU), aims to illuminate and provoke debate on whole-of-government efforts to conduct reconstruction, stabilization, counterinsurgency, and irregular warfare operations. Since the inaugural issue of *PRISM* in 2010, our readership has expanded to include more than 10,000 officials, servicemen and women, and practitioners from across the diplomatic, defense, and development communities in more than 80 countries.

*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, best practices, or training and education innovations. 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 the 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.

Potential authors can submit their manuscript for blind peer review at <prism@ndu.edu>. Writing guidelines, tips, and tricks are available at <<https://ndupress.ndu.edu/Journals/PRISM/>>.

## DISCLAIMER

This is the authoritative, official U.S. Department of Defense (DOD) edition of *PRISM*. Any copyrighted portions of this journal may not be reproduced or extracted without permission of the copyright proprietors. *PRISM* should be acknowledged whenever material is quoted from or based on its content.

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of DOD or any other agency of the Federal Government, or any other organization associated with this publication.

## FEATURES

- 3** The Essence of the Strategic Competition with China  
By Michael J. Mazarr
- 23** Rediscovering a Strategic Purpose for NATO  
By Peter Ricketts
- 33** The Evolution of Authoritarian Digital Influence: Grappling with the New Normal  
By Shanthi Kalathil
- 53** Quantum Computing's Cyber-Threat to National Security  
By Steve Grobman
- 69** No Competition Without Presence: Should the U.S. Leave Africa  
By Katherine Zimmerman
- 89** China's Strategic Objectives in a Post-Covid-19 World  
By Benjamin Tze Ern Ho
- 103** International Competition to Provide Security Force Assistance in Africa: Civil-Military Relations Matter  
By Jahara Matisek
- 115** Don't Trust Anyone: The ABCs of Building Resilient Telecommunications Networks  
By Andy Purdy, Vladimir M. Yordanov, and Yair Kler
- 131** Is China Expansionist?  
By Kishore Mahbubani

## INTERVIEW

- 140** General (Ret.) Joseph Votel  
Interviewed by Michael Miklaucic

## BOOK REVIEWS

- 147** Exercise of Power: American Failures, Successes, and a New Path Forward in the Post-Cold War World, by Robert Gates  
Reviewed by James Stavridis
- 150** The Return of the Russian Leviathan, by Sergei Medvedev  
Reviewed by John Herbst
- 153** The Dragons and the Snakes: How the Rest Learned to Fight the West, by David Kilcullen  
Reviewed by Carter Malkesian



"A geopolitical competition between free and repressive visions of world order is taking place in the Indo-Pacific region."  
National Security Strategy of the United States of America, 2017. (Staff Sgt. D. Myles Cullen (USAF), 22 March 2007)

# The Essence of the Strategic Competition with China

Michael J. Mazarr

U.S. national security strategy and defense policy have come to focus on China as the primary emphasis in the “strategic competition” outlined by recent U.S. strategy documents.<sup>1</sup> Outside government, an avalanche of recent reports and essays lays out the China challenge in sometimes fervent terms, depicting an ideologically threatening revisionist state with malign intentions. As the *Financial Times* columnist Martin Wolf put it recently, “Across-the-board rivalry with China is becoming an organizing principle of U.S. economic, foreign and security policies.”<sup>2</sup>

There is little question that China’s growing power, its military buildup, its bold regional and eventually global ambitions, and its outsized self-conception pose very real challenges to the United States and the post-war, rule-based order. China is neither infinitely powerful nor wholly malicious. But its belligerent coercion of its neighbors, threat to use force to absorb Taiwan,<sup>3</sup> violations of human rights, predatory economic behavior, and many other activities mark its rise as a potential threat to U.S. security and any sort of rule-based international system.

Yet there remains a question of precisely what *sort* of challenge China poses—and, by extension, the true essence of the emerging competition. This article argues for one answer to that question: At its core, the United States and China are competing to shape the foundational global system—the essential ideas, habits, and expectations that govern international politics. It is ultimately a competition of norms, narratives, and legitimacy; a contest to have predominant influence over the reigning global paradigm. That paradigm, I will argue, is comprised of four components; economic and political values, cultural influences, leading rules and norms embodied in international law, agreements, and practice, and leadership of and standards reflected in international institutions. The article also contends that, despite its massive investments in propaganda tools and economic statecraft, China remains starkly ill-equipped to win such a competition—but the United States could, through self-imposed mistakes, lose it.

The article makes this case in four parts. First it offers reasons why other components of the competition often said to be central—military, economic, and clashing geopolitical interests—are in fact

---

Michael Mazarr is a senior political scientist at the RAND Corporation. The views expressed here are his own and do not reflect the findings of a specific RAND study. Portions of this essay previously appeared in an edited set of essays released by the Strategic Multilayer Assessment in the Joint Staff J-7.

secondary aspects of the emerging rivalry. Second, the essay reviews various theories of power to make the case that direct, coercive power is both less effective and less sustainable in the long-term than more indirect, systemic forms of the kind at stake in the competition for the wider paradigm. Third, this analysis examines theories of legitimacy and legitimate authority to further define the ways in which states gain systemic influence. Fourth and finally, drawing on those theoretical foundations, the essay defines the characteristics of the current competition for the paradigm and outlines implications for U.S. policy.

## Secondary Components

Many assessments of the U.S.-China competition focus on three leading issues; the military and economic parts of the overall competition and specific geopolitical disputes involving Chinese territorial ambitions. These three elements are crucial and require U.S. attention and effort but are best viewed as secondary or supporting elements of the main contest.

The argument here is not that these more material or “harder” forms of power are unimportant to the competition. Indeed, as I will argue below, material power, and especially aspects of economic power and influence, establish part of the basis for success in normative terms. Claims to ideological supremacy must rest on strong material foundations. Investments in the long-term foundations of economic competitiveness, such as key emerging industries, research and development, and economic justice and equality, remain critical. The argument here is rather that such investments are means to a more important end and will not on their own win the competition—either for the United States or China. What is ultimately at stake is not a higher GDP or advantage in selected military systems; it is the power to exercise predominant influence over the defining ideas, rules, and institutions of world politics.

## *The Military Competition*

The U.S.-China contest, for example, has an important military component. China poses an obvious danger to Taiwan. It has coerced other claimants to contested areas of the South China Sea, waged a limited war against Vietnam, and tangled with India over disputed land. It is engaged in a potent military buildup. Even short of war, credible military power is a critical supporting instrument to reassure friends and allies and avert a creeping belief that there is no alternative but to knuckle under to China.

Yet the military threat posed by China is muted in comparison to classic militaristic predators, at least for now. Beijing is not set to launch vast armies and fleets to invade and conquer its neighbors.<sup>4</sup> Prospective targets of adventurism are mostly too large and populous to be absorbed in this way; many are too far away; the benefits of owning territory are minimal; the difficulty of power projection is now extreme;<sup>5</sup> the risk of war with the United States and others would be too great. While China’s long history is hardly free of adventurism, invade-and-occupy strategies have mostly been alien to China’s modus operandi beyond its own territory: It prefers to overawe Asia rather than occupy it. In its “gray zone” tactics and elaborate economic investment programs, China gives every indication of intending to pursue its goals short of the use of force. China’s dominant strategies, in short, are not built around conquest; the competition is not likely to be resolved by military power.

This part of the competition is also constrained because China’s military ambitions, even at their most extensive, have no prospect of threatening vital U.S. interests. Chinese military seizure of Taiwan would be a tragedy and a crime, and the United States should not endorse Beijing’s coercive control over the country—but it would not threaten the existence of the United States. Even Chinese military hegemony over Southeast Asia, as much as it would impair U.S. and allied freedom of action and as much as the United States should strongly support

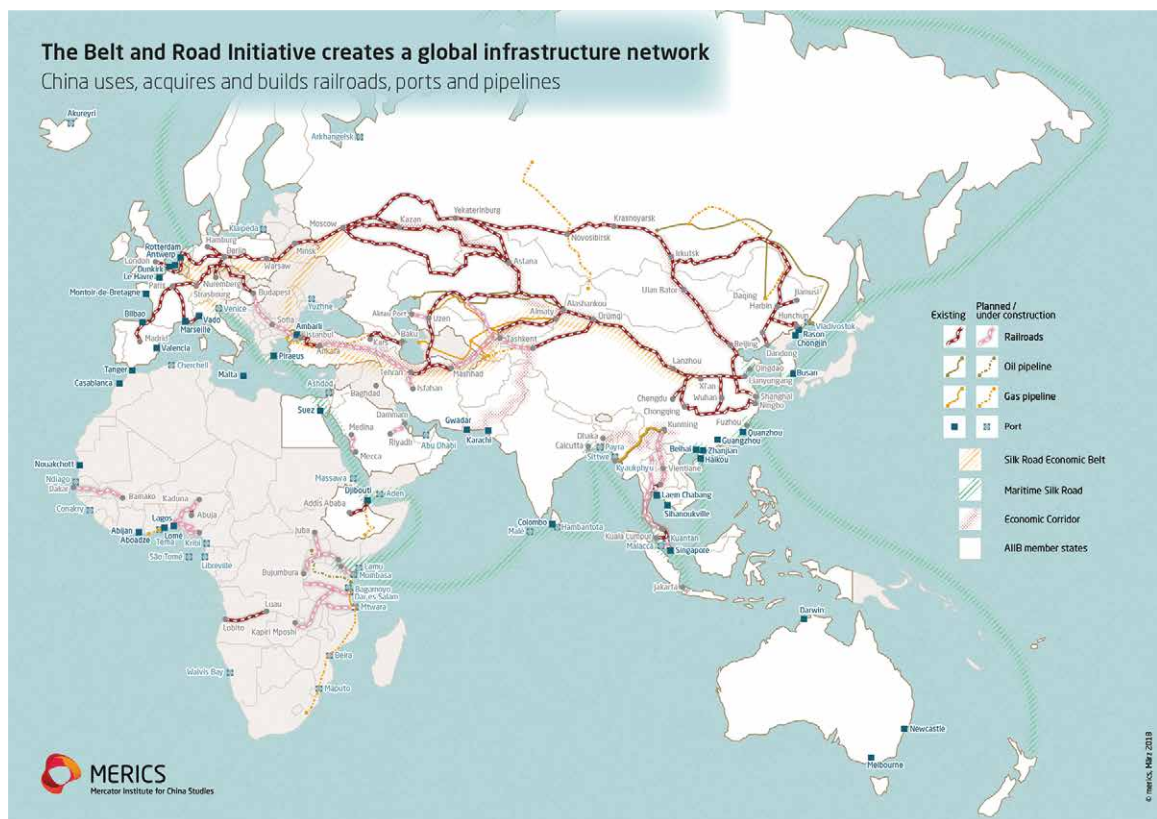
others in the region to oppose it, does not represent anything close to an existential threat. The French-German rivalry of the 1930s—to take only one example—was centrally and primarily a military competition for the obvious reason that each state posed a direct military threat to the other, threats that had been repeatedly exercised in previous centuries. Nothing like that core military aspect exists in the U.S.-China relationship. Neither of the two countries poses a direct, existential military threat to the other's homeland.

### *The Economic Competition*

The competition also has critical economic elements. Most broadly, economic performance, and the ability to compete in leading industries, provide the foundation for competitive strength. China is aiming for

dominance in a range of key industries. It is using foreign investment—notably through the Belt and Road Initiative—to reorient Eurasia around a Chinese hub. Some of its strategies for doing so are aggressively incompatible with a rule-based economic order.

Yet while economic instruments are leading tools, the competition is not at its core an economic dispute. In its state-led developmentalism China is merely practicing an approach many rising powers have used, from supporting key industries to investing in frontier industries to buying—or stealing—foreign technology.<sup>6</sup> Such state-led strategies are not wholly incompatible with a shared, nondiscriminatory global economic order; indeed, the coming years are likely to see more energetic versions of industrial policy in many countries, including the United States.



China has invested more than 70 billion USD into BRI-related infrastructure projects according to the MERICS BRI database. (Merics Institute for China Studies)

China's engagement with the shared international economic order has been imperfect but hardly a sham, reflecting many real reforms.<sup>7</sup> It aims to make itself rich and powerful, not to destroy the economies of others. Economics, at the end of the day, is a positive-sum affair. If China is willing to constrain its economically predatory activities—and that remains an open question—the United States and China ought to be able to compete vigorously across many industries even as they remain at peace and collaborate on issues of mutual concern.

These limits suggest that the competition is not primarily, at its essence, an economic one. Economics alone will not provide China with the leverage to dominate key regions or issues. A good example is the economic dependence China has managed to achieve in regard to countries in Asia—dependence that has not prevented these countries from pushing back vigorously against Chinese coercion.<sup>8</sup> The level of countries' overall trade dependence with China has remained mostly stable in recent years, and Chinese foreign direct investment represents a modest component of most countries' total. The recent push in many countries to diversify sources of supply, sparked both by the tariff war between the United States and China and then the pandemic crisis, will also mitigate China's ability to use economics to achieve unique competitive advantage.

### *Geopolitical and Territorial Disputes*

Third and finally, the United States and China also have conflicting interests in specific regional disputes—chief among them, the struggle for the alignment of other states and China's sovereign claims to Taiwan and contested areas of the South China Sea. How these are resolved will set important precedents that shape world politics. But in none of these cases do the United States or China have interests that are at once vital and irreconcilable. China's objectives are not necessarily specific enough to

demand an absolute clash of interests; what it means, for example, by regional predominance is largely to be determined. Even the claim to Taiwan does not necessarily come with a specific timeline or form in which it must be resolved.

In terms of maritime control, there is no specific level of Chinese influence in the South China Sea that would pose a threat to vital U.S. interests. The potential remains for a tough, sometimes bitter, but nonetheless peaceful reconciliation of China's growing ambitions in Asia with U.S. national interests. Nor is either likely to prevail in absolute terms. Too many targets of their influence, from India and Vietnam to Indonesia and South Korea and even the Micronesian Island states, are vigorously determined to retain their sovereign independence. Simply put, neither the United States nor China has ambitions that *necessitate* efforts to challenge the vital interests of the other.

### **The Faces of Power**

The emerging U.S.-China competition, then, has important military, economic, and geopolitical components. Each of those issues demands significant U.S. attention and investment, from a credible military posture in Asia to government-funded research and development in key technologies to intensive diplomacy with pivotal states. But it is in another area that we find the true fulcrum of the contest, the hub around which these supporting elements will revolve, the contest whose outcome will be most decisive. That is in the competition for influence over the guiding narratives, ideas, and norms of the international system. The next two sections of this article examine two literatures that help make the case why this is so: Each represents a school of research on the nature of world politics, and each offers important insights about the ways great powers can prevail in strategic competitions. They have to do with the character of effective and sustainable power and the nature of legitimate authority wielded by great powers.



Many definitions of power long focused on its most straightforward variety; direct coercive or persuasive power—the ability to make some person or entity do something they would otherwise not do.<sup>9</sup> This is the form of power many observers are concerned that China has begun to wield, through economic and military force, in Asia and beyond. But over the course of the last half-century, scholars increasingly came to appreciate other, more indirect, subconscious and ideational forms of power—other faces or lenses which focus on shaping the agendas, habits, and worldviews that guide behavior.<sup>10</sup> These other interpretations of power speak to the ways in which actors achieve influence over people and groups by “shaping their perceptions, cognitions and preferences,”<sup>11</sup> and they point to the ways in which the United States has enjoyed such a predominant international position in the post-war era.

Direct power is forcing a state to liberalize its economy. Indirect power is creating a global marketplace (and, more than that, a dominant conventional wisdom) that makes its elites and leaders believe that such liberalization is in their interests. It involves influencing how people think—how they conceive their interests and very identities—rather than trying to coerce or bribe them into making a specific choice. It shapes what others believe they want, and why.

Indirect power can be more decisive than direct power.<sup>12</sup> Strong-arming other great powers is often impossible: As Iran and North Korea are reminding the United States, even weaker states can refuse the demands of stronger ones. Conflicting interests, national pride, the political interests of the target government, and a dozen other factors dull the impact of direct forms of power. But when the overall context shapes how those states view their own interests in ways aligned with U.S. objectives, U.S. influence is forcefully magnified. Even the realist Hans Morgenthau recognized this difference when he argued that,

*Cultural imperialism is the most subtle and, if it were ever to succeed by itself alone, the most successful of imperialistic policies. It aims not at the conquest of territory or at the control of economic life, but at the conquest and control of the minds of men as an instrument for changing the power relations between two nations. If one could imagine the culture and, more particularly, the political ideology ... of State A conquering the minds of all the citizens determining the policies of State B, State A would have won a more complete victory and would have founded its supremacy on more stable grounds than any military conqueror or economic master.*<sup>13</sup>

Some Marxist and postmodern thinkers describe such a process in more dystopian terms—as a form of thought control, more about submission than persuasion.<sup>14</sup>

Dystopian or not, such cultural power provides an important part of the story of how the United States won the Cold War and then attained a predominant global position afterward. Military deterrence of communist aggression was one part of the Cold War story, though arguably, past a certain point, not the dominant one. Nuclear weapons made big wars infeasibly costly, and the United States learned in Vietnam (as the Soviet Union did in Afghanistan) that even limited military force was at best a defensive measure. Rather, the United States prevailed in the Cold War contest primarily because its ideas, norms, structures, and institutions “conquered the minds” of elites and leaders the world over, including many within the Soviet bloc itself. Ideas associated with the United States and its friends and allies established hegemony over a predominant component of the international community—today, a bloc that represents well over three-quarters of world GDP and world military spending.<sup>15</sup>

Ideas need to have a persuasive basis to enjoy such success, and material factors were essential to the victory of the ideas associated with American power.<sup>16</sup> America's leading economic standing in 1945 and again in 1989, and its predominant military power after the Cold War, underwrote the credibility and appeal of its ideas. It was the Soviet system's inability to compete in material terms, and not a sudden affection for liberal values, that provided the main fuel for reform. The attraction of western-style reforms among Soviet leaders only emerged as a product of direct economic need: The Soviet Union was going bankrupt and needed to change. Ideas seldom conquer world politics absent material support systems—military and economic power that legitimizes and backs up those ideas.<sup>17</sup>

The most fundamental process, though—one unquestionably underwritten by material success—was the fact that the United States came to represent the metropole of the dominant ideas of world politics, ideas that were dominant in part because they were also associated with specific material outcomes, but also because they embodied inherently legitimate and appealing concepts—the appeal of liberal governance, human rights, and the cultural muscle of American films, music, and literature. The critical competitive advantage was this interlocking package; credible military power and impressive economic achievements tied to a larger, coherent set of social and cultural ideas with inherent legitimacy. Over time, this package had tremendous appeal, attracting states hoping to boost their security or economic fortunes. Few made this choice because the United States forced them to do it; most did so because the context and its dominant narratives made them believe it was in their own interests.<sup>18</sup>

This normative and systemic power manifested itself in very real sinews. They ranged from international economic institutions, to global human rights conventions and the advocacy organizations

that rose up around them, to the spread of American entertainment and media, to vast flows of students and tourists and military officers, to the gradual thickening of webs of international law and legal precedent.<sup>19</sup> These sinews then produced hundreds of practical outcomes which advanced U.S. interests: Developing nations agreed to rule-of-law reforms which produced a more stable global economy; trading partners assented to concessions and deals when required by the World Trade Organization; states were more apt to sign on to nonproliferation-oriented policies and sanctions in service of shared norms. The emergence of ideational hegemony thus left the United States much more likely to get what it wanted across numerous issue areas. One result was astonishingly positive trends in areas the United States sought to influence—democracy, human rights, economic growth and development, economic freedom, and the rule of law.

Despite its broadly shared values and norms, China sees this dominant paradigm as a by-product of American hegemony and Chinese second-class citizenship, a status it is furiously determined to shed. China—like Russia—also views the ideas associated with the reigning order as justifying regime change narratives which ultimately threaten the rule of the Communist Party. As I will argue below, however, China is poorly equipped to succeed in these more indirect avenues to power, or to offer a compelling alternative to the ideas associated with the post-war U.S.-led order.

## The Contest for Legitimate Authority

A second literature provides another useful way of understanding the competition for the international system and offers other reasons why that competition is so important to great power rivalry; the concept of legitimacy or “legitimate authority.” Max Weber and other classic scholars developed the notion to help explain sustainable and effective forms of governance within states, and over time

others applied them to the international arena. These scholars emphasize a similar point to the analyses of the nature of power: Direct, material, coercive or directive power is not always the most effective or sustainable. Authority that comes from a perception of legitimacy is more lasting and ultimately influential—and the post-war U.S.-led order reflects elements of this more than a China-led order could do in the 21<sup>st</sup> century.

### *Understanding Legitimacy*

One scholar defines legitimacy as, “The normative belief by an actor that a rule or institution ought to be obeyed. It is a subjective quality, relational between actor and institution, and defined by the actor’s *perception* of the institution.”<sup>20</sup> A perception of legitimacy is distinct from coercion and rationalist perception of self-interest: Individuals or states may comply with a rule because they are forced to do so, because they perceive clear material interest in doing so—or because they view it as legitimate. The scholar Ian Hurd, one of the most thoughtful recent scholars of international legitimacy issues, explains that,

*Compliance with a rule may be motivated by a belief in the normative legitimacy of the rule (or in the legitimacy of the body that generated the rule). Legitimacy contributes to compliance by providing an internal reason for an actor to follow a rule. When an actor believes a rule is legitimate, compliance is no longer motivated by the simple fear of retribution, or by a calculation of self-interest, but instead by an internal sense of moral obligation: Control is legitimate to the extent that it is approved or regarded as “right.”*

The ability of great powers to set such norms then becomes a form of power to the degree that they are internalized by recipient nations and taken as a rule, or that is “authoritative over the actor.”<sup>21</sup> The political scientist John Gerard Ruggie has

similarly argued that, “Political authority represents a fusion of power with legitimate social purpose.”<sup>22</sup>

Legitimacy can arise from many sources.<sup>23</sup> First, like indirect or systemic power, it can be grounded in a perception of material benefits—things that provide “favorable outcomes” to participating states, groups, or individuals. People and states find legitimate that which meets their own material needs and interests. But material outcomes are not the only, or even always the most important, sources of legitimacy. It can also arise from a belief that the governing institutions reflect a basic sense of fairness, or be grounded in a perception of adherence to “correct procedure.” The validity of a norm and the soundness of a legitimate authority are also partly a function of a faith in enforcement:<sup>24</sup> When members of a community have no faith that norms will be enforced, the validity of the overall system of authority wanes. Finally, legitimacy emerges in part from “the intrinsic qualities of the norms and ideas being articulated by the hegemon.”<sup>25</sup> Norms which uphold human dignity, for example, have an inherent legitimacy that a resort to brute force would not.

The emergence of a perception of legitimacy in these and other ways is not entirely distinct from the process of determining national interests, objectives, or even strategies for achieving them. Perceptions of legitimacy help to determine, as one author says, “what gets included in the calculus of interest.”<sup>26</sup> That is, a perception of legitimate authority becomes a critical part “of the state learning what it *wants*.”<sup>27</sup> A good example is in the post-war territorial integrity norm: States have accepted the legitimacy of institutions and processes that generated it and to some extent the leaders of the international system who enforce it. States no longer “want” territorial acquisition as they once did—surely in part because of material reasons (territory is no longer as valuable as it once was), but also because of a conception of what is “legitimate” behavior.

These restrictions derive in part from the close connection between legitimacy and community. Legitimate authority is grounded in an agreed community with shared rules: “For there to be legitimacy there needs to be a community/society, and the fact that legitimacy makes sense within it is clear evidence that such a community/society actually exists.” An implication is that, once states have recognized a given authority and its norms as legitimate (and perceive an essential validity in the larger system), those who refuse to abide by those norms lose their “rightful membership in the family of nations.”<sup>28</sup> This is partly because a system of legitimate authority will define the “normal pattern of behavior” expected of community members, and in turn shape “the structure of opportunities faced by states” in ways that alter their choice of ends and strategies for achieving them.<sup>29</sup>

This clash between opposing systems of ideas reflects a clear historical pattern—recurring contests over legitimating narratives in great power rivalries.<sup>30</sup> Burgeoning material power is essential but not enough: Great powers, especially rising powers, must demonstrate that their bid for influence is legitimate. If they cannot, their power will always be limited by natural push-back from the larger system. Even the most dominant powers cannot bully their way to everything they want: Dominating the space of ideas, ideologies, and narratives is the basis of more complete and lasting competitive success.<sup>31</sup>

### *The Normative Foundation of Hegemony*

This close connection between legitimate authority and communal identity helps to explain why legitimacy—while partly dependent on the compelling image of material power—also has non-material roots. Richard Ned Lebow has described ancient Greek conceptions of multiple forms of power: They “understood,” Lebow suggests, “the transformative power of emotion: how it could combine with reason to create shared identities, and with it, a general

propensity to cooperate with or be persuaded by certain actors.”<sup>32</sup> Legitimate authority appeals to such emotions, to the willingness to see one’s identity as part of a community which has the accepted right to enunciate certain rules for the collective group.<sup>33</sup> This is even true of the most powerful states: Even the hegemon in such a system must be subject to its rules.<sup>34</sup>

Lebow has discussed how the Greeks distinguished various forms of power and influence; that achieved through deceit (*dolos*) as opposed to that achieved through more legitimate persuasion, “by holding out the prospect of building or strengthening friendships, common identities and mutually valued norms and practices” (*peithō*). This latter form of power, according to many classic Greek historians and philosophers, is ultimately more lasting and effective “because it has the potential to foster cooperation that transcends discrete issues, builds and strengthens community and reshapes interests in ways that facilitate future cooperation.” Lebow continues;

*Capability-based theories of influence like realism assume that influence is proportional to power, measured in terms of material capabilities. ... The Greek understanding of the psyche suggests that capability-based influence always has the potential to provoke internal conflict and external resistance because of how it degrades the spirit—and all the more so when no effort is made to give it any aura of legitimacy through consultation, institutionalization, soft words and self-restraint. Peithō is least likely to generate resistance, especially when initiated by an actor whose right to lead ... is widely accepted.<sup>35</sup>*

Ancient Greek thinkers made a second distinction to understand the character of systemic leadership; between what they called *hēgemonia* or legitimate authority grounded in accepted

institutional position, contributions to the common good, and shared norms, and *archē* or coercive, hierarchical rule over others grounded in superior material capabilities.<sup>36</sup> There are many exceptions, both in terms of countries with a more negative appraisal of the United States and U.S. behavior on specific issues, but broadly speaking what has made U.S. post-war power unique is the degree to which it has reflected *hēgemonia* rather than *archē*.

As with legitimacy and power more generally, the achievement of an acknowledged and sustainable variety of hegemony thus has normative foundations.<sup>37</sup> It is not just a measure of material power, but a “thick phenomenon encompassing elite and mass beliefs” which points to the “substantive ideational content” as being important. Ideological or normative agreement among elites and populaces

is as important as coercive power in a sustained and legitimate hegemony. If a normative order appeals only to elites, its power will be less complete and sustainable than an order whose norms reach into the “common sense” of the people.<sup>38</sup>

Three scholars define a hegemonic order as one “in which a leading state or coalition can establish and impose rules on other great and secondary powers.” As a result of the normative foundations of hegemony, they conclude that,

*A hegemon cannot impose rules without securing a broad measure of consent through the production and reproduction of a legitimating ideology. The legitimating ideology serves to promote and protect the taken-for-granted rules and ideas that structure international order.*<sup>39</sup>



The 1945 San Francisco Conference at which 46 nations signed the United Nations Declaration establishing one of the key institutions of the post-war U.S.-led international system.(UN Photo/Historical Photo)

This degree of consent distinguishes legitimate hegemony from empire or “pure domination” (or in ancient Greek terms, *hēgemonia* versus *archē*) and means that the hegemon can “rule without using coercion at every turn. Instead, other great-power states accept the hegemon’s leadership because they can see a place for themselves in the order.”<sup>40</sup>

This appeal to inclusive and communal interests is a critical part of the story of U.S. power in the post-World War II era. As Lebow explains, post-war U.S. leaders “created economic, political, military and juridical institutions that, at least in part, tended to restrain powerful actors and reward weaker ones.” As a result, “American hegemony during the Cold War was based on the sophisticated recognition that the most stable orders are those ‘in which the returns to power are relatively low and the returns to institutions are relatively high.’”<sup>41</sup> To be sure, the United States advanced its own selfish interests after 1945 on many occasions, and sometimes took actions that were excessive or needlessly unilateral. And all throughout the Cold War, American material power—economic as well as military—provided critical underpinnings for the systemic victory. Yet in pursuing a version of legitimate authority, the United States exercised its power less crudely and coercively than many hegemonies and created a normative order with legitimacy and appeal.<sup>42</sup> It has variously been described as a “benign” or inclusive hegemon,<sup>43</sup> one whose leadership gained greater legitimacy because it is perceived in broad ways to be exercised in the name of an international community as much as for the United States itself.<sup>44</sup> The resulting shared order has had significant value for the United States,<sup>45</sup> but it has also worked to the advantage of many others.

The resulting paradigm created a platform for the United States to exercise influence through socialization. As John Ikenberry and Charles Kupchan have argued, states can exercise power

directly through material incentives. But they can also work through the more indirect forms of power noted above, seeking to alter,

*...the substantive beliefs of leaders in other nations. Hegemonic control emerges when foreign elites buy into the hegemon’s vision of international order and accept it as their own—that is, when they internalize the norms and value orientations espoused by the hegemon and accept its normative claims about the nature of the international system. ... Power is thus exercised through a process of socialization in which the norms and value orientations of leaders in secondary states change and more closely reflect those of the dominant state. Under these circumstances, acquiescence is achieved by the transmission of norms and reshaping of value orientations and not simply by the manipulation of material incentives.*<sup>46</sup>

The result has been an architecture of legitimate authority that made the U.S. post-war role nearly unique in the annals of historical great powers, especially those with hegemonic degrees of authority. It was the normative, paradigmatic, systemic, and rule-based power that made the U.S. role so different, so lasting, and so much less likely to prompt strong balancing by others.<sup>47</sup> Robert Cox argues that hegemonic power is propped up by “universal norms, institutions, and mechanisms which lay down general rules of behavior for states and for those forces of civil society that act across national boundaries.”<sup>48</sup> Ikenberry and Kupchan explain that effective socialization is grounded in legitimate authority, or “the common acceptance of a consensual normative order that binds ruler and ruled and legitimates power.”<sup>49</sup> Based on a number of historical case studies, they conclude that, “The ability to generate shared beliefs in the acceptability or legitimacy of a particular

international order—that is, the ability to forge a consensus among national elites on the normative underpinnings of order—is an important if elusive dimension of hegemonic power.”<sup>50</sup>

The concept of identity is an important part of the foundation for legitimate orders. A nation’s conception of its own identity establishes the basis for its view of whether it fits into a given normative order. If the influence of orders runs through elites to populations, governments will face greater difficulties joining orders that run directly counter to deeply established national identities.<sup>51</sup> A nation with a powerfully Islamic self-conception would be hard-pressed to easily integrate into an explicitly Christian order; a democracy would naturally resist an order based on autocratic norms. The predominance of established democracies among the world’s leading economies and major powers, the power of national identity, and the need to build a global order in accord with the identities of the major powers, will be substantial barriers to China’s legitimate hegemony of any order.

## A Fight for the Paradigm

These forms of structural or paradigmatic power are precisely what is at stake in the current U.S.-China rivalry. The emerging strategic competition reflects, at its core, a struggle over the context, the field in which world politics unfolds—the prevailing ideas, narratives, norms, rules, and institutions that shape states’ interests. This makes it an ideological competition, but of a specific sort. The revolutionary ideological adventurism central to Soviet and Chinese strategy in the Cold War is not characteristic of current Chinese policies. It is instead a competition between two would-be leaders of a governing ideational order, each offering a basic political model, essential economic principles, and other aspects of a set of norms and values.<sup>52</sup>

The international paradigm as conceived here has four main pillars. First are the prevailing global

political and economic values—whether elites and populaces tend toward values such as democracy, liberal economic policies, free trade, and human rights. These could be measured by such yardsticks as total numbers of regimes reflecting certain values, indices of political and economic freedom, and public opinion polling on favored values.

A second pillar of the international paradigm is cultural influences: Which countries, systems, peoples or groups set the global standards in cultural habits and in such areas as film, television, music, and literature? Influence in this pillar can be measured by prevalence of global cultural influence, opinion polls, and emergent habits and practices.

The third pillar of the current paradigm is global rules and norms as established in international law, conventions, and practice. These range from the territorial non-aggression norm enshrined in the UN Charter and many other compacts, to the core elements of international maritime law and the law of war, and can be measured in terms of formal agreement as well as the degree to which they are respected.

The fourth and final pillar is international institutions, both intergovernmental and non-governmental. Influence here can be measured by leadership positions and the policy stances the institutions take.

The primary U.S. task in the emerging competition is to preserve the astonishing advantages that accrue from being the hub of a shared and widely appreciated order of dominant ideas, norms, habits, and perspectives in each of these four pillars of the paradigm. Competing in military, economic, and geopolitical areas remains important, but these contests do not reflect the *essence* of the competition, which is ultimately a struggle for control of the global paradigm. Win that fight, and the rest is likely to fall into place. Lose it, or allow the ideational context to fragment (as is already occurring, partly because of U.S. actions), and U.S. power and interests will confront a vastly more hostile world.

### *Limits to China's Normative Legitimacy*

China's task is clear; to establish a competing ideational pole in world politics. It has been vocal about its desire to promote an alternative socioeconomic model—the so-called “Beijing Consensus,” the China Model, the China Dream. Its increasingly aggressive attacks on U.S. and western values and ideas hope to discredit them in the eyes of much of the rest of the world.<sup>53</sup> Yet the scholarship on power, legitimacy, and paradigmatic influence through institutions and norms strongly suggests that China confronts formidable, indeed perhaps insurmountable, barriers to success in these terms. As three scholars have argued, during a period of partial or broad-based power transition, “when the identity of the rising state is consistent with the ideologies and identities underlying the order, hegemony is likely to be stable.” When the rising state's values contradict those of the establish paradigm, on the other hand, it will be hard-pressed to create a new hegemony.<sup>54</sup> This is exactly the problem China faces today—and it stems not from simple policy or strategy differences, but from a fundamental, systemic clash between the identity of the Chinese Communist Party and the norms underlying the prevailing order.

To begin with, Beijing has no universal set of values and norms to offer as the foundation of a new, Sino-centric world paradigm. The cheerful phrases that populate its public diplomacy do not describe any coherent system, and anyway are daily contradicted by its own autocratic behavior at home and abroad. (Beijing cannot proclaim itself an advocate of democracy while working assiduously to silence critics abroad through Orwellian forms of harassment.)<sup>55</sup> Well-funded state propaganda tools can do little in this regard: Ideational power emerges from societies in an organic process, largely through example and the work of private actors. It cannot be forced into place in a five-year plan.<sup>56</sup>

Economically, despite its impressive record, China has no easily-exportable model of growth

beyond classic state-led development—which has failed as often as it has succeeded.<sup>57</sup> The shining example of its economic model is anyway likely to dim, due to slowing growth, an aging society, and blowback against its predatory and corrupt practices abroad. The more intriguing concepts Beijing has put on offer, such as a more fully democratic and pluralistic international order, run counter to China's historically hierarchical instincts. They are also easily co-opted, if the United States is willing to embrace a more shared and humbler version of leadership. Moreover, world politics is different than it was in 1945—with more diverse and dispersed sources of power, richer flows of information, less respect for authority—in ways that will make it tougher for Beijing to achieve the deference it reportedly craves.<sup>58</sup>

China, of course, represents a very different sort of economic rival than the Soviet Union. Its economic engine is vastly larger and more effective; its mastery of numerous advanced technologies outside the military sphere well beyond anything the Soviet system could muster. In this sense we cannot expect or hope for a rapid change in the Chinese system itself, as it encounters insurmountable barriers to competitive vibrancy. It will have an economic gravitational force unlike anything the Soviet Union ever achieved and continue to serve as a viable model for handfuls of nations which choose its system as a model. Beijing will surely have a significant degree of economic influence.

It will also be able to translate these forms of economic power into some degree of systemic influence. It is using economic power in part to place senior officials in key posts in international organizations, including the United Nations.<sup>59</sup> It is using economic muscle to establish parallel institutions on a host of issues, from development to regional political forums. It is using dominance of key industries, such as 5G telecommunications, to gain a leading role in global standard-setting. It is bribing and





Police seemingly indiscriminately arrested protestors in Hong Kong on riot related charges. (Bill Gallo, VOA News, 18 November 2019)

coercing other countries into compliance with some aspects of its systemic goals. As noted above it is investing billions in a “global megaphone” of social media, broadcast entities, classic propaganda, and other forms of influence.<sup>60</sup>

But these strategies are likely to take Beijing only so far in the quest for systemic leadership and a veto power on the policies and actions of others. Its actions are prompting increasing levels of concern and blowback in countries from Europe to Australia to South Korea, and even selected African countries. China has managed to generate highly negative public opinion in a range of countries it has sought to bully, from the United States to Canada, Sweden, Vietnam, and Japan.<sup>61</sup> A recent survey of opinion in Southeast Asia found a range of attitudes, including significant respect for Chinese achievements, but growing concern about the implications of rising Chinese power and an almost universal belief that Chinese military strength was a threat to the region.<sup>62</sup> If anything, China’s multiple hard line actions of recent years—its crackdown on Hong Kong (now

intensified in recent months), repression in Xinjiang Province, threats against journalists and politicians abroad, direct coercive behavior in the South China Sea, and many other actions are promoting more resistance rather than accommodation.

One recent study conducted in-depth analyses of public opinion and public discourse data to characterize elements of national identity in states identified as current great powers, including Brazil, France, Germany, India, Japan, and the United Kingdom. Their research found significant support for both democratic and (less universally) neoliberal values—and very little support for countervailing Chinese norms. “While some aspects of western neoliberal hegemony are contested,” the study concluded, “the distribution of identity among the great powers provides strong support for western hegemony.” The study highlighted the intense dilemma facing China’s quest for a legitimate hegemony, noting that, “it is unlikely that China can build an ideology that would simultaneously satisfy its domestic needs and appeal to others.”<sup>63</sup>

These shortcomings are on vivid display in China's most recent attempt to promote its own leadership of the international system—its efforts to build a narrative of Chinese success and altruism during the current COVID-19 pandemic crisis. These efforts have had at best partial success and there has been significant blowback in many places to China's behavior and its narrative.<sup>64</sup> During the crisis, the actions of its so-called “Wolf Warrior” diplomats—nationalist and aggressive officials seemingly determined to flaunt Chinese power and reject any challenge—have become even more bellicose. The reaction, in many quarters, has been one of growing concern and outrage.<sup>65</sup> Those reactions betray again a consistent theme: Many other countries view Beijing's exercise of its power and influence as essentially self-serving. The nature of China's view of the world—Sino-centric, hierarchical, culturally exclusive, domineering—undermines its efforts to exercise legitimate authority, and its lack of an inherent set of appealing values ruins its potential to benefit from indirect forms of power.

The limits to potential Chinese hegemony also emerge in more classic geopolitical terms. Any rising, would-be hegemon wanting to establish the normative basis for a new order must recruit partners in its cause. A hegemonic transition, “is likely only when the rising state is able to form a counter-hegemonic coalition of revisionist great powers.”<sup>66</sup> Given the normative and identity constraints noted above, it is difficult to see how China could draw major powers into its hegemonic system in anything like a consent-based model. It will not be able to gather any of the world's leading developed democracies into its fold—a constraint that rules out Europe, Japan, South Korea, Australia, New Zealand, and many other countries, states which comprise (along with the United States) some three-quarters of world GDP.

Nor will Beijing be able to recruit those neighbors who see China primarily as a threat, such as

India and Vietnam. Rising democracies (again India along with Brazil, Colombia, Mexico, Indonesia, and others) hope for Chinese investment but, as noted above, their normative identity suggests that they would resist an order built on autocratic principles. Even China's partnership with Russia appears to have significant limits, as would be expected for two countries that have traditionally viewed each other with great suspicion and even hostility. In sum, there is no counter-hegemonic coalition with any real geopolitical heft available for China to assemble.

### *The Contest for the System: America's Inherent Competitive Advantages*

China's effort to win legitimate authority does meet the first condition noted above for such influence—offering material benefits. But that is all. It is not willing to commit to institutions and processes that reflect true procedural fairness in critical circumstances such as South China Sea maritime disputes or human rights. It actively undermines the procedural soundness of many international institutions in pursuit of its own unique interests. It refuses to participate in the enforcement of critical norms in areas such as nonproliferation, human rights, rule of law, and trade fairness. In sum China's approach to power does not meet many of the conditions of legitimate authority. Historically, China gained such authority through narrower avenues—material power and a claim of cultural superiority—which will not be enough for the 21<sup>st</sup> century equivalent of a “tribute system.”

The greatest risk in this systemic competition, in fact, may not originate with China at all. It originates in the decades-long rise of challenges to the legitimacy of the prevailing neoliberal model within the international order itself. The United States faces two epochal trends, not one; the rise of China, but also the emergence of an ecological, socioeconomic, and ontological crisis of the prevailing paradigm. If this latter crisis can be resolved and the U.S.-led ideational

order placed on a renewed footing, then there is really no way that China can advertise its increasingly repressive, economically slackening, internationally belligerent model as a sensible alternative.

This means that, for the United States, the current strategic competition is likely to be won in the same way that the Cold War was won, from the inside out—built on a 21<sup>st</sup> century foundation of social, environmental, and economic reforms, investments, and initiatives which revalidate the prevailing liberal-democratic approach to politics and economics, likely including steps to enhance the sharing of wealth and levels of economic justice inherent to the system. As in the Cold War, military capabilities, geoeconomic statecraft, and geopolitical maneuvering remain important as complementary tools. But together they will constitute a large holding action, with wins and losses along the way, which need never be viewed as a zero-sum contest. The United States will prevail, if it does, in more ideational and systemic terms.

The United States need have little fear that China will somehow convince leaders, elites, and populaces around the world that repressive, state-led development under Beijing's tutelage is desirable. This is not to suggest that the United States will prevail in the systemic competition without effort. Several new or expanded initiatives are clearly called for, including;

- a better-resourced, more innovative and professional set of tools for the information competition—to bring greater light to Beijing's violations of shared norms and promote the legitimacy of the American-led order;
- expanded economic aid, humanitarian assistance, and disaster relief (HA/DR) efforts in the developing world to sustain positive views of the U.S. global role;
- enhanced tools to counteract Chinese economic coercive diplomacy, including a revised BUILD Act and multilateral coordination to offer

alternatives to the investment financing in the Belt and Road Initiative;

- reforms to international institutions to provide greater voice for rising powers and exceptions to the conditionality that can push some countries in the direction of accepting Beijing's often less-conditioned aid and investment;
- renewed investments in—rather than withdrawal from—key international institutions, agreements, and processes.

These initiatives demand significant new investments as well as effective strategic coordination across the U.S. government. Maintaining decisive advantage in systemic competitions will demand real effort. Beyond such specific policy responses, however, the most significant threats to U.S. goals lie in the potential for two self-imposed mistakes. One is a failure to respond to the challenges to the prevailing socioeconomic model—climate change, inequality and stagnating wages, health and human security, and issues of cultural identity in an integrating world. This would provide China more ammunition in the ideational war and exacerbate the polarization and policy incoherence that undermines American leadership.

The United States could also lose ground through a second mistake—a fresh bout of unilateralism and self-righteous pugnaciousness. The new competition is getting underway in very different circumstances than the last: World politics is far more multipolar than in 1945, and any new global order will have to be more diverse, embracing distinct and mutually-respectful American, European, Japanese, Brazilian, Indonesian, Korean, Indian, and other varieties of social and economic models as well as approaches to specific security challenges (including China). It will be all too easy for the United States to take a panicked and rigid approach to the competition, demanding that all see it in the same irreconcilable terms, insisting

that they choose sides in ways few want to do, and in the process alienating many potential partners.<sup>67</sup>

Such a response, Richard Ned Lebow concludes, would violate historical lessons about the dangers of coercive forms of hegemony and undermine the image of legitimate American authority that “previously allowed it to translate its power into influence in efficient ways.” An America headed down this road would increasingly be forced to “use threats and bribes to get its way.” Such an outcome, if it did emerge, would, Lebow concludes, constitute “another tragic proof of arguably the most fundamental truth of politics; that friendship and persuasion create and sustain community, and community in turn enables and sustains the identities that allow rational formulation of interests. In the last resort, justice and power are mutually constitutive.”<sup>68</sup>

U.S. strategy since 1945, while guilty of many excesses, tragic errors, and occasional coercive beligerence, has reflected these insights remarkably well for a dominant great power. To ignore them now would be to surrender the greatest U.S. competitive advantage in the emerging competition with China. The United States is primed for success in the long-term competition with China for relative authority over an increasingly shared, diverse, fragmented, and multipolar international system. It merely needs to remember the practices and values that have brought it to this point and can underwrite continued influence in the future. **PRISM**

## Endnotes

<sup>1</sup> U.S. Department of Defense, “Indo-Pacific Strategy Report,” June 1, 2019, 8.

<sup>2</sup> Martin Wolf, “The Looming 100-Year U.S.-China Conflict,” *Financial Times*, June 4, 2019.

<sup>3</sup> Chris Buckley and Chris Horton, “Xi Jinping Warns Taiwan That Unification Is the Goal and Force Is an Option,” *New York Times*, January 1, 2019, at <https://www.nytimes.com/2019/01/01/world/asia/xi-jinping-taiwan-china.html>.

<sup>4</sup> For a nuanced view of the meaning of China’s current military ambitions, see M. Taylor Fravel, “China’s ‘World-Class Military’ Ambitions: Origins and Implications,” *The Washington Quarterly*, Vol. 43, No. 1 (Spring 2020), 85-99.

<sup>5</sup> Michael J. Mazarr, “Toward a New Theory of Power Projection,” *War on the Rocks*, April 15, 2020, at <https://warontherocks.com/2020/04/toward-a-new-theory-of-power-projection/>.

<sup>6</sup> On China’s developmental model as a classic example of state-led development, see Shaun Breslin, “The ‘China Model’ and the Global Crisis: From Friedrich List to a Chinese Mode of Governance?” *International Affairs*, Vol. 87, No. 6 (2011).

<sup>7</sup> See Nicholas Lardy, *Integrating China into the Global Economy* (Washington, D.C.: The Brookings Institution, 2002) and Stephen S. Roach, “America’s False Narrative on China,” Project Syndicate, April 26, 2019. For a broader assessment of China’s approach to the post-war order, see Michael J. Mazarr, Timothy R. Heath and Astrid Stuth Cevallos, *China and the International Order* (Santa Monica, CA: The RAND Corporation, 2018).

<sup>8</sup> Denny Roy, “China Won’t Achieve Regional Hegemony,” *The Washington Quarterly*, Vol. 43, No. 1 (Spring 2020), 101-117.

<sup>9</sup> The classic statement of the first face of power is Robert A. Dahl, “The Concept of Power,” *Systems Research and Behavioral Science*, Vol. 2, 1957, 201-215. See on this Steven Lukes, “Robert Dahl on Power,” *Journal of Political Power*, Vol 8, No. 2, 2015, 261-271.

<sup>10</sup> One of the most famous of these new interpretations is Steven Lukes, *Power: A Radical View* (Basingstoke: Macmillan, 2<sup>nd</sup> Edition, 2005). A classic argument about agenda setting is Bachrach, P. and Baratz, M. (1962) ‘Two Faces of Power’, *American Political Science Review*, 56: 947-52.

<sup>11</sup> Charles Tilly, quoted in Lukes, *Power*, 11. Joseph Nye’s conception of “soft power” is one of the most famous versions of more indirect forms; see Nye, *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2009), and *The Future of Power* (New York: PublicAffairs, 2011).

<sup>12</sup> Steven Lukes, “Power and the Battle for Hearts and Minds,” *Millennium*, Vol. 33, No. 3 (2005), 477-493.

<sup>13</sup> Hans Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, Brief Edition (New York: McGraw Hill, 1993), 72.

<sup>14</sup> Thinkers like Gramsci use the term “hegemony” to describe the power over thoughts that these underlying forms of power grant. For an argument connecting Gramscian hegemony to modern ideas of soft power, see Geraldo Zahran and Leonardo Ramos, “From Hegemony to Soft Power: Implications of a Conceptual Change,” in Inderjeet Parmar and Michael Cox, *Soft Power and U.S. Foreign Policy* (London: Routledge, 2010).

<sup>15</sup> Michael J. Mazarr, “Preserving the Post-War Order,” *The Washington Quarterly*, Vol. 40, No. 2 (Summer 2017).

<sup>16</sup> Stephen G. Brooks and William C. Wohlforth, “Power, Globalization, and the End of the Cold War,” *International Security*, Vol. 25, No. 3 (Winter 2000/01).

<sup>17</sup> Scholars of power such as Adam Przeworski have argued from a theoretical foundation that ideas cannot conquer populations without some connection to the peoples’ material interests; see Przeworski, *Capitalism and Social Democracy* (New York: Cambridge University Press, 2012).

<sup>18</sup> Alexander Cooley and Daniel Nexon argue, in *Exit from Hegemony: The Unraveling of the American Global Order* (New York: Oxford University Press, 2020), that a key component of the U.S. Cold War hegemonic position was that few states saw any viable alternative other than participating in the U.S.-led system. A more multilateral order, they contend, will provide more exist options for more states.

<sup>19</sup> For a comparison of this process with China’s claims to leadership, see Mark Beeson, “Can China Lead?” *Third World Quarterly*, Vol. 34, No. 2 (2013), 235-236.

<sup>20</sup> Ian Hurd, “Legitimacy and Authority in International Politics,” *International Organization*, Vol. 53, No. 2 (Spring 1999), 381. See also Ian Hurd, *After Anarchy: Legitimacy and Power in the United Nations Security Council* (Princeton, NJ: Princeton University Press, 2007), 30-34.

<sup>21</sup> Hurd, “Legitimacy and Authority in International Politics,” 400. Max Weber stresses the importance of legitimacy in any social order as a basis for respect for rules. He defined “authority” as the situation in which “power is married to legitimacy”; quoted in Hurd, *After Anarchy*, 60. See also Ian Clark, “Legitimacy in a Global Order,” *Review of International Studies*, Vol. 29 (2003), 79, and Henry A. Kissinger, *A World Restored: The Politics of Conservatism in a Revolutionary Era* (London: Victor Gollancz, 1977 [1957]).

<sup>22</sup> John Gerard Ruggie, *Constructing the World Polity: Essays on International Institutionalization* (London: Routledge, 1998), 64. See also Ruggie, “What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge,” *International Organization* 52, no. 4 (1998): 855-85.

<sup>23</sup> Hurd, *After Anarchy*, 66-73.

<sup>24</sup> Hurd, *After Anarchy*, 46.

<sup>25</sup> Ikenberry and Kupchan, “Socialization and Hegemonic Power,” 293.

<sup>26</sup> Hurd, “Legitimacy and Authority in International Politics,” 386.

<sup>27</sup> Hurd, *After Anarchy*, 42, emphasis in original; and 45. See also Hurd, “Legitimacy and Authority in International Politics,” 387-388. See also David Beetham, *The Legitimation of Power*, 2<sup>nd</sup>. Ed. (Basingstoke: Palgrave Macmillan, 2013), xi, who agrees that “To the extent that people acknowledge power as rightful ... they will feel a corresponding obligation to obey and support it without having to be bribed or coerced into doing so.”

<sup>28</sup> Clark, “Legitimacy in a Global Order,” 80, 84.

<sup>29</sup> Hurd, *After Anarchy*, 45-46.

<sup>30</sup> Charles A. Kupchan, “The Normative Foundations of Hegemony and The Coming Challenge to Pax Americana,” *Security Studies*, Vol. 23, No. 2 (2014), 221. Stacie Goddard has traced the importance of legitimation strategies in explaining the lack of balancing against Prussia in the mid-19<sup>th</sup> century; Stacie E. Goddard, “When Right Makes Might: How Prussia Overturned the European Balance of Power,” *International Security*, Vol. 33, No. 3 (Winter 2008/09).

<sup>31</sup> G. John Ikenberry and Charles A. Kupchan, “Socialization and Hegemonic Power,” *International Organization* 44, no. 3 (1990), 283.

<sup>32</sup> Richard Ned Lebow, “Power, Persuasion and Justice,” *Millennium*, Vol. 33, No. 3 (2005), 553.

<sup>33</sup> Hurd, *After Anarchy*, 63.

<sup>34</sup> Another scholar has argued that “all political power is deeply embedded in webs of social exchange and mutual constitution” must ultimately rest “on legitimacy.” Christian Reus-Smit, *American Power* (London: Polity, 2004), 64-65.

<sup>35</sup> Lebow, “Power, Persuasion and Justice,” 554-557.

<sup>36</sup> Lebow, “Power, Persuasion and Justice,” 557-565.

<sup>37</sup> Charles A. Kupchan, “The Normative Foundations of Hegemony and The Coming Challenge to Pax Americana,” *Security Studies*, Vol 23, No. 2 (2014).

<sup>38</sup> Bentley B. Allan, Srdjan Vucetic and Ted Hopf, “The Distribution of Identity and the Future of International Order: China’s Hegemonic Prospects,” *International Organization*, Vol. 72, No. 4 (2018), 843, 847.

<sup>39</sup> Allan, Vucetic and Hopf, “The Distribution of Identity and the Future of International Order,” 845.

<sup>40</sup> Allan, Vucetic and Hopf, “The Distribution of Identity and the Future of International Order,” 845.

<sup>41</sup> Lebow, “Power, Persuasion and Justice,” 579.

<sup>42</sup> See for example G. John Ikenberry, “Institutions, Strategic Restraint, and the Persistence of American Postwar Order,” *International Security* Vol. 23, no. 3 (1998): 43-78.

<sup>43</sup> See for example Michael Mandelbaum, *The Case for Goliath: How America Acts as the World’s Government in the Twenty-First Century* (New York: PublicAffairs, 2005); Stephen G. Brooks, “Can We Identify a Benevolent Hegemon?” *Cambridge Review of International Affairs*, Vol. 25, No. 1 (March 2012), 27; and Duncan Snidal, “The Limits of Hegemonic Stability Theory,” *International Organization*, Vol. 39, No. 4 (1985).

<sup>44</sup> This argument is made in Simon Bromley, *American Power and the Prospects for International Order* (Cambridge: Polity Press, 2008). This argument is discussed and endorsed by Brooks, “Can We Identify a Benevolent Hegemon?” 30-31. See also G. John Ikenberry and Charles Kupchan, “The Legitimation of Hegemonic Power,” in David P. Rapkin (ed.), *World Leadership and Hegemony* (Boulder, CO: Lynne Rienner, 1990), 49-69.

<sup>45</sup> Michael J. Mazarr and Ashley L. Rhoades, *Testing the Value of the Postwar International Order* (Santa Monica, CA: RAND Corporation, 2018).

<sup>46</sup> G. John Ikenberry and Charles A. Kupchan, “Socialization and Hegemonic Power,” *International Organization*, Vol. 44, No. 3 (Summer 1990), 285-286.

<sup>47</sup> See for example Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton, N.J.: Princeton University Press, 1984), 39; Robert Gilpin, *War and Change in World Politics* (New York: Cambridge University Press, 1981), p. 34.

<sup>48</sup> Robert W. Cox, Production, *Power and World Order* (New York: Columbia University Press, 1987), p. 172.

<sup>49</sup> Ikenberry and Kupchan, “Socialization and Hegemonic Power,” 289.

<sup>50</sup> Ikenberry and Kupchan, “Socialization and Hegemonic Power,” 289.

<sup>51</sup> Allan, Vucetic and Hopf, “The Distribution of Identity and the Future of International Order,” 848-853.

<sup>52</sup> Randall L. Schweller and Xiaoyu Pu, “After Unipolarity: China’s Visions of International Order in an Era of U.S. Decline,” *International Security*, Vol. 36, No. 1 (Summer 2011).

<sup>53</sup> The essentially negative and accusatory tone of China’s narrative is discussed in William A. Callahan, “Identity and Security in China: The Negative Soft Power of the China Dream,” *Politics*, Vol. 35, Nos. 304 (2015), 221-226.

<sup>54</sup> Allan, Vucetic and Hopf, “The Distribution of Identity and the Future of International Order,” 854.

<sup>55</sup> Four years ago, David Shambaugh summarized China’s vast and costly efforts to promote its reputation and ideas—and noted that they had largely failed. “Soft power cannot be bought,” he concluded. “It must be earned”—and the nature of China’s system produces powerful roadblocks to success. David Shambaugh, “China’s Soft-Power Push: The Search for Respect,” *Foreign Affairs*, Vol. 94, No. 4 (July-August 2015), 107.

<sup>56</sup> Joseph Nye, “What China and Russia Don’t Get About Soft Power,” *Foreign Policy*, April 29, 2013. For a review of evidence on China’s lack of success with these tools see Ian Hall and Frank Smith, “The Struggle for Soft Power in Asia: Public Diplomacy and Regional Competition,” *Asian Security*, Vol. 9, No. 1 (2013).

<sup>57</sup> Scott Kennedy, “The Myth of the Beijing Consensus,” *Journal of Contemporary China*, Vol. 19 (June 2010).

<sup>58</sup> This argument is made in Beeson, “Can China Lead?” 245-246.

<sup>59</sup> Tung Cheng-Chia and Alan H. Yang, “How China Is Remaking the UN In Its Own Image,” *The Diplomat*, April 9, 2020; Kristin Lee, “It’s Not Just the WHO: How China Is Moving on the Whole U.N.,” *Politico*, April 15, 2020.

<sup>60</sup> Sarah Cook, “Beijing’s Global Megaphone,” *Freedom House Special Report*, 2020, at <https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone>.

<sup>61</sup> Laura Silver, Kat Devlin and Christine Huang, “Attitudes toward China,” *Pew Research Center*, December 5, 2019, at <https://www.pewresearch.org/global/2019/12/05/attitudes-toward-china-2019/>.

<sup>62</sup> The ASEAN Studies Center at ISEAS-Yusof Ishak Institute, “The State of Southeast Asia 2020,” *Survey Report*, January 16, 2020, at [https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport\\_2020.pdf](https://www.iseas.edu.sg/images/pdf/TheStateofSEASurveyReport_2020.pdf).

<sup>63</sup> Allan, Vucetic and Hopf, “The Distribution of Identity and the Future of International Order,” 855-864; the quotes are from 862.

<sup>64</sup> Steven Erlanger, “Global Backlash Builds Against China Over Coronavirus,” *New York Times*, May 3, 2020, <https://www.nytimes.com/2020/05/03/world/europe/backlash-china-coronavirus.html?searchResultPosition=1>; Charles Dunst, “Beijing’s Propaganda Is Finding Few Takers,” *Foreign Policy*, April 20, 2020, at <https://foreignpolicy.com/2020/04/20/coronavirus-propaganda-china-developing-world/>; Simon Marks, “Coronavirus Ends China’s Honeymoon in Africa,” *Politico*, April 16, 2020, at <https://www.politico.com/news/2020/04/16/coronavirus-china-africa-191444>; and Michael Green and Evan S. Medeiros, “The Pandemic Won’t Make China the World’s Leader,” *Foreign Affairs*, April 15, 2020, at <https://www.foreignaffairs.com/articles/united-states/2020-04-15/pandemic-wont-make-china-worlds-leader>.

<sup>65</sup> Kathrin Hille, “Wolf warrior’ Diplomats Reveal China’s Ambitions,” *Financial Times*, May 11, 2020.

<sup>66</sup> Allan, Vucetic and Hopf, “The Distribution of Identity and the Future of International Order,” 854.

<sup>67</sup> See for example Noah Barkin, “The U.S. is Losing Europe in Its Battle with China,” *The Atlantic*, June 4, 2019.

<sup>68</sup> Lebow, “Power, Persuasion and Justice,” 581.



2019 NATO Days strengthen alliances, partnerships; Ostrava, Czech Republic, 21 September 2019, attended by over 200,000 thousand visitors. (U.S. Air Force photo by Senior Airman Alexandria Lee)



# Rediscovering a Strategic Purpose for NATO

By Peter Ricketts

Watford is at first sight an unlikely place for a gathering of world leaders. This nondescript suburb to the north of London found itself briefly in the media spotlight one chilly afternoon in December 2019. Boris Johnson had taken time out from his election campaign just before polling day to host a meeting of NATO leaders. It was intended to be a signal of allied unity in the 70<sup>th</sup> anniversary year of the 1949 Washington Treaty.

Unity was not, however, the theme uppermost in the minds of the participants as they made their way to a country house hotel for their meeting. Nor was it the focus of the accompanying media throng. The build-up to the Watford meeting had been dominated by a coruscating interview with French President Emmanuel Macron, published in the *Economist* magazine on 7 November 2019. He made the headlines with his phrase that NATO was “brain dead.” But the interview provided a searching analysis of what was wrong with the transatlantic alliance. His point of departure was the shift in American national security priorities towards confrontation with China, and the fact that President Donald Trump was the first occupant of the White House who did not support the idea of European integration. Macron saw that as reinforcing the urgency for Europe to establish what he called “military and technological sovereignty,” a new formulation of the old Gaullist ambition for European strategic autonomy.

The Macron diagnosis of NATO’s plight was that there was no longer any shared strategic objective among its members. He was still furious about a sequence of events which had played out in Western Syria in the previous weeks. President Trump had suddenly withdrawn U.S. forces who were supporting Kurdish militia in the region in their operations against the Islamic State. As soon as the U.S. forces withdrew, Turkish President Recep Tayyip Erdogan sent Turkish forces across the border to attack the very Kurdish units the U.S. had been supporting. Neither country gave any forewarning to NATO allies, even though France was still working with the Kurds and had military personnel in the area—some of whom allegedly came under fire during the Turkish advance. What, asked M. Macron, did this lack of political consultations mean for the credibility of NATO’s Article 5 collective defence guarantee? What if the Syrian regime responded with a military offensive against Turkey—would other allies be willing to go to war in support of Turkey?

---

Peter Ricketts is a retired British senior diplomat and a life peer. He sits as a crossbencher in the House of Lords.

The question was not entirely hypothetical. In February 2020, Syrian forces with Russian support mounted air strikes against the Turkish forces in Syria, killing over 30 Turkish troops. Turkey promptly demanded consultations in NATO under Article 4 of the Treaty. This gives any member state the right to call for consultations whenever they consider that their territorial integrity, political independence, or security is threatened. Ambassadors of NATO countries duly assembled, offered their condolences for the death of Turkish soldiers, condemned the Syrian air strikes and expressed solidarity with Turkey. Appearances were saved, but the bigger question remained—if Syrian forces had crossed into Turkish territory, in retaliation for a Turkish intervention conducted without consultation with NATO allies, how many of those allies would have been willing to commit troops to a war with Syria?

NATO leaders were not about to try to answer that question in Watford. They therefore played safe and decided to set up a “forward-looking reflection process” under the auspices of the Secretary General to make proposals to “further strengthen NATO’s political dimension including consultation.” In March 2020, NATO Secretary General Jens Stoltenberg announced the appointment of a 10-person group to take this forward.<sup>1</sup>

Redefining NATO’s political role is nothing new. In fact, the very first such exercise—the Three Wise Men’s report of 1956—recommended that the organisation, which had until then been almost entirely military, should develop non-military cooperation and specifically political consultations between members. The Harmel Report of 1967 marked another inflection point, proposing that the Cold War strategy of deterrence should be balanced by more emphasis on *détente*. The questions about NATO’s political role became more insistent after the end of the Cold War. The summit of Allied leaders which I helped to organise in London in June

1990 agreed to extend the hand of friendship to former Warsaw Pact adversaries, and thereby opened the door to NATO enlargement and to the offer of a cooperative relationship with Moscow through the NATO-Russia Council.

NATO adapted fast to the collapse of the Soviet Union and played a vital political role in the stabilisation of Europe. But the organisation’s strategic unity was stretched to the limit by the sequence of expeditionary military operations it led in the two decades after 1990. Twice, the European allies pleaded with President Bill Clinton to commit America’s military and diplomatic muscle to help put an end to ethnic cleansing in the Balkans, first in Bosnia and then Kosovo. These were crises of far more direct national security interest to Europeans than to the U.S. Twice, Clinton agreed to a major U.S. contribution to NATO airstrikes and then peacekeeping missions. After 9/11, the Europeans and Canadians returned the favor, invoking Article 5 of the treaty for the first and only time in solidarity with their U.S. ally. They then followed the American lead in contributing to the NATO-led Afghanistan operation. Many struggled to explain to public opinion what their forces were doing there and why—as German Foreign Minister Joschka Fischer put it—their security started at the Hindu Kush. But it was the 2003 Iraq war that broke allied solidarity. Although the damage was patched up and NATO opened an officer training academy in Baghdad in 2004, the Iraq effect turned western opinion against using ground forces to try to solve other countries’ problems. The NATO-led Libya air campaign was the curtain-call for an interventionist NATO mission in the wider world. The secondary role which President Barack Obama ordered U.S. forces to play in Libya was a vivid reminder that European security was already moving down the list of U.S. national security priorities.

That was inevitable as the American focus shifted to the Indo-Pacific region and to competition



When the rebellion against Muammar Qaddafi broke out in Lybia in March 2011, NATO launched an air campaign in support of the rebels, but avoided committing boots on the ground. (By Bernd Brincken - Own work, 19 April 2011)

with China. The then-U.S. Defence Secretary, Jim Mattis, was doing no more than confirming an established fact when he announced in presenting the U.S. National Defence Strategy in January 2018 that “great power competition, not terrorism, is now the primary focus of U.S. national security.”<sup>2</sup> It was a statement heavy with implications for America’s NATO allies. The world in which the U.S. regarded Europe and its neighbourhood as the fulcrum of global stability was over. That was the beginning of a real divergence in strategic priorities among NATO member states. The Europeans themselves were deeply divided among themselves. For countries on NATO’s Northern and Eastern flanks, the overriding national security threat was from Russia. For those looking south across the Mediterranean, migration pressures were the highest priority. For Turkey, it was the instability in Syria and the threat

from what they saw as Kurdish terrorism. For France, it was that Europe risked losing its sovereignty in a world of great power competition.

To complete that list, what is Britain’s strategic priority? That is harder to answer. It has been impossible to discern any clear direction in British foreign policy since the 2016 referendum vote pitchforked the country into four years of bitter and divisive argument about how to tear itself away from its 45-year membership of the European Union. The two pillars of its post-war national strategy—to be both a central player in Europe and the closest partner of the United States—are now both in need of a fundamental reappraisal. So far, the only answer successive British governments have produced is the empty slogan “Global Britain.” Now, an Integrated Review of Security, Defence, Development and Foreign Policy has been launched,<sup>3</sup> but, like so much

other government business, it has been delayed by the COVID-19 pandemic.

When the Review does appear, one of its conclusions should be that NATO has become more important to Britain as the main forum for political and security dialogue with its closest partners, and that Britain therefore has a strong national interest in taking a leading role in rebuilding the mutual confidence which is the bedrock of the alliance. That can only be achieved if the Europeans, Canadians, and the U.S. administration are all willing to take the necessary steps.

On the European side, two would make a real difference. First, taking on a greater share of the defence burden is a necessary, even if not a sufficient, condition for re-vitalising NATO. U.S. Presidents since Dwight Eisenhower in the 1950s have been calling for this. The Europeans (and Canadians) were far quicker than the U.S. to take the peace dividend in the years after 1989—while expecting the U.S. protective umbrella to remain in place. By 2018, U.S. defence spending amounted to 71 percent of NATO's combined defence expenditure while U.S. GDP was only 51 percent of the total of NATO countries. The goal of spending 2 percent of GDP on defence was first set at the NATO Summit in 2006. But it was only in 2014 that there was any noticeable increase in overall defence spending by non-U.S. NATO members, and this was largely in response to the Russian invasion of Ukraine that year. The NATO Secretary General confirmed in late 2019 that over the previous five years member states had spent an extra \$130 billion, with nine meeting the 2 percent target, up from five the previous year. Even Germany committed to increasing its defence spending from 1.2 percent to 1.5 percent by 2025 and increasing the size of the Bundeswehr from 176,000 to over 200,000.

The combination of a more threatening international climate, and the sharply-increased pressure from President Donald Trump from

2017—including the suggestion that he would only come to the defence of countries that were meeting the goal of spending 2 percent—was working before the pandemic pitched the world into a deep recession. The impact that this will have on the budget decisions of NATO member states remains unclear as I write. It must now be less likely that there will be further major increases for defence in the foreseeable future. But the threats from adversarial states have not diminished because of the human health crisis. Countries like Britain, which are committed to continuing to meet the 2 percent target, have a responsibility to press those which are not to sustain their announced increases in spending. And there is much that European allies can do to make their defence procurement more efficient and better targeted on filling gaps in capability.

That leads to the second step the European NATO members must take; to ensure that the concept of European strategic autonomy develops in a way that is compatible with NATO. It has always been an ambiguous, not to say slippery, term; autonomy from what precisely and for what purpose? My participation in the European debates on this issue since the 1989 Saint Malo agreement between Britain and France on European defence,<sup>4</sup> has shown me that different European countries give different answers to these questions. French governments have always operated on the assumption that one day Europe will have to take on responsibility for its own defence, and that the EU should be preparing actively for that by reducing dependence on the U.S. and by developing the capacity to undertake military action—up to major combat operations—alone. Germany has until recently had a more Atlanticist reading of autonomy, interpreting it as intended to strengthen the European role within NATO. It is true that German thinking on defence has moved since 2017 in a more European direction as a result of the estrangement between Washington and Berlin. But in my assessment the current German Government still

sees autonomy more in terms of efficient European defence industries than military separation from the U.S. The British approach has always been even further towards the pro-NATO end of the spectrum, sceptical that the EU is institutionally suited to taking on a real defence role, and in favor of European countries improving their military capability mainly as a contribution to NATO.

The combination of President Trump's open doubting of the value of NATO at the start of his term and Britain's departure from the EU has given President Macron the opportunity to push harder for the French interpretation of European strategic autonomy. But he has only found limited support from among EU member states, especially when French reasoning is pushed to the extreme of suggesting a European Army. The closer that countries are to Russia, the more they are conscious that the EU will not be in any state for many years to provide a credible deterrent. British defence academics Michael Clarke and Helen Ramscar concluded in a 2019 study;

*Even a cursory examination of European military forces reveals how completely dependent they would be on the United States in the event of any significant continental conflict—to provide some initial mass and then reinforcement, for transport, engineering, air cover, tactical command and control, intelligence—to name only the most obvious deficiencies. Nothing the European powers are pledged to improve over the next 10 years, either through NATO or rejuvenated EU defence initiatives, will create the step change necessary to alter this simple fact.... They could not defend themselves alone in a war for their own territories or for survival.<sup>5</sup>*

It would bring greater honesty and clarity to the debate about NATO's future role if the EU accepted that the goal of strategic autonomy was not

a preparation for dispensing with the U.S. as an ally. The careful balance struck in the UK-French Saint Malo agreement remains the best way of reconciling the various approaches in Europe. This document made clear that strengthening European military capabilities both contributed to "the vitality of a modernised Atlantic Alliance" and gave the EU its own option to deploy military forces where "the alliance as a whole was not engaged." EU members accepted in practice that their fledgling military capacity would be used at the lower end of the military spectrum, for example on missions like peacekeeping, training, and disaster relief. That position remains the center of gravity in the European debate. The French are outliers in maintaining their ambition of complete autonomy from the United States at some point. But the very fact of talking, as President Macron sometimes does, of a European Army may encourage some in Washington to conclude that they no longer need to invest in European security through NATO, even though the European countries are patently unprepared to counter-balance the threat from Russia alone.

In short, a NATO in which European member states and Canada bore more of the financial burden and contributed more of the military capability would be a more durable NATO, but only if the latent ambiguity in the concept of strategic autonomy can be clarified in a NATO-friendly direction.

There is work to do as well in the United States to restore confidence in the fundamental NATO bargain. A community of democracies built on a political commitment to mutual military support depends crucially on trust. That trust has been undermined by the doubts expressed by the Head of State of NATO's largest member about the value of the organisation and whether the U.S. would come to the aid of a NATO member who was not meeting the 2 percent target. The evidence that the Europeans are now taking their defence more seriously and spending more on it creates the



Despite the restrictions in place due to COVID-19, the U.S. Air Force 31<sup>st</sup> Fighter Wing remains lethal and combat ready, prepared to deter or defeat any adversary who threatens U.S. or NATO interests. (U.S. Air Force photo by Airman Thomas S. Keisler IV)

opportunity for U.S. administrations present and future to reaffirm their confidence in the value of the transatlantic alliance. They are on solid ground in doing so since NATO is better prepared militarily for its core task of territorial defence than at any time since the Cold War. The United States, Britain, and other NATO members have deployed combat-ready forces to Poland and the Baltic States. The Pentagon has spent \$2.2bn on pre-positioning warfighting equipment in Europe. Readiness has been improved. NATO has stepped up work against threats in space and cyber space. Congressional support for NATO remains strong, as evidenced by the large delegations from both Houses who decamp every year for the Munich Security Forum, the high point of the Alliance's annual round of ruminations. And American public opinion has consistently been

favorable to NATO judging from the annual survey from the Pew Research Center, even though the level of support dropped from a high of 64 percent who viewed NATO positively in 2018 to 52 percent in 2019, perhaps reflecting the tone of Presidential comments in the early part of the Administration.

The steps set out above would all help improve the climate of transatlantic relations in which the Reflection Group will be working. But the only way to restore a sense of shared strategic purpose to NATO is to re-establish honest political consultations among the allies on the issues of greatest security concern to them. It was the lack of such open consultations over the intentions of the United States and Turkey in Syria which soured the build-up to the Watford gathering, as we have seen. Given that the epicenter of global security is shifting

to Asia, and that the problems of the post-pandemic world will go far beyond the transatlantic area, it is time to broaden the scope of political consultations in NATO. Asian security issues should figure more prominently. Many European countries may not have much to offer on this issue in substance, but all would be affected by a worsening security situation in the region. All have an interest in showing that the transatlantic alliance remains relevant to core American security interests. America's allies in Asia should be invited regularly to the NATO table to take part. Australian and New Zealand forces fought bravely as part of the NATO-led operation in Afghanistan. Japan provided logistic support. All are comfortable at working as NATO partners and would enrich the dialogue on the security challenge from China. South Korea is on the front line of the most dangerous regional flashpoint and would be a natural partner as well.

Reinforced NATO consultations on these lines would also provide an excellent forum for the democracies to coordinate their approach to strategic technologies of the future. The rows over Huawei's access to the British and other 5G telecoms markets showed how dependent the West has become on China for design and manufacturing in some critical areas. Western countries need to think and plan together if they are to safeguard sovereign capabilities in key technologies of the future such as telecoms and artificial intelligence, and the advanced manufacturing processes associated with them.

The Reflection Group will now also have to consider what the pandemic means for the future of international cooperation and for NATO's political role. They might begin by recalling that NATO was never just an alliance against the Soviet Union. From the outset, it was a partnership to uphold the wider values of its member states. That is explicit in the Treaty, although these provisions are now largely forgotten. The Preamble to the Treaty makes the ringing declaration that the member states,

*... are determined to safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy, individual liberty and the rule of law. They seek to promote stability and well-being in the North Atlantic area.*

Article 2 takes NATO way beyond the parameters of a military alliance:

*The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them.*

This wider role was a vital part of NATO's purpose in the mind of the founding fathers. One of the principal negotiators of the Washington Treaty, Britain's Foreign Secretary Ernest Bevin, commented in a radio address shortly after signing the document that it was,

*An endeavour to express on paper the underlying determination to preserve our way of life—freedom of the press, freedom of religion, and the rights and liberty of the individual.<sup>6</sup>*

Part of the answer to finding a new political role for NATO in the post-pandemic world is to get back to this original sense that it is a community of democracies, not just a military alliance. The references in the Treaty to well-being, stability, and economic cooperation give plenty of scope for NATO to turn its vast experience in logistics, planning, and command and control to the new imperative of much greater resilience against disruptive threats of all kinds. The organisation

is already active in helping its member states to prevent a catastrophic cyber-attack and to deal with the consequences if one occurs. Its main contribution to resilience more generally is the Euro-Atlantic Disaster Response Coordination Centre (EADRCC). This little-known NATO body acts as a clearing-house for matching requests for assistance in emergencies with offers of support. In the first weeks of the COVID-19 crisis it organised several deliveries of equipment and supplies mainly to smaller allies and NATO partner countries. But its activities were invisible to the wider public. NATO could step up significantly its support for resilience in member states and partner countries against future disruptive events using its extensive military planning and command and control assets. That is a distinctive contribution it can make to wider international efforts to improve foresight and preparedness. It would enable NATO to take a more prominent role in future civil emergencies.

As well as being of material benefit to future work on resilience, building up NATO's contribution to human security in this way would have a positive impact on how the organisation is perceived by public opinion. The generation under the age of 40 in most Allied countries would have struggled even before the pandemic to say what NATO was for. They would not have seen any evidence since then that NATO was relevant in the greatest human health crisis in the world for a century. Nor does it have any obvious relevance to the other overriding priority for this generation—the climate emergency. If NATO is to survive, it must both find a new sense of shared purpose among member states and articulate that in a way that resonates with the generation for whom the Cold War is ancient history. It needs to get much better at communicating to public and parliamentary opinion in all member states the practical contribution a reformed NATO can make to their security and well-being. Many of the high-readiness capabilities needed to deter would-be

state adversaries are also a precious resource for governments in dealing with disruptive shocks of all kinds. That is the kind of adaptability NATO has shown over the decades. It would be consistent with the wider values set out in the overlooked parts of the Washington Treaty.

The most insidious threat to the future of NATO is not the divergence of strategic priorities between member states. Provided all subscribe to the principles of democracy, individual liberty, and the rule of law, there will be much more that unites them than divides them. It is when allied governments start to move away from these fundamental freedoms that the real problems arise. Turkey is the only member of NATO to be ranked by Freedom House in their latest “Freedom in the World” survey as “not free,” reflecting the suppression of political rights and civil liberties by President Erdoğan.<sup>7</sup> Hungary is graded only “partly free”—and that was before Prime Minister Victor Orban used the current crisis to give himself powers to rule by decree for an indefinite period. If these trends continue, NATO will face intensely difficult choices. There is no provision in the Washington Treaty for a member state to be expelled. Any such proposal would provoke a grave crisis. But the elastic of tolerance for authoritarian policies cannot be stretched indefinitely in a democratic alliance.

That is a problem well beyond the remit of the Reflection Group. It is also not a static one. Opposition parties in Turkey have already made gains against President Erdogan's AKP party in local elections. The experience of the COVID-19 pandemic may also strengthen the attractions of alliance relationships. The first reactions to the pandemic in most countries have inevitably been to accentuate national self-reliance. But rebuilding prosperity and security will demand competence from governments and greater cooperation and solidarity among nations. NATO was conceived in the aftermath of the last global cataclysm. The mutual



support it can offer its members will be just as relevant to the process of reconstruction that lies ahead. That is a message that those member states who are currently moving away from the organization's core values would do well to ponder. **PRISM**

---

## Endnotes

<sup>1</sup>NATO, "Secretary General appoints group as part of NATO reflection process", NATO press release, March 31, 2020, [https://www.nato.int/cps/en/natohq/news\\_174756.htm](https://www.nato.int/cps/en/natohq/news_174756.htm).

<sup>2</sup>Reuters, "U.S. military puts 'great power competition' at heart of strategy: Mattis", January 19, 2018, <https://www.reuters.com/article/us-usa-military-china-russia/u-s-military-puts-great-power-competition-at-heart-of-strategy-mattis-idUSKBN1F81TR>.

<sup>3</sup>United Kingdom, Prime Minister's Office, "PM outlines new review to define Britain's place in the world", press release, February 26, 2020, <https://www.gov.uk/government/news/pm-outlines-new-review-to-define-britains-place-in-the-world>.

<sup>4</sup>For an analysis of the St Malo agreement and its aftermath, see *The EU and Defence: The Legacy of St Malo* Peter Ricketts RUSI Journal Vol 162, No 3 June/July 2017.

<sup>5</sup>Michael Clarke and Helen Ramscar, *Tipping Point: Britain, Brexit and Security*, (London: I.B. Tauris, November 28, 2019), P.205.

<sup>6</sup>As quoted in *The life and times of Ernest Bevin*; (Vol. 3), *Ernest Bevin, Foreign Secretary, 1945-1951*, Alan Bullock 1983, Vol. 3 p. 671.

<sup>7</sup>See *Freedom in the World 2020* at <https://freedom-house.org/report/freedom-world>.



(Eduard Muzhevsky)

# The Evolution of Authoritarian Digital Influence

## Grappling with the New Normal

By Shanthi Kalathil

As the world contends with the wide-ranging ramifications of the global COVID-19 pandemic, it has been simultaneously beset by the global information crisis, which mimics the shape of the pandemic itself in its viral effects across huge segments of the global population.

Misinformation—unwittingly spread false information—is rampant. Overarching narratives, targeted propaganda, and particularly disinformation—the deliberate generation of false or misleading information designed to engender public cynicism or uncertainty—are being piped into the global information bloodstream in large quantities. While some of this comes from domestic political actors, determined authoritarian regimes and their proxies have been quick to seize this window of opportunity for asymmetric transnational impact. Many of those targeted, including governments, institutions, and segments of societies, have been too overwhelmed to respond effectively.

These networked, cross-border influence operations by authoritarian actors have grown in sophistication and effectiveness in recent years,<sup>1</sup> shaping narratives and targeting democratic institutions during important geopolitical moments.<sup>2</sup> While not disavowing more traditional forms of propaganda, authoritarian regimes are increasingly using digital influence operations as a method of censorship and manipulation, flooding the information space<sup>3</sup> with false or misleading narratives designed to crowd out independent voices and expertise. Their motivations may be as narrow as seeking to muddy facts around particular incidents, or as broad as endeavoring to damage institutions and social cohesion in democracies<sup>4</sup> by exploiting and amplifying social, political, and economic vulnerabilities.<sup>5</sup> There is increasing evidence that authoritarian networks are amplifying, cross-pollinating,<sup>6</sup> and learning from one another.<sup>7</sup> Key authoritarian state and state-linked actors in this space include those from the People's Republic of China (PRC), Russia, Iran, Saudi Arabia, Venezuela, and others.<sup>8</sup>

But while the current moment shows these patterns in stark relief, this is not a new dynamic. Over the past several years, such challenges emanating from the networked, global information ecosystem have moved to the heart of great power competition for the United States and other democracies around the world. While this is slowly prompting a rethink of the typical national security toolkit, democratic governments remain back-footed and hampered by lack of capacity and broader coordination. Existing structures, policy processes,

---

Shanthi Kalathil is the Senior Director of the International Forum for Democratic Studies at the National Endowment for Democracy.

and prescriptions have yet to catch up with the scale of the challenge. Meanwhile, authoritarian regimes use the current chaotic moment to fine-tune their global approaches and press their advantage. The non-governmental sector (including media and tech platforms) and the broader public represent both a soft target as well as a source of resilience—yet are not fully integrated into policy conversations and potential solutions.

In a time of growing distrust of institutions—and doubts about democracy’s capacity to deliver—authoritarian regimes are no longer content to quell democratic stirrings within their own borders. In ways subtle and overt they are actively using the global information space to take aim at the values and institutions undergirding the rules-based international order, discrediting the idea of democracy, and attempting to weaken key democratic norms. Far from merely aiming at boosting approval ratings at home and abroad, for them this is an existential question about the survival of their governance systems, and the values that should underpin the international system going forward.

This article examines recent trends and developments in authoritarian regimes’ transnational digital influence operations, particularly in light of the COVID-19 pandemic. It will address changes in the information environment that have proved fertile for such operations, the methods and goals of key players in this space, and provide insight on ways that democratic governments can update their own thinking and processes to increase resilience and capacity.

## Digital Influence Operations

A number of terms have been used to describe a range of activity in the information space; hybrid warfare, psychological warfare, active measures, fake news, disinformation, propaganda, coordinated inauthentic behavior, information/influence operations. While not interchangeable, they all describe

a range of interrelated malign activity, intended to mislead or deceive, in the global information space. For the purposes of this article, the term “digital influence operations” will be used to broadly capture the categories of digital activity most commonly employed by authoritarian regimes internationally to manipulate, censor, and degrade the integrity of the information space for strategic purposes.

While these efforts take place in the digital space and are deeply networked, they are not limited to “bots,” or automated online programs. Due to widespread bot activity during democratic elections around the world in recent years, the perception that inauthentic coordinated activity forms the entirety of such efforts can lead to poorly aimed responses. In fact, authoritarian digital influence efforts leverage all elements of the information space, including through ownership of online media outlets and tech platforms, business and advertising pressure, and traditional censorship techniques. In the case of the PRC in particular, this extends to a wide spectrum of efforts designed to influence the architecture, norms, and governance of the global information space in a direction that favors the Chinese Communist Party (CCP)<sup>9</sup> and a related restriction of free expression, distinguishing this from efforts by democratic governments.

To narrow the scope of inquiry, this essay will limit its examination to the motivations and methods of transnational authoritarian digital influence operations. It will not examine purely domestic authoritarian campaigns to crack down on home-grown dissent or manipulate information. Similarly, it will not seek to address authoritarian regimes’ cyber exploits including hacking or other intrusions, but recognizes that these elements frequently go together<sup>10</sup> with digital influence operations and complement each other. Finally, while the role of major tech platforms in facilitating disinformation is a vast and related research issue, it is beyond the ambit of this essay to thoroughly address, except to

acknowledge that without a robust response from the world's tech platforms, other efforts to combat authoritarian digital influence operations are not likely to be as effective.

## A Fertile Environment for Digital Influence Operations

Changes in the information environment have in some ways enhanced authoritarian regimes' abilities to deploy transnational digital influence operations, even as traditional aspects of democratic resilience (such as financially sustainable independent media) have degraded. Over the past decade, the global information space has been characterized by greater connectivity, speed, and (in some instances) transparency, but also hyper-volatility,<sup>11</sup> the decline of traditional and trusted intermediaries (such as local news outlets or key editorial positions), and widespread media capture.<sup>12</sup> Moreover, the explosive growth in connectivity over the past decade and a half has also coincided with a resurgence in globally assertive authoritarianism as well as backsliding on key political and civil rights in a number of countries (what some have termed the democratic recession).<sup>13</sup>

It is notable, however, that whereas in the past it was assumed that democracy would clearly benefit from a more democratized, decentralized information space with fewer gatekeepers, this has not necessarily materialized. In fact, some of democracies' traditional strengths have become weaknesses in the new environment. Commercial competition among media providers used to be thought a determinant in enhancing the quality and credibility of competition; however, in the current environment, struggling independent, for-profit media can be and are frequently competing not only against each other but also against outlets (in both the physical and digital space) that are bankrolled by free-spending, authoritarian governments, or those affiliated with them. Not only does this present an uneven playing field, but commercial pressures may

also lead outlets to relax editorial scrutiny of outside contributors, who may be concealing business interests linking them to authoritarian governments.<sup>14</sup> Disinformation outlets may also disguise themselves as independent journalism while failing to adhere to standard, best-practice accountability measures, such as bylines, mastheads, verification, corrections, and community service principles. Meanwhile, real news generation atrophies because platforms have absorbed the revenue of local independent journalism.<sup>15</sup> All of this can facilitate the success of authoritarian regimes' strategies to disrupt and subvert the information systems of targeted countries and regions.<sup>16</sup>

This has been paralleled by the rise of the "attention economy," which monetizes clicks and can drive information consumers toward particularly viral or sensational pieces of content.<sup>17</sup> Even as major technology platforms monetize attention, they maximize the data gathered from individual users, what some have called the surveillance capitalism model,<sup>18</sup> which can have strong negative implications for individual privacy<sup>19</sup> and create openings for authoritarian practices. The collection of vast amounts of data on individuals can enable precision microtargeting of messages, offering a potential goldmine for purveyors of disinformation. This combination can create a perfect storm of opportunity for authoritarian regimes and others who exploit these opportunities, including, for instance, the black market for attention (demonstrated by NATO studies of paid fake engagement on social media platforms).<sup>20</sup> As Ronald Deibert has summarized, the algorithms underlying social media also propel authoritarian practices that can facilitate manipulation, undermine accountability, and enable surveillance that can act as a proxy for authoritarian control.<sup>21</sup>

While it is not only authoritarian regimes that are able to manipulate the current information environment—far from it, as authoritarian-leaning populists from backsliding democracies

demonstrate—it is striking that studies of state actors employing such tactics highlight the prominent role played by major authoritarian regimes such as China and Russia. The Oxford Internet Institute’s (OII) recent inventory<sup>22</sup> of organized social media manipulation highlights not only authoritarian regimes’ growing capabilities to harness the information space within their own borders, but notes that around the world, there has emerged a key handful of sophisticated state actors who have been able to use computational propaganda for foreign influence operations. This handful consists of seven countries (China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela), five of which are ranked as “Not Free” (and one as “Partly Free”) by Freedom House’s comprehensive measure of civil and political rights.<sup>23</sup> OII gives special mention to the PRC as having become a major player in the global disinformation order, whose aggressive use of Facebook, Twitter, and YouTube should raise concerns for democracies.<sup>24</sup> As noted further on in this article, these techniques have expanded and explored new modalities since the onset of the COVID-19 pandemic.

It should be noted that while authoritarian regimes can frequently be the source of global digital influence operations, the viral spread of disinformation requires person-to-person transmission; that is, there must be a demand for bad or misleading information that matches the supply. Analysis of why information consumers consume the content they do, and in particular why they may seek out and share misleading content for emotional or ideological validation, is important to understanding the broader dynamics behind the spread of disinformation in the current environment.<sup>25</sup> The answer may be linked to the psychology of news consumption and opinion formation. Research shows that across geographic contexts, deeply polarized societies with low trust in the media may be more susceptible to these psychological drivers behind consumption of

misinformation or disinformation.<sup>26</sup> All of this has implications for response, as noted below.

## **Illustrative Tactics and Methods of Authoritarian Digital Influence Operations**

Individual countries have differing strategic objectives and have pioneered different tactics, but they have also sought to pull best practices from each other and amplify each other when it serves their purposes. Many authoritarian regimes have a common interest in not merely burnishing their own images internationally, but in sowing distrust in democracy and the rule of law generally. Discrediting democracy as a governance model is a goal that all authoritarian regimes share, and the cost of doing so through the tactics described here has grown radically cheaper in recent years. Moreover, for many authoritarian regimes, control of information and narrative is seen as key to regime security, and inextricably bound up in their foreign policies. The following section highlights some key countries’ digital influence tactics and operations, but is by no means meant to be exhaustive.

### *Innovations in Disinformation: Russia*

Various aspects of Russian digital influence operations across North America, Europe, and beyond are now well known, and appear to have served as a model for other authoritarians’ efforts. Many are now familiar with the Kremlin’s attempts to utilize the information space to propel disinformation, sow distrust, promote polarization, and disrupt elections, particularly in the immediate run-up to the U.S. 2016 presidential election. Yet these efforts did not start there, nor did they end there. As some have noted, Russia’s much-vaunted Internet Research Agency, run by a key Putin ally, originally was set up to manipulate domestic discourse within Russia.<sup>27</sup> Such efforts then moved outward, gradually being tested in near-abroad environments such

as Ukraine, before being deployed successfully in countries much farther afield. These activities may have been put in place well before any elections: Studies have found that Russian digital influence operations on platforms such as Twitter may have been set up and running well in advance of key election dates, speaking to foresight and planning as well as a long-term approach.<sup>28</sup>

Contrary to some perceptions, these operations do not rely solely on perpetuating overt falsehoods. Key tactics employed by Russian military intelligence (GRU) and others have included, according to a Stanford study, the updating for the digital age of such longstanding tactics as narrative laundering (legitimization of created narratives through repetition citations across media), and boosterism (repetitive content reinforcing the perception that a certain narrative represents a popular point of view). The digitization of old methods, according to the Stanford study, includes creation of online sock puppets, front websites purporting to be independent media, byline placement in politically aligned outlets, and dissemination and amplification via social networks.<sup>29</sup>

These tactics have been applied across weak and backsliding democracies, as well as more authoritarian environments, often in instances less well-known than the much publicized efforts surrounding the 2016 U.S. elections. In Turkey, for instance, censorship and manipulation already characterize the domestic information environment and render it susceptible to digital influence operations from the outside, including from Russia. Some argue that in addition to common strategies such as boosting both government and opposition narratives to foster division, pro-Russian digital influence operations in Turkey use a “forced perspective” approach that relies not on falsehoods, but on manipulating accurate information in order to remove context and distort the public narrative in favor of Russia’s objectives.<sup>30</sup> Meanwhile, emerging studies on

Russian digital influence operations across sub-Saharan Africa appear to show operations relying on private chat channels, as well as native-speaker local subcontractors, adding a wrinkle to attribution of disinformation campaigns.<sup>31</sup>

### *Growing Sophistication: Iran*

Iran’s transnational digital influence operations have only in recent years come to the attention of the broader security and international affairs community. Analysis by the Atlantic Council notes that Iranian sock puppets, operating as early as 2010, have grown exponentially in recent years, with Facebook identifying (as of early 2020) approximately 2,200 assets directly affecting six million users, and 8,000 Twitter accounts responsible for roughly 8.5 million messages. These information operations, according to the Atlantic Council, have typically contrasted with Russian tactics; rather than sowing disinformation, they have tended to exaggerate Iran’s moral authority while minimizing Iran’s repression of its citizens.<sup>32</sup> As is the case with Russia and other authoritarian regimes, the Iranian approach is informed by the government’s domestic experience with social media censorship and manipulation, particularly in the aftermath of the 2009 Green Movement protests, but with more sophisticated techniques being deployed domestically in more recent years. For instance, during the January 2018 nationwide protests, Twitter bots attempted to discredit widely shared videos of rallies, while pro-regime accounts guided protestors to the wrong locations and sought to convey that protests were small and localized.<sup>33</sup>

This growing sophistication has translated to past and ongoing transnational digital influence operations.<sup>34</sup> FireEye Threat Intelligence has identified networks of English-language social media accounts, thought to be organized in support of Iranian political interests, engaging in inauthentic behavior, with several of those and related accounts

subsequently removed by Facebook, Instagram, and Twitter in early 2020. According to FireEye, the broader network has leveraged authentic media content to promote desired political narratives that align with Iranian interests.<sup>35</sup>

### *Targeted Harassment: Saudi Arabia*

Saudi Arabia's harassment of journalist Jamal Khashoggi prior to his murder is well known, but such attacks reportedly formed just a part of a broader pattern of troll farm-generated harassment of critics, dissidents, and others. According to OII, externally focused Twitter bot networks and disinformation increased following Khashoggi's murder in October 2018, seeking to cast doubt on key Saudi officials' roles in the murder, but other activities include posting of pro-government messages, inflammation of sectarian tensions, and targeting of key rivals.<sup>36</sup> According to the *New York Times*, Saudi operatives have been particularly active on Twitter, which has been used widely for news in the country since the Arab Spring uprisings.<sup>37</sup> Analysis of a December 2019 takedown of 88,000 Twitter accounts managed by Smaat, a digital marketing company based in Saudi Arabia, showed links to "a significant state-backed information operation" that combined commercial content with attacks on critics of the Saudi regime and criticism of Qatar, Iran, and Turkey.<sup>38</sup> Among its neighbors, Saudi Arabia is hardly singular for engaging actively in digital influence operations; half of the 12 countries identified by the OII as expending considerable human and financial resources on digital influence operations were from the Middle East, including Egypt, Iran, Israel, Saudi Arabia, Syria, and the UAE.<sup>39</sup>

### *Expanding Through the Broader Information Ecosystem: China*

Until relatively recently, the Chinese Communist Party's (CCP) digital influence operations were considered relatively minimalist and ineffective, limited

to tweeting harmless and obvious propaganda through official social media channels. This itself has been a misunderstanding of the CCP's full approach, as the party's longstanding effort to influence the global information environment has been multifaceted and directed simultaneously at infrastructure, governance, norms, standards, and technological development—all in addition to projecting disinformation and shaping broader narratives through journalism training and exchanges, content linkups, and leverage over private business.<sup>40</sup> In this sense, its digital influence goals are uniquely broad and ambitious, representing an effort to reshape the structure of the internet and emerging technology.<sup>41</sup>

While this article does not dwell at length on the PRC's longstanding efforts to reshape norms, platforms, technological development, and governance through both state action and the private sector, it is important to note that such activities surround and predate<sup>42</sup> the more public digital influence tactics that have been on more recent display. Recent elections in Taiwan and the Hong Kong protests for democracy proved a key inflection point for understanding the Chinese party-state's evolving and more complex approach to digital influence operations. While the official digital footprints of Chinese state media accounts can be overt in their propaganda, *sub rosa* digital influence operations have taken aim at the legitimacy of the Hong Kong protests, at the credibility of the protestors themselves, and at the integrity and legitimacy of the Taiwan elections and individual candidates.<sup>43</sup> Analysis conducted by the Australian Strategic Policy Institute of a 2019 network targeting the Hong Kong protests that was subsequently taken down by Twitter found that while the specific information operation appeared relatively hastily put together and unsophisticated, there was evidence that the network had been repurposed from earlier accounts—demonstrating that actors linked to the Chinese government may have been running covert



digital influence operations on western social media platforms for at least two years prior.<sup>44</sup>

None of this is to say that the official digital footprint of state media is ineffective—far from it. While some point to the unsubtle regurgitation of CCP talking points, there is growing evidence that such outlets are gaining in credibility and reach. As the *Economist* points out, the English-language Facebook page of state broadcaster CGTN is followed by 77 million, the most of any news site; the PRC also runs five of the six media outlets with the biggest Facebook followings, and if current growth continues Chinese state media may attract more followers in the coming years than even the most popular sports and entertainment celebrities in the world.<sup>45</sup>

It is important to note that the PRC's digital influence operations are not limited to western-originated platforms such as Facebook and Twitter. Chinese internet companies are now among the biggest in the world, and they provide potentially powerful alternate platforms to those from Silicon Valley—often with more obscure and less rights-protecting content policies and algorithms, data privacy practices, and governance structures,<sup>46</sup> governed within a PRC system where the Party is above the rule of law. Even companies that may wish to act independently are constrained by the pressures placed on the private sector within the PRC. There is evidence that platforms originating in China are pressured to hew to CCP content guidelines—even outside of China's borders, as evidenced by censorship<sup>47</sup> and manipulation on, among others, globally popular Chinese-owned social media platform TikTok.<sup>48</sup>

Meanwhile, as WeChat grows in popularity throughout the world, politicians and others in democracies are increasingly using it for political speech,<sup>49</sup> even given widespread evidence of content censorship along CCP guidelines.<sup>50</sup> Politically motivated censorship and manipulation of content on Chinese-owned platforms is typically not

considered to be a “digital influence operation” in the classic sense, but it is likely that these less noticeable forms of content manipulation, aiming to delete topics sensitive to the CCP from the global conversation, will become even more prevalent if China's technology aims and presence continue on their current trajectory.<sup>51</sup>

## Digital Influence Operations: Supercharged by COVID

The coronavirus pandemic has provided a significant window of opportunity for heightened digital influence operations, allowing authoritarian regimes to exploit information ecosystem weaknesses to drive disinformation while mutually amplifying and reinforcing narratives related to overarching strategic goals. While authoritarian regimes are not the only ones taking advantage of confusion, panic, and misleading information during this crisis, they have been able to leverage their skill at censorship and information manipulation within their own borders to ample effect beyond them, particularly while institutions that might hold them to account are occupied elsewhere. On the other side of this “supply” of the equation, the psychological factors behind the “demand” side of the so-called “infodemic” may drive even greater disinformation virality among large segments of the population, particularly during the current crisis.<sup>52</sup>

New research from the OII on misinformation and disinformation around the coronavirus pandemic indicates a high degree of reach for authoritarian information, with content from the state-backed, English-language outlets of the PRC, Russia, Iran, and Turkey reaching audiences of millions around the world. The study found that while these outlets produce less content than more independent outlets, they can achieve ten times the amount of effective engagement—all while pushing conspiracy theories and discrediting democracy.<sup>53</sup>

Instances of prevalent disinformation, propaganda, conspiracy theory, and misleading narratives have proliferated. These have included (inter alia); that the coronavirus is a biological weapon deployed by either China, the United States, or the UK; that the virus originated in the United States or Italy rather than in China; that migrants are spreading the virus; that the virus is linked to 5G; that the entire virus is a hoax; and that the virus is linked to longstanding conspiracy theories regarding “chemtrails” and similar narratives.<sup>54</sup>

In Latin America rumors have spread that the virus was engineered to spread H.I.V., while in Iran it is portrayed as a western plot.<sup>55</sup> While it can be difficult to disaggregate organically spread misinformation from directed digital influence operations, several specific examples can be attributed to existing major entities in this space.

### *Thank you, Putin. Thank you, Russia*

Unsurprisingly, the dominant authoritarian players in digital influence operations have parlayed their existing innovation and success into more widespread manipulation of information during the global pandemic. The Kremlin, for instance, has not only continued but deepened its strategy of amplifying divisions, sowing distrust, and exacerbating crises.<sup>56</sup> According to a report by the European Union’s External Action Service, Russia’s RT Spanish is among the top-20 most engaged sources on major platforms on subjects related to the coronavirus. Moreover, the report found the Kremlin’s disinformation strategies targeting international audiences to focus primarily on conspiracy theories regarding global elites exploiting the virus, aimed at creating distrust in national and European health-care systems, institutions, and scientific experts.<sup>57</sup>

The Kremlin has used the crisis to further drive disinformation in support of strategic objectives, such as exacerbating anti-NATO sentiment among Eastern European audiences. In Lithuania,

a legitimate news site was hacked to post a false story claiming a U.S. soldier there had contracted the virus, while pro-Russian news outlets have claimed Lithuanian authorities would be shutting down pro-Russian media outlets, for instance, or that strategic food reserves had been destroyed.<sup>58</sup> Beyond Eastern Europe, the Kremlin has been active in countries hit hard by the pandemic, including Italy, where the information environment has already been dominated by domestically generated and spread misinformation and disinformation. According to the Atlantic Council’s DFR Lab, the Kremlin’s “from Russia with love” message has accompanied shipments of medical supplies and experts, with supporting narratives amplified in both Russia and Italy. Social media content has included a YouTube video titled “Russia tries to help Italy. But is someone mysteriously boycotting it,” watched by more than 25,000 people and liked over 8,000 times; meanwhile, images surrounding aid transport insinuated that EU countries were obstructing help from Russia. Such images were accompanied by hashtags #italexit and #uscITA, supporting Italy leaving the EU.<sup>59</sup> While these campaigns bear similarities to past information operations, the chaotic and saturated information environment surrounding the pandemic may help them achieve added resonance and reach.

As has been the case in the past, authoritarian-generated digital influence operations need not rely on false information to achieve effect. Russian influence operations have also amplified genuine feelings of gratitude among the Italian population for medical and scientific assistance; one video shows an Italian man replacing an EU flag with a Russian one, accompanied by a sign saying, “Thank you Putin. Thank you, Russia.”<sup>60</sup> Such narratives can be circular and cyclical. At times, disinformation narratives from Italy are also directed back into Russia. For instance, Italian-generated anti-NATO narratives surrounding the

Defender Europe 20 military exercise were circulated back into Russia just as they were beginning to fade away in Italy itself.<sup>61</sup>

### *Go China, Go Italy*

As the other dominant player in authoritarian global digital influence operations, and as the institution with perhaps the most at stake in building alternate narratives surrounding the origin of the pandemic, the CCP has engaged in concerted, global action promoting its own narratives and disinformation in the current moment. Some have marked the CCP's current effort to position itself as a responsible global leader as a new phase in China's manipulation of the global information space.<sup>62</sup> Particularly in the context of the coronavirus pandemic, elements of CCP digital influence strategy have mimicked more aggressive, Kremlin-style tactics in the service of promoting conspiracy theories, sowing distrust in institutions, and discrediting democracy.<sup>63</sup>

For instance, a March investigation published by ProPublica revealed over 10,000 fabricated Twitter accounts involved in a coordinated influence campaign, with ties to the Chinese government. Hijacked accounts were found to have pivoted from denigrating Chinese dissidents and discrediting the Hong Kong protests to posting disinformation about the coronavirus outbreak, and frequently linking several of these topics. In this operation, many posts appeared aimed at influencing ethnic Chinese outside China's borders.<sup>64</sup> Such operations sometimes build on past ones, and may overlay each other. In May 2020, Twitter took down a number of accounts linked to Chinese state actors, targeting Chinese-speaking audiences worldwide and apparently building on previous efforts to influence perceptions of the Hong Kong protests and Chinese billionaire Guo Wengui. The Australian Strategic Policy Institute found that the network had pivoted to attempt to influence perceptions on key issues including the U.S. government's response to domestic protest.<sup>65</sup>

The PRC's digital influence operations are not limited to Chinese-language efforts. According to some reports, state-run, English-language media accounts have used major platforms such as Twitter and Facebook to push narratives of western incompetence and Chinese government generosity.<sup>66</sup> As analysis by the Alliance for Securing Democracy points out, during much of March 2020, four of the top ten most-engaged articles on Facebook from China's state media outlets tracked in its proprietary dataset featured content critical of the U.S. response, while the Twitter account for China's embassy in Italy rose to become one of the ten most-engaged accounts within the organization's dataset. This account generally tweeted glowing stories about China's virus response, but Twitter accounts belonging to top Chinese officials have also spread conspiracy theories that raise doubt about the virus' origin and point to the United States as a source. These conspiracy theories, far from being spread by a single actor, were amplified by several other diplomatic accounts as well as Chinese media outlets.<sup>67</sup> Moreover, they appear to have begun circulating through unofficial accounts as early as January 2020.<sup>68</sup>

Few countries have pushed back publicly on these activities, and in fact, there are indications that behind-the-scenes pressure has resulted in some muting their response to these tactics. In April, the *New York Times* reported that European Union officials softened their criticism of China in a report documenting how governments push disinformation about the coronavirus pandemic, although EU officials denied this was the case.<sup>69</sup>

Taiwan, whose effective response to the virus has been somewhat minimized due to China's broad influence over international institutions including the WHO,<sup>70</sup> often serves as the front line for detecting disinformation from PRC entities. In early March, analysts detected a cross-platform disinformation campaign targeting Taiwan, possibly

emanating from Chinese netizens organizing of their own accord, claiming that the Taiwanese government was hiding virus cases, or that bodies of those who passed away were being hidden or burned in secret. Differences in vocabulary, tones, and characters helped distinguish messages generated in the PRC as opposed to Taiwan, even when their origin was intended to be concealed.<sup>71</sup>

In Italy, where the outbreak was early and widespread, the information environment proved a relatively hospitable target for CCP influence operations and narratives—the Five Star Movement has traditionally supported warmer relations with Beijing, while the country was the first major European country to join the Belt and Road Initiative.<sup>72</sup> Among social media praising Chinese health assistance and celebrating closer cooperation, one analysis found that nearly half of the tweets between March 11 and 23 featuring the hashtag #forzaCinaeItalia (“Go China, go Italy”) and over a third hashtagged #grazieCina (“thank you China”) were bot-originated. Misleading content was also prevalent: Bots also spread a video purporting to show Italian citizens chanting, “Thank you China” from their windows (and later debunked), a video also shared by official Chinese accounts.<sup>73</sup>

Broader PRC narratives have also pushed authoritarian governance as preferable to democracy during the crisis, and have more generally sought to weaken European cohesion and solidarity. A blog post written by the Chinese ambassador to France scolded European critics of the PRC and suggested lessons the world should learn from China’s ostensibly more effective authoritarian model.<sup>74</sup> In Europe more broadly, some analysts have raised the concern that a combination of disinformation and PRC health diplomacy, echoed by local proxies on the continent, could pave the way for wider influence in other sectors in the wake of the crisis.<sup>75</sup> More generally, the CCP’s more assertive approach to the information space may have repercussions

for citizens of autocracies as well as vulnerable and advanced industrialized democracies around the world. Far from being understood as a cautionary tale, it is possible that with enough narrative massaging, China’s initial suppression of information and clampdown on whistleblowers may provide a model for others, with implications for international cooperation on pandemic response—authoritarian leaders may be less likely to share information with other countries, permit observation from outside experts, or collaborate internationally.<sup>76</sup> Such ripple effects would have long-lasting implications for governance as well as public health.

While there is not sufficient space in this article to address the full scope of CCP aims and tactics in the broader information ecosystem, there are early signs that a greater public acceptance of health surveillance may lead to opportunities for the Chinese party-state to extend its surveillance capabilities at home and abroad. Partnerships currently being put in place, in a variety of localities around the world<sup>77</sup> may aid the collection and processing of vast amounts of data, something analysts have identified as a party-state priority.<sup>78</sup> Moreover, China’s longstanding efforts to harness elements of the information space—including platforms, influencers, and other nodes of the broader ecosystem—may pay dividends in the current environment. Statements from pop stars and other influencers praising China’s response<sup>79</sup> demonstrate that the party-state’s robust and carefully built propaganda apparatus, including documentaries, entertainment, and other elements, can be brought to bear on the current moment.<sup>80</sup>

### *Convergence and Amplification*

The heightened chaos and swirl of misinformation surrounding the COVID-19 crisis has presented wider opportunities for authoritarian regimes to exacerbate divisions as well as amplify each other when strategically advantageous. For instance, there



A charter flight carrying a 9-member Chinese aid team and 31 tons of medical supplies arrived in Rome, March 12, 2020. (People's Daily, 13 March 2020)

are indications that digital influence operations surrounding the virus have served to further heighten tensions, and provide opportunities for attacks, among Gulf adversaries.<sup>81</sup>

At the same time, the efforts of Beijing, the Kremlin, Tehran, and others can complement each other even when specific narratives diverge, as many have an interest in weakening democratic cohesion.<sup>82</sup> In spreading a particular conspiracy theory regarding the purported U.S. origin of the virus, Chinese officials have relied upon and retweeted narratives put forth by organizations, some of which have reportedly received Russian money, that already have an audience in western countries. These official account amplifications have then

found themselves echoed in the wider disinformation echo chamber that exists in the United States and across the world.<sup>83</sup>

According to analysis by the Alliance for Securing Democracy, since November 2019 three of the top five outlets most retweeted by Beijing-linked accounts were funded by the Russian or Iranian governments, while individuals associated with Russian government-funded outlets or pro-Kremlin websites were among the 100 most retweeted accounts by Chinese accounts in their proprietary dataset.<sup>84</sup> Thus, while some analysts have stressed differences in the Russian and Chinese approaches,<sup>85</sup> it is possible that the current pandemic may provide even greater opportunities

for collaboration and amplification, relying on the global disinformation echo chamber for maximum reach, than existed in the past.

Some may ask if opportunities for collaboration and amplification necessarily lead to “impact.” The question of impact is a tricky one, since it can be defined in numerous ways. Does only evidence of a real-world outcome that can be directly attributed to an influence operation count as impact? What about less quantifiable shifts in the nature and structure of the global information environment? The truth is, metrics for measuring the “impact” of digital influence operations are still evolving. Researchers can track how far certain operations spread, into which networks, and so on, using social network analysis and other methods. But we are still developing ways to understand how authoritarian digital influence operations may target and influence perceptions around specific narratives in certain countries, and specialized polling methodologies have not yet been put to this purpose.<sup>86</sup> Until more granularity in attribution emerges, one can point to correlations; for instance, in Serbia, where China has been blanketing the country with information and other types of influence operations, four out of ten Serbians think China is the biggest donor to the country (it is in fact the EU).<sup>87</sup>

## Getting to a Resilient Democratic Response

While the issues laid out here have pressing and direct ramifications for national security and great power competition, traditional security-based frameworks, processes, and “weapons” do not easily stretch to accommodate these challenges. Because these operations strike at the heart of democratic societies, societies themselves must be part of the solution—in ways that go beyond typical conceptions of national security, yet also protect key civil and political rights.

This can be challenging from a policy perspective. Issues relating to democracy, authoritarianism, and the quality of the media environment have typically been relegated to a different basket of concerns in the foreign policy context than those concerning, for instance, cyber threats. While the former is typically addressed through support for freedom of expression, key political rights, and independent media in other countries, the latter is typically considered a defense or homeland security issue. Authoritarian digital influence operations do not fall neatly into any of these categories, and at times touch multiple dimensions across foreign and domestic policy.

But addressing authoritarian digital influence operations outside the traditional national security lens is not straightforward. In the current policy discourse, this may devolve to putting the onus primarily on the technology platforms to take care of the problem. Yet tech platform action, while necessary, cannot form the sum total of the response. Certainly, the tech platforms have become more proactive in identifying and taking down coordinated inauthentic behavior stemming from state or state-linked actors: Much of the research and takedown action cited in this article stems from company action. The current coronavirus pandemic has further incentivized companies to get tougher on conspiracy theories and other forms of mis- and disinformation that may have public health ramifications.<sup>88</sup>

That said, there is widespread sentiment that technology companies must do more to prevent authoritarian digital influence operations in particular, while at the same time not focusing unduly on content-based remedies that may inadvertently chill speech and comport with authoritarian aims. The European Commission Vice President overseeing the EU’s Code of Practice on Disinformation—self-regulation under which platforms have committed to deleting fake accounts and regularly

reporting on manipulation—has urged companies to do more than they are currently.<sup>89</sup> At the same time, civil society organizations have raised concerns that making platforms more broadly liable for speech they host may have a chilling effect on expression and could contribute to a splintered global internet.

Some solutions propose bypassing the sticky issue of content moderation in favor of more seriously interrogating the business model underlying the major platforms, which—in the name of data collection and attention—may provide fertile ground for such influence campaigns. Others suggest ways to alter the design of platforms to encourage more credible content to rise to the fore. Karen Kornbluh and Ellen Goodman have suggested, for instance, user interface defaults that favor transparency, through better labeling; user-customized algorithmic recommendations and ways to track content complaints; and design solutions that introduce friction into the system (say, by limiting forwarding on messages, or encouraging users to read articles before sharing). All of this would make it harder for disinformation to thrive (and, conversely, easier for users to engage constructively). These changes, they argue, would need to be accompanied by privacy laws updated for the digital age—making it harder for all sorts of actors to gain access to individuals’ data and target them for influence operations—and national security information sharing between and with the platforms on authoritarian digital influence operations and other actions targeting democratic integrity.<sup>90</sup> These and other innovative suggestions point to a future in which tech companies can—if they wish—build resilience into the design and functioning of their platforms.

Because regulatory or other solutions to the platform issue seem overly complex and burdensome, many turn to the idea of “digital literacy” as the answer to building a resilient response to authoritarian digital influence operations. Yet, just as the

entire onus cannot be laid at the feet of the technology companies, it also cannot be the burden of the individual information consumer to simply become more literate and effective in sorting out authentic from inauthentic behavior. While the initial flurry of activity around disinformation and other digital influence operations focused on fact-checking, this is increasingly seen as just one part of a multilayered solution rather than an effective fix on its own. For one thing, sometimes—as highlighted in examples here—the information amplified in digital influence operations is actually true; it is simply being presented without context, or twisted in such a way to fit overarching narratives. Moreover, fact-checking does little against broader narratives and coordinated campaigns of inauthentic activity that are then picked up and amplified by organic networks. Even the most ambitious fact-checking campaign finds it difficult to travel as far and as fast as the original piece of information. Fact-checking also does not address the psychological drivers behind the “demand” for disinformation on the part of news consumers: If individuals are invested in a particular political narrative, they may be more likely to reject corrective information and rationalize their pre-existing beliefs.<sup>91</sup>

Not all digital literacy efforts are the same, and there have been pioneering efforts that deliberately seek to inoculate news consumers against authoritarian disinformation in particular—for instance, in Ukraine.<sup>92</sup> As these efforts are rolled out more broadly, there will need to be stronger efforts to learn relevant lessons from pilots and scale up in a way that is effective. But the learning curve on digital literacy remains steep, even as it is frequently mentioned as a kind of cure-all for a variety of ills related to mis- and disinformation.

The gatekeepers of the information ecosystem—traditional and digital media companies, editors, curators, and others—have their own role to play in mitigating the scope and scale of

authoritarian digital influence efforts. Some have recommended a blueprint for action on norm building across information-related industries, applied to both consumers and producers, with a particular focus on the labeling of authoritarian state-linked media.<sup>93</sup> Certainly, more widespread recognition of the part played by specific authoritarian media outlets in the broader authoritarian digital influence spectrum would help inoculate societies to their divisive aims, and might limit their reach. Action to clearly label outward-facing digital influence operations that utilize platforms banned at home by authoritarian countries might also help distinguish such content in a helpful way for information consumers.

Because the challenge has been so complex, democracies have been slow to devise comprehensive responses to the challenge. They have also been slow to more fully embrace as part of the solution key non-governmental aspects of resilience, including elements of the media, technology, cultural, academic, and other sectors. Yet, precisely because these challenges are cross-cutting and interdisciplinary, the response to them must be similarly multidimensional. On these issues, governments may lead, but they must also look for leadership to these institutions, that—even absent formal public-private partnerships—must take action on their own, and preferably together. Although authoritarian digital influence operations as addressed here are distinct from cybersecurity threats, this aspect of the necessary response is similar: These elements of civil society form the fabric of the “critical infrastructure” in the information space, and thus must play an active role in its protection. Moreover, these efforts would ideally go beyond voluntary piecemeal initiatives to encompass collective vision and action, on norms as well as specific measures. The ideas presented here represent an attempt to broaden the aperture for national security thinking on these ideas.

As the trends leading up to the current information crisis demonstrate, the need to address acute and persistent challenges emanating from the information space will form a distinct feature of the international security environment for the foreseeable future. It is imperative that democratic governments and civil society together lead a robust and multi-layered counter-strategy, preferably one firmly premised upon democratic values. In the meantime, authoritarian regimes will continue to press their advantage, whether democracies muster an effective response or not. **PRISM**

## Endnotes

<sup>1</sup> Christopher Paul and Miriam Matthews, *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It*. (Santa Monica: RAND Corporation, 2016). Available at <https://www.rand.org/pubs/perspectives/PE198.html>.

<sup>2</sup> Maksymilian Czuperski, John Herbst, Eliot Higgins, Frederic Hof, and Ben Nimmo, *Distract, Deceive, Destroy: Putin at War in Syria*. (Washington, DC: Atlantic Council, April 2016). Available at <https://publications.atlanticcouncil.org/distract-deceive-destroy/assets/download/ddd-report.pdf>.

<sup>3</sup> Seva Gunitsky, “The Great Online Convergence: Digital Authoritarianism Comes to Democracies,” *War on the Rocks*, Feb. 19, 2020. Available at <https://warontherocks.com/2020/02/the-great-online-convergence-digital-authoritarianism-comes-to-democracies/>.

<sup>4</sup> *Report Of The Select Committee On Intelligence, United States Senate, On Russian Active Measures: Campaigns And Interference In The 2016 U.S. Election, Volume 2: Russia’s Use Of Social Media With Additional Views*. Available at [https://www.intelligence.senate.gov/sites/default/files/documents/Report\\_Volume2.pdf](https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf).

<sup>5</sup> Dean Jackson, “Issue Brief: How Disinformation Impacts Politics and Publics,” *International Forum for Democratic Studies*, May 29, 2018. Available at <https://www.ned.org/issue-brief-how-disinformation-impacts-politics-and-publics/>.

<sup>6</sup> Javier Lesaca, “Why did Russian social media swarm the digital conversation about Catalan independence?” *The Washington Post*, Nov. 22, 2017. Available at <https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/>.



<sup>7</sup> Jessica Brandt, “Beijing’s Viral Disinformation Activities,” Power 3.0, April 2, 2020. Available at <https://www.power3point0.org/2020/04/02/beijings-viral-disinformation-activities/>.

<sup>8</sup> Samantha Bradshaw and Philip N. Howard, *The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation*. Working Paper 2019.2. Oxford, UK: Project on Computational Propaganda. Available at <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf>.

<sup>9</sup> Shanthi Kalathil, *Beyond the Great Firewall: How China Became a Global Information Power*. (Washington, DC: Center for International Media Assistance, March 2017). Available at <https://www.cima.ned.org/resource/beyond-great-firewall-china-became-global-information-power/>.

<sup>10</sup> Kim Zetter and Joseph Cox, “Here Is the Technical Report Suggesting Saudi Arabia’s Prince Hacked Jeff Bezos’ Phone,” *Vice*, Jan. 22, 2020. Available at [https://www.vice.com/en\\_us/article/v74v34/saudi-arabia-hacked-jeff-bezos-phone-technical-report](https://www.vice.com/en_us/article/v74v34/saudi-arabia-hacked-jeff-bezos-phone-technical-report).

<sup>11</sup> Shanthi Kalathil, “Transparency and Volatility: International Relations in the Information Age,” in Shanthi Kalathil, ed., *Diplomacy, Development and Security in the Information Age* (Washington, DC: Institute for the Study of Diplomacy, Georgetown University, 2011) Available at [https://cpb-us-e1.wpmucdn.com/blogs.rosevelt.edu/dist/a/14/files/2010/09/Diplomacy\\_Development\\_Security\\_in\\_the\\_Information\\_Age-1.pdf](https://cpb-us-e1.wpmucdn.com/blogs.rosevelt.edu/dist/a/14/files/2010/09/Diplomacy_Development_Security_in_the_Information_Age-1.pdf).

<sup>12</sup> Anya Schiffrin, ed., *In the Service of Power: Media Capture and the Threat to Democracy*. (Washington, DC: Center for International Media Assistance, 2017). Available at <https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/1174/cima-media-capture-book-f.pdf>.

<sup>13</sup> Christopher Walker, Alexis de Tocqueville Annual Lecture, Institute for Political Studies, Catholic University of Portugal, March 5, 2020.

<sup>14</sup> Edward Lucas, *Firming Up Democracy’s Soft Underbelly: Authoritarian Influence and Media Vulnerability* (Washington, D.C.: International Forum for Democratic Studies, February 2020). Available at <https://www.ned.org/sharp-power-democratic-resilience-series-firming-up-democracys-soft-underbelly/>.

<sup>15</sup> Karen Kornbluh, Ellen Goodman, and Eli Wiener, *Safeguarding Democracy Against Disinformation* (Washington, DC: The German Marshall Fund of the United States, 2020). Available at <http://www.gmfus.org/publications/safeguarding-democracy-against-disinformation>.

<sup>16</sup> Anne-Marie Brady, *Marketing Dictatorship: Propaganda and Thought Work in Contemporary China* (Lanham, Md: Rowman & Littlefield, 2008).

<sup>17</sup> Mark Bergen, “YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant,” Bloomberg, April 2, 2019. Available at <https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant>.

<sup>18</sup> Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. (New York: PublicAffairs, 2019).

<sup>19</sup> Nathalie Marechal and Ellery Roberts Biddle, *It’s Not Just the Content, It’s the Business Model: Democracy’s Online Speech Challenge*. (Washington, DC: Ranking Digital Rights, New America Foundation, March 2020). Available at <https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/>.

<sup>20</sup> Emma Woollacott, “Social Media Platforms Easy To Manipulate, NATO Advisers Find,” *Forbes*, Dec. 6, 2019. Available at <https://www.forbes.com/sites/emmawoollacott/2019/12/06/youtube-is-easiest-platform-to-manipulate-nato-advisers-find/#4aeba8fc3255>.

<sup>21</sup> Ronald Deibert, “The Road to Digital Unfreedom: Three Painful Truths About Social Media.” *Journal of Democracy* 30, no. 1 (2019): 25–39. Available at <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/>.

<sup>22</sup> Bradshaw and Howard, *Global Disinformation Disorder*.

<sup>23</sup> Available at <https://freedomhouse.org/explore-the-map?type=fiw&year=2020>.

<sup>24</sup> Bradshaw and Howard, *Global Disinformation Order*.

<sup>25</sup> Dean Jackson, “Issue Brief: The ‘Demand Side’ of the Disinformation Crisis,” International Forum for Democratic Studies, Aug. 2, 2018. Available at <https://www.ned.org/issue-brief-the-demand-side-of-the-disinformation-crisis/>.

<sup>26</sup> Samuel Woolley and Katie Joseff, *Demand for Deceit: How the Way We Think Drives Disinformation*. (Washington, DC: International Forum for Democratic Studies, January 2020). Available at <https://www.ned.org/wp-content/uploads/2020/01/Demand-for-Deceit.pdf>.

<sup>27</sup> Peter Pomerantsev, *This Is Not Propaganda: Adventures in the War Against Reality*. (New York: Public Affairs, 2019).

<sup>28</sup> Tim Starks, Laurens Cerulus, and Mark Scott, “Russia’s manipulation of Twitter was far vaster than believed,” *Politico*, June 5, 2019. Available at <https://www.politico.com/story/2019/06/05/study-russia-cybersecurity-twitter-1353543>.

<sup>29</sup> Renée DiResta and Shelby Grossman, *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019*. (Stanford: Internet Observatory Cyber Policy Center, 2019). Available at <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf>.

<sup>30</sup> H. Akin Unver, "Russia Has Won the Information War in Turkey," *Foreign Policy*, April 21, 2019. Available at <https://foreignpolicy.com/2019/04/21/russia-has-won-the-information-war-in-turkey-rt-sputnik-putin-erdogan-disinformation/>.

<sup>31</sup> Shelby Grossman, Daniel Bush, and Renée DiResta, *Evidence of Russia-Linked Influence Operations in Africa* (Stanford: Stanford Internet Observatory Cyber Policy Center, 2019). Available at [https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019\\_sio\\_-\\_russia\\_linked\\_influence\\_operations\\_in\\_africa.final\\_.pdf](https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf).

<sup>32</sup> Emerson T. Brooking and Suzanne Kianpour, *Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century* (Washington, D.C.: Atlantic Council, 2020). Available at <https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/>.

<sup>33</sup> Bradshaw and Howard, *Global Disinformation Order*.

<sup>34</sup> "#TrollTracker: An Iranian Messaging Laundromat," DFRLab, Aug. 29, 2018. Available at <https://medium.com/dfrlab/trolltracker-an-iranian-messaging-laundromat-218c46509193>.

<sup>35</sup> Alice Revelli and Lee Foster, "'Distinguished Impersonator' Information Operation That Previously Impersonated U.S. Politicians and Journalists on Social Media Leverages Fabricated U.S. Liberal Personas to Promote Iranian Interests," *FireEye Threat Research*, Feb. 12, 2020. Available at <https://www.fireeye.com/blog/threat-research/2020/02/information-operations-fabricated-personas-to-promote-iranian-interests.html>.

<sup>36</sup> Bradshaw and Howard, *Global Disinformation Order*.

<sup>37</sup> Katie Benner, Mark Mazzetti, Ben Hubbard and Mike Isaac, "Saudi's Image Makers: A Troll Army and a Twitter Insider," *The New York Times*, Oct. 20, 2018. Available at <https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html>.

<sup>38</sup> Renée DiResta, Shelby Grossman, K.H., and Carly Miller, *Analysis of Twitter Takedown of State-Backed Operation Attributed to Saudi Arabian Digital Marketing Firm Smaat* (Stanford: Internet Observatory Cyber Policy Center, 2019). Available at <https://cyber.fsi.stanford.edu/io/news/smaat-twitter-takedown>.

<sup>39</sup> Leena Khalil, "Inside the Middle East's epic online propaganda war," *Wired*, Sept. 29, 2019. Available at <https://wired.me/technology/privacy/inside-the-middle-east-epic-online-propaganda-war/>.

<sup>40</sup> Sarah Cook, *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence Since 2017*. (New York: Freedom House, 2020). Available at <https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone>.

<sup>41</sup> Kalathil, *Beyond the Great Firewall*.

<sup>42</sup> Danielle Cave, Samantha Hoffman, Alex Joske, Fergus Ryan and Elise Thomas, *Mapping China's Technology Giants*. Australian Strategic Policy Institute, Report No. 15, 2019. Available at <https://www.aspi.org.au/index.php/report/mapping-chinas-tech-giants>.

<sup>43</sup> Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," *Foreign Policy*, June 26, 2019. Available at <https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/>.

<sup>44</sup> Tom Uren, Elise Thomas and Jacob Wallis, *Tweeting through the Great Firewall: Preliminary analysis of PRC-linked information operations against the Hong Kong protest*. Australian Strategic Policy Institute, Report No. 25, 2019. Available at <https://www.aspi.org.au/report/tweeting-through-great-firewall>.

<sup>45</sup> "China is using Facebook to build a huge audience around the world," *The Economist*, April 20th, 2019. Available at <https://www.economist.com/graphic-detail/2019/04/20/china-is-using-facebook-to-build-a-huge-audience-around-the-world?cid=cust/ednew/n/bl/n/2019/04/17n/owned/n/n/nwl/n/n/NA/228993/n>.

<sup>46</sup> *2019 Ranking Digital Rights Corporate Accountability Index*. Available at <https://rankingdigitalrights.org/index2019/>.

<sup>47</sup> Lily Kuo, "TikTok 'makeup tutorial' goes viral with call to action on China's treatment of Uighurs," *The Guardian*, Nov. 26, 2019. Available at <https://www.theguardian.com/technology/2019/nov/27/tiktok-makeup-tutorial-conceals-call-to-action-on-chinas-treatment-of-uighurs>.

<sup>48</sup> Alex Hern, "Revealed: how TikTok censors videos that do not please Beijing," *The Guardian*, Sept. 25, 2019. Available at <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing>.

<sup>49</sup>Michael Walsh, Stephen Dziedzic, and Jason Fang, “Why are Australian politicians intensifying their presence on Chinese social media platforms?” Australian Broadcasting Corporation, April 4, 2019. Available at <https://mobile.abc.net.au/news/2019-04-04/why-are-australian-politicians-jumping-on-chinese-social-media/10966152?pfmredir=sm>.

<sup>50</sup>See, e.g., numerous articles analyzing WeChat censorship by Canada-based Citizen Lab. Available at <https://citizenlab.ca/tag/wechat/>.

<sup>51</sup>Christopher Walker, Shanthi Kalathil, and Jessica Ludwig. “The Cutting Edge of Sharp Power.” *Journal of Democracy* 31, no. 1 (2020): 124–37.

<sup>52</sup>Woolley and Joseff, *Demand for Deceit*.

<sup>53</sup>Jonathan Bright, Hubert Au, Hannah Bailey et al, “COVID-19 Series Coronavirus Coverage by State-Backed English-Language News Sources: Understanding Chinese, Iranian, Russian and Turkish Government Media,” Oxford Internet Institute, April 8, 2020. Available at <https://comprop.oii.ox.ac.uk/research/state-media-coronavirus/>.

<sup>54</sup>“EEAS Special Report: Disinformation on the coronavirus – short assessment of the information environment,” EUvsDisinfo, March 19, 2020. Available at <https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/>.

<sup>55</sup>Max Fisher, “Why Coronavirus Conspiracy Theories Flourish. And Why It Matters,” *The New York Times*, April 8, 2020. Available at <https://www.nytimes.com/2020/04/08/world/europe/coronavirus-conspiracy-theories.html#click=https://t.co/heCj4k07Sc>.

<sup>56</sup>Robin Emmott, “Russia deploying coronavirus disinformation to sow panic in West, EU document says,” Reuters, March 18, 2020. Available at <https://www.reuters.com/article/us-health-coronavirus-disinformation/russia-deploying-coronavirus-disinformation-to-sow-panic-in-west-eu-document-says-idUSKBN21518F>.

<sup>57</sup>“EEAS Special Report,” March 19, 2020.

<sup>58</sup>Patrick Tucker, “Russia Pushing Coronavirus Lies As Part of Anti-NATO Influence Ops in Europe,” Defense One, March 26, 2020. Available at <https://www.defenseone.com/technology/2020/03/russia-pushing-coronavirus-lies-part-anti-nato-influence-ops-europe/164140/>.

<sup>59</sup>“Russia exploits Italian coronavirus outbreak to expand its influence,” DFR Lab, March 30, 2020. Available at <https://medium.com/dfrlab/russia-exploits-italian-coronavirus-outbreak-to-expand-its-influence-6453090d3a98>.

<sup>60</sup>Natalia Antelava and Jacopo Iacoboni, “The influence operation behind Russia’s coronavirus aid to Italy,” Coda Story, April 2, 2020. Available at <https://www.codastory.com/disinformation/soft-power/russia-coronavirus-aid-italy/>.

<sup>61</sup>“Italian anti-NATO coronavirus narrative recycled in Russia,” DFR Lab, March 23, 2020. Available at <https://medium.com/dfrlab/italian-anti-nato-coronavirus-narrative-recycled-in-russia-46f14537c25a>.

<sup>62</sup>David Shullman, “How China is Exploiting the Pandemic to Export Authoritarianism,” War on the Rocks, March 31, 2020. Available at <https://warontherocks.com/2020/03/how-china-is-exploiting-the-pandemic-to-export-authoritarianism/>.

<sup>63</sup>Jessica Brandt and Bret Schaefer, “Five Things to Know About Beijing’s Disinformation Approach,” Alliance for Securing Democracy, March 30, 2020. Available at <https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach/>.

<sup>64</sup>Jeff Kao and Mia Shuang Li, “How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus,” ProPublica, March 26, 2020. Available at <https://www.propublica.org/article/how-china-built-a-twitter-propaganda-machine-then-let-it-loose-on-coronavirus>.

<sup>65</sup>Jake Wallis, Tom Uren, Elise Thomas et al, *Retweeting Through the Great Firewall: A Persistent and Undeterred Threat Actor*. Australian Strategic Policy Institute, Policy Brief/Report No. 33, 2020. Available at [https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall\\_1.pdf?ZzW5dlyqlOOgG5m9oHj9DWsjtXD6TCA](https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Retweeting%20through%20the%20great%20firewall_1.pdf?ZzW5dlyqlOOgG5m9oHj9DWsjtXD6TCA).

<sup>66</sup>Jane Lytvynenko “Chinese Propaganda Is Trying To Paint The Country As A Leader In Coronavirus Response,” BuzzFeed, March 30, 2020. <https://www.buzzfeednews.com/article/janelytvynenko/chinese-state-media-coronavirus>.

<sup>67</sup>Jessica Brandt, “Beijing’s Viral Disinformation Activities,” Power 3.0, April 2, 2020. Available at <https://www.power3point0.org/2020/04/02/beijings-viral-disinformation-activities/>.

<sup>68</sup>Vanessa Molter and Graham Webster, “Coronavirus Conspiracy Claims: What’s Behind a Chinese Diplomat’s COVID-19 Misdirection,” Stanford Cyber Policy Center, March 31, 2020. Available at <https://cyber.fsi.stanford.edu/news/china-covid19-origin-narrative>.

<sup>69</sup> Matt Apuzzo, “Pressured by China, E.U. Softens Report on Covid-19 Disinformation” *The New York Times*, April 24, 2020. Available at <https://www.nytimes.com/2020/04/24/world/europe/disinformation-china-eu-coronavirus.html>.

<sup>70</sup> Hal Brands, “China’s Global Influence Operation Goes Way Beyond the WHO,” *Bloomberg*, March 31, 2020. Available at <https://www.bloomberg.com/opinion/articles/2020-03-31/china-s-influence-operation-goes-beyond-who-taiwan-and-covid-19?srnd=opinion>.

<sup>71</sup> Nick Monaco, “No Rest for the Sick: Coronavirus Disinformation from Chinese Users Targets Taiwan,” *Digital Intelligence Lab*, March 5, 2020. Available at <https://medium.com/digintel/china-coronavirus-disinfo-targets-taiwan-2490d99ce6a9>.

<sup>72</sup> Mattia Ferraresi, “China Isn’t Helping Italy. It’s Waging Information Warfare,” *Foreign Policy*, March 31, 2020. Available at <https://foreignpolicy.com/2020/03/31/china-isnt-helping-italy-its-waging-information-warfare/>.

<sup>73</sup> Francesco Bechis and Gabriele Carrer, “How China Unleashed Twitter Bots To Spread COVID-19 Propaganda in Italy,” *Formiche*, March 31, 2020. Available at <https://formiche.net/2020/03/china-unleashed-twitter-bots-covid19-propaganda-italy/>.

<sup>74</sup> Available at [http://www.amb-chine.fr/fra/zfzj/t1762848.htm?utm\\_source=Disinformation+Matters&utm\\_campaign=a2dc1afaca-EMAIL\\_CAMPAIGN\\_2020\\_04\\_01\\_12\\_17&utm\\_medium=email&utm\\_term=0\\_610841f0e2-a2dc1afaca-255848637](http://www.amb-chine.fr/fra/zfzj/t1762848.htm?utm_source=Disinformation+Matters&utm_campaign=a2dc1afaca-EMAIL_CAMPAIGN_2020_04_01_12_17&utm_medium=email&utm_term=0_610841f0e2-a2dc1afaca-255848637).

<sup>75</sup> Naja Bentzen, “COVID-19 foreign influence campaigns: Europe and the global battle of narratives,” *European Parliamentary Research Service*, April 2020. Available at [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649367/EPRS\\_BRI\(2020\)649367\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649367/EPRS_BRI(2020)649367_EN.pdf).

<sup>76</sup> Shullman, “How China is Exploiting the Pandemic.”

<sup>77</sup> Morgan Meaker, “Marseille’s fight against AI surveillance,” *Coda Story*, March 26, 2020. Available at <https://www.codastory.com/authoritarian-tech/ai-surveillance-france-crime/>.

<sup>78</sup> Samantha Hoffman, *Engineering global consent: The Chinese Communist Party’s data-driven power expansion*, Australian Strategic Policy Institute, October 14, 2019. Available at <https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion>.

<sup>79</sup> Jiayun Feng, “I want no smoke with the Chinese: Cardi B wins fans in China with coronavirus rants,” *supchina*, March 26, 2020. Available at <https://supchina.com/2020/03/26/i-want-no-smoke-with-the-chinese-cardi-b-wins-fans-in-china-with-coronavirus-rants/>.

<sup>80</sup> Kalathil, *Beyond the Great Firewall*.

<sup>81</sup> Ryan Grace, “COVID-19 prompts the spread of disinformation across MENA,” *Middle East Institute*, March 20, 2020. Available at <https://www.mei.edu/publications/covid-19-prompts-spread-disinformation-across-mena>.

<sup>82</sup> Tony Romm, “Facebook disables Russian and Iranian efforts to manipulate users, raising new 2020 election fears,” *The Washington Post*, Feb. 12, 2020. Available at <https://www.washingtonpost.com/technology/2020/02/12/facebook-russia-iran-myanmar-disinformation/>.

<sup>83</sup> Julian E. Barnes, Matthew Rosenberg, and Edward Wong, “As Virus Spreads, China and Russia See Openings for Disinformation,” *The New York Times*, March 28, 2020. Available at <https://www.nytimes.com/2020/03/28/us/politics/china-russia-coronavirus-disinformation.html>.

<sup>84</sup> Brandt, “Beijing’s Viral Disinformation Activities.”

<sup>85</sup> Jean-Baptiste Jeangène Vilmer and Paul Charon, “Russia as a Hurricane, China as Climate Change: Different Ways of Information Warfare,” *War on the Rocks*, January 21, 2020. Available at <https://warontherocks.com/2020/01/russia-as-a-hurricane-china-as-climate-change-different-ways-of-information-warfare/>.

<sup>86</sup> Christopher Walker, Shanthi Kalathil and Jessica Ludwig, “Forget Hearts and Minds,” *Foreign Policy*, Sept. 14, 2018. Available at <https://foreignpolicy.com/2018/09/14/forget-hearts-and-minds-sharp-power/>.

<sup>87</sup> Mentioned in a tweet by Mikko Huotari, data attributed to RFE/RL. Available at [https://twitter.com/m\\_huotari/status/1271816348486832128](https://twitter.com/m_huotari/status/1271816348486832128).

<sup>88</sup> Leo Kelion, “Coronavirus: YouTube tightens rules after David Icke 5G interview,” *BBC*, April 7, 2020. Available at <https://www.bbc.com/news/technology-52198946>.

<sup>89</sup> Florian Eder, “Věra Jourová: Platforms ‘need to open up’ algorithms to deal with disinformation,” *Politico*, Dec. 6, 2019. Available at <https://www.politico.eu/article/vera-jourova-platforms-need-to-open-up-algorithms-to-deal-with-disinformation/>.

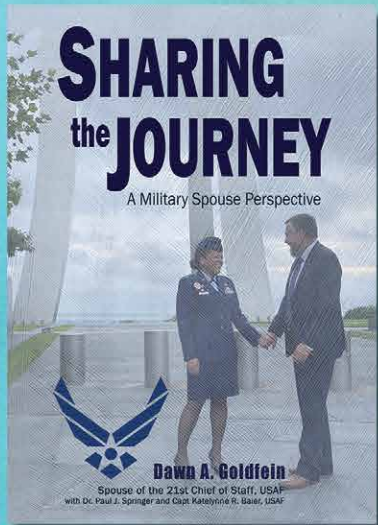
<sup>90</sup> Karen Kornbluh, Ellen Goodman, and Eli Wiener, *Safeguarding Digital Democracy: Digital Innovation and Democracy Initiative Roadmap* (Washington, D.C.: The German Marshall Fund of the U.S., March 2020). Available at <http://www.gmfus.org/publications/safeguarding-democracy-against-disinformation>.

<sup>91</sup> Woolley and Joseff, *Demand for Deceit*.

<sup>92</sup> For instance, see IREX’s “Learn to Discern” media literacy programs: <https://www.irex.org/project/learn-discern-l2d-media-literacy-training>.

<sup>93</sup> Lucas, *Firming Up the Soft Underbelly*.

# Check out the latest publications from Air University Press



## Sharing the Journey: A Military Spouse Perspective

Dawn A. Goldfein with Dr. Paul J. Springer and Capt Katelynne R. Baier

A unit's command team is the partnership among the commander, the senior noncommissioned officer (NCO), and a volunteer lead spouse. As the primary advisor, ambassador, and advocate for the spouses and families of members in the unit, finding the right person to undertake the critical role of volunteer lead spouse is one of the most important decisions a commander will make. Once a spouse in the unit decides to take on the role, it can be challenging and incredibly rewarding to navigate working with military leadership, state or local government, base programs and organizations, and other military spouses to take care of families. This book captures "words of wisdom" collected by Mrs. Dawn Goldfein, spouse of the 21st Chief of Staff of the Air Force and Gen David L. Goldfein over their 37-year career. For command teams that seek to understand and leverage the military "spouse network" of command, lead, key, and key spouse mentors within their unit or their installation, it offers a treasure trove of useful ideas and stories.

## The Secret Sauce for Organizational Success

Communications and Leadership on the Same Page

Tom Jurkowsky  
Rear Admiral, US Navy, Retired

## The Secret Sauce for Organizational Success: Communications and Leadership on the Same Page

Rear Admiral Tom Jurkowsky, US Navy, Retired

Admiral Jurkowsky's distinguished military career culminated in service as the Navy's Chief of Information, and he worked on a variety of events, from the Tailhook Scandal to various incidents at the Naval Academy. His book highlights the importance of honesty, clear messaging, and a positive relationship with the press in order to effectively manage strategic communications. The goal of *The Secret Sauce for Organizational Success* is for both communication practitioners and their leaders to learn from the author's experiences and motivate both, in tandem, so that they always do the "right thing."

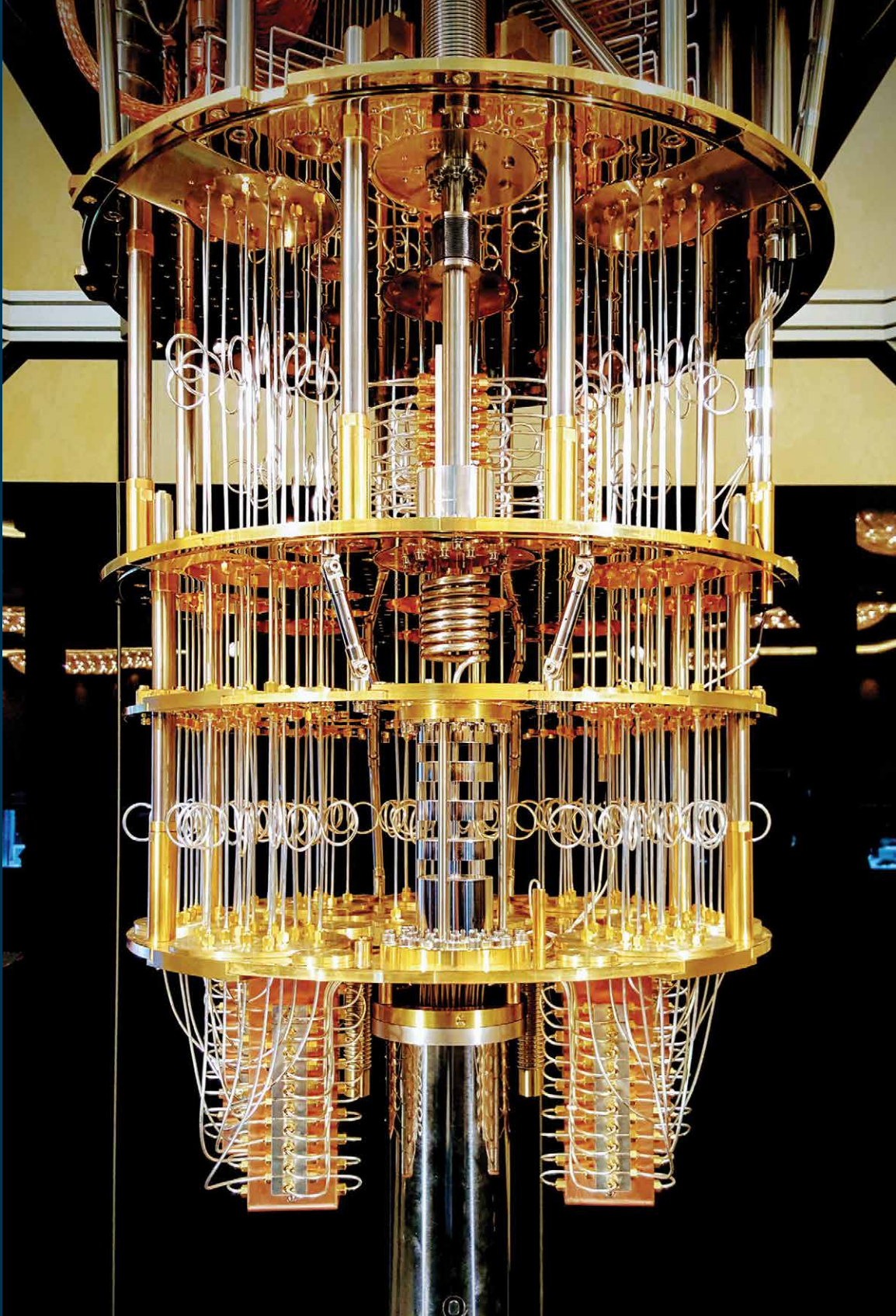


AIR UNIVERSITY PRESS

<https://www.airuniversity.af.edu/AUPress/>

<https://www.facebook.com/AirUnivPress/>

<https://twitter.com/aupress/>



IBM's Q Quantum Computer

# Quantum Computing's Cyber-Threat to National Security

By Steve Grobman

Quantum computing has the potential to bring tremendous advancements to science, including biology, chemistry, physics, and many other disciplines. The practical application will empower a stronger defense against future pandemics similar to COVID-19, not only in the acceleration of the development of vaccines and treatments, but also in optimizing currently unsolvable logistics problems such as how to deliver and route vaccines. In computer science, the “traveling salesman problem” shows it is impractical to find the optimal shortest path to visit cities once the list grows to even a few dozen. This same challenge in delivering vaccines to rural areas during a pandemic is exactly the type of problem that quantum computing will be well suited to solve.

However, like all technology, in the wrong hands, quantum computing can be a dangerous tool. In the field of cybersecurity, for example, nation-states will be able to use quantum technology to break the public cryptographic systems that secure and enable us to trust much of our digital world, including web traffic, emails, and countless uploads and downloads of everything from confidential files to software updates.

The United States has maintained a leading capability in signals intelligence and the protection of national secrets for almost a century. This position has shortened conflicts and prevented the escalation to war, saving millions of lives. Currently, publicly available information suggests there is a significant gap between the United States and our geopolitical rivals in quantum technology investment which suggests that our country could quickly find itself at a significant technological disadvantage in signals intelligence.<sup>1</sup> On the defensive side, we must move faster to re-tool the algorithms, protocols, and systems that encrypt our public and private sector data. Given that encrypted data can be captured today and decrypted at a later time, we cannot afford to think of quantum in terms of “eventually” or “tomorrow” because the threat it poses is a national security risk today.

## What History Teaches Us

Our own history tells us that nations with superior technology in signals intelligence save lives and help determine winners and losers in war and overall geopolitics. A conservative estimate shows that, without the Allies' ability to break Axis communications encrypted by the powerful Enigma encryption machine, an additional

---

Steve Grobman is Senior Vice President and Chief Technology Officer of McAfee LLC.

14 million lives would have been lost during World War II. Especially impactful to the war effort was the codebreakers' ability to help the Allies dodge U-Boats and accelerate preparations for the D-Day invasion of Europe; advantages that made the difference between life and death for millions.<sup>2</sup>

Forty years later, on September 5, 1983, President Ronald Reagan addressed the American people and played intercepted communications from the Soviet military providing evidence that the shoot-down of Korean Air 007 was intentional. Because of this, the President was able to publicly hold the Soviets accountable for their hostile action against innocent civilians.<sup>3</sup>

In our modern era, the long-term national security of the United States has relied on the ability of the U.S. military to identify attacks against U.S. citizens before they occur and hold the actors accountable. It was signals intelligence that made it possible to intercept and monitor key communications that led to locating and killing Osama Bin Laden, the mastermind of the 9/11 terrorist attacks.

What these events all have in common is U.S. leadership in signals intelligence. The advantages, the lives saved, the diplomatic coups, and the maintenance of peace and stability would not have been possible had the United States and its allies fallen behind its adversaries technologically.

What does this history teach us? The story of the Enigma codebreakers does not end with World War II. It provides a cautionary glimpse of future risks organizations and nations will face once quantum computing becomes a viable security challenge. The Allies kept their codebreaking achievement secret, meaning dozens of governments inherited the Enigma machines and continued to use them for decades believing their security to be unbreakable. British and American intelligence services were able to monitor communications from other governments throughout some of the most critical years of the Cold War. Accordingly, the revelations

about the compromised Enigma communications remained a secret, well into the 1970s, when a series of books exposed the work and accomplishments of the British WWII code breakers.<sup>4</sup>

Nations that lead in quantum computing for cryptanalysis, the science of breaking cryptography, will have a similar inherent advantage in signals intelligence in the years to come. All nations face challenges in moving to quantum resistant algorithms, including the many years it will take to transition away from the current, quantum-vulnerable implementations.

The ability to use quantum computing to decrypt data encrypted with existing implementations will enable unprecedented visibility to high valued data. Prior to quantum cryptanalysis becoming viable, data collection of encrypted, long-term, time sensitive information is still advantageous as it may be possible to decrypt it in the future when quantum cryptanalysis is practical. If the United States were to lose the quantum computing technology race with nation-state rivals such as China, our loss of signals intelligence leadership would be significant and impactful.<sup>5</sup>

Like the Allies following World War II, U.S. adversaries may not disclose critical breakthroughs in quantum viability. Rival nation-states could use their quantum supremacy to break encryption and access our country's most sensitive information for years without the United States and our allies becoming aware of the compromise.

## Quantum Versus Encryption

Quantum computing is a broad and complex capability that is not yet practical for real-world applications. The capability, when made practical, will be suited for special classes of problems and not a direct replacement for the general-purpose computing capabilities enabled by modern silicon compute architecture. Moore's Law, the guiding principle of expectations for the tech industry, theorized that



the number of transistors and other components in dense integrated circuits would double every year: In short, doubling computing power without significantly increasing cost. The theoretical paradigm shift of quantum computing has the potential to take Moore's Law to a significantly higher level, increasing computing power by a factor of about 10,000.<sup>6</sup>

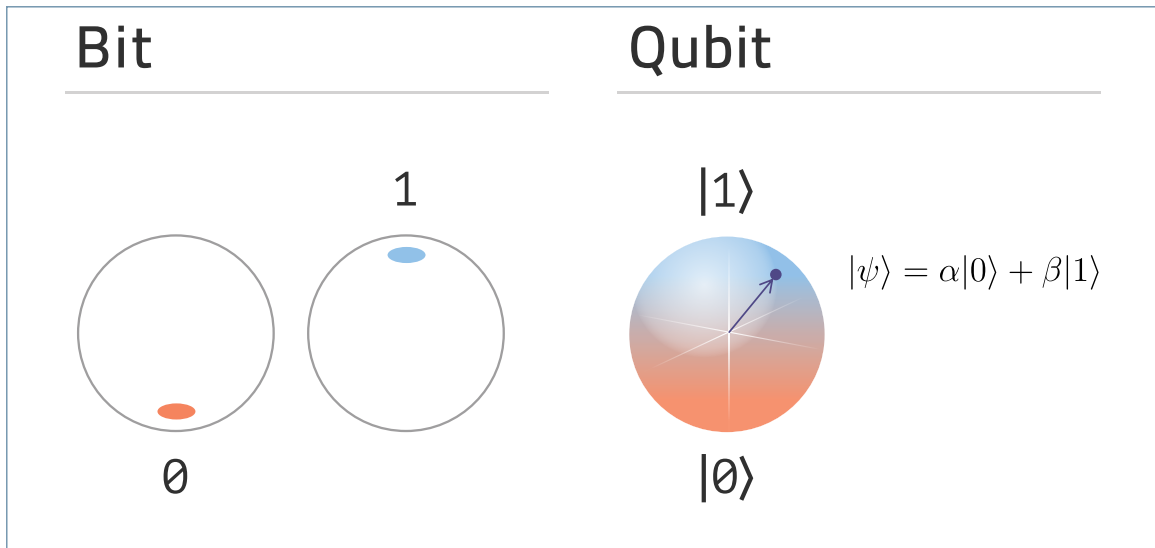
The quantum physics behind quantum computing exist in theory, but have not yet become practical, translatable electric processes for computing. The timeframe for building a large-scale quantum computer is complicated and uncertain with speculation varying widely. Many scientists believe the building of such a powerful computer is now limited to an engineering challenge, but controlling counter-intuitive physics of subatomic scales in a practical computer is not easy. Harnessing error-causing vibrations, electromagnetic waves, and temperature fluctuations are among the challenges facing engineers. Some scientists predict we will overcome these obstacles within the next 20 years, resulting in computers powerful enough to decrypt the predominant public key schemes currently in use. However, this speculative timeline is largely tied to the amount of research resources being focused on the challenge.

Today's encryption is built on a set of algorithms that work together and are implemented in the protocols, standards, and products that protect the world's data. Two main classes of algorithms exist; symmetric and asymmetric. Symmetric algorithms use the same key to both encrypt and decrypt data, while asymmetric algorithms use a key pair (one key is public and the other is private). The value of an asymmetric—also known as public key—algorithm is that anyone can encrypt data (using the public key) for a specific entity such that only they can decrypt it (with the private key). Generally, symmetric key algorithms in use today—AES-256 for example—are not vulnerable to known quantum (or traditional) attacks. The concern is largely on major

public key algorithms in use today, namely RSA and "Elliptic Curve" which are believed to be susceptible to quantum-based attacks.

The RSA encryption algorithm is the foundational encryption standard upon which most modern secure network protocols and data security systems are built. Named for its inventors—Ron Rivest, Adi Shamir, and Leonard Adleman—it bases its security on the premise that it is computationally infeasible to factor a very large number into its corresponding primes. For example, we can easily multiply the prime numbers 13 and 97 to get 1,261; but the reverse math problem is much more difficult (starting with 1,261 and finding the two underlying primes). Today's computers can both multiply the primes and find the primes for smaller numbers, but as the numbers become exceptionally large, as they do in the generation of encryption keys, the factoring challenge becomes computationally impractical. The RSA algorithm is founded on the assumption that, even with improvements in future computing capabilities, the math required to perform the factoring would take too long to make the decryption workable in practice without possessing the decryption key.

Quantum computing, however, changes the underlying assumptions about how computing works and, therefore, how quickly computers can perform math calculations. Quantum computing relies on the principles of quantum physics to solve specialized classes of mathematical problems that are not practical to solve on traditional computers. Unlike conventional digital computers that are based on transistors and encode data into binary digits (bits), these new computers would use quantum bits (qubits). Qubits can exist in multiple states simultaneously, offering the potential to compute a large number of calculations in parallel. Similar to traditional computing where the number of bits in a compute architecture determines the size and scale of possible computations, in quantum computing the number of qubits will influence the scale of



Qubit vs. bit. States of classical bit compare to quantum bit superposition. (Shutterstock/Astibuag)

mathematical problems a quantum computer can solve. The parallel nature of the qubit creates the potential to determine the underlying RSA prime numbers used to generate encryption keys that can access RSA-encrypted data. While it is possible to factor numbers using traditional computing, the size of numbers used in encryption makes it impractical.

Mathematician Peter Shor has shown that an algorithm (Shor's Algorithm) exists to identify the underlying factors of a prime number. The unique property of this algorithm is that it executes significantly faster on a quantum computer as compared to execution on a traditional computer. This approach overall is exponentially faster than the fastest known factoring capability available today on traditional computers, the general number field sieve, which works in sub-exponential time.<sup>7</sup>

Quantum computers are likely to be too large and expensive for today's cyber criminals to build and maintain directly, leaving their use to large technology companies, a few well-funded research institutions, and nation-states. While cloud computing will extend the reach of quantum to cyber criminals, the scalability and opportunity cost of

using quantum for cyber-crime will be outweighed by traditional criminal cyber activities. Certain nation-states on the other hand are well-funded and able to capitalize on the value of using quantum to advance their national security objectives.

Some tech industry luminaries question the likelihood that quantum computing will achieve the capacity to break encryption. MIT Professor Ron Rivest—the “R” in RSA—has serious doubts about whether quantum computers will become a reality at the size and scale needed to break his and other encryption algorithms. “I give fusion power a higher chance of succeeding than quantum computing,” Rivest said at the 2020 RSA Conference in San Francisco. “There is a lot of scaling that has to be done before you can break cryptography, and I am not sure it can be done.”<sup>8</sup>

Rivest has acknowledged that small quantum computers do exist, and they have demonstrated that they can factor smaller numbers. But he characterizes these computers as merely “the foothills” of much bigger things to come in quantum. Rivest is confident in his belief that while it is possible that nation-states have more substantial capabilities,

intelligence agencies are not decades ahead of the academic and other civilian quantum research and development progress.<sup>9</sup>

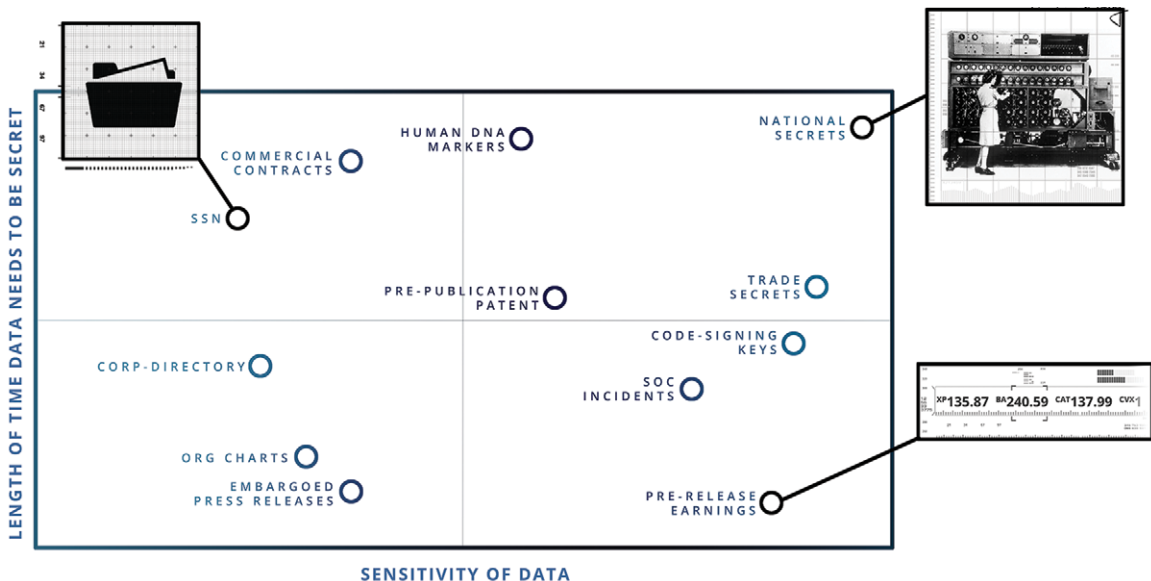
Conversely, a 2019 Global Risk Institute survey of 22 quantum computing experts agreed that the technology will definitely become a threat to encryption systems within 15 to 20 years.<sup>10</sup> Even Rivest acknowledges that while he hopes that the entities attempting to build quantum computers to break RSA will “fail,” the work to “future-proof” encryption to repel quantum-powered attacks is without a doubt essential.<sup>11</sup> Most experts agree that quantum supremacy has plausible viability in the next decade, making it critical to invest and act today, as the impact of not taking action may result in the catastrophic scenario of adversarial nations holding a monopoly on universally reading the world’s secrets.

### A Problem for Today, Not Tomorrow

There is a common assumption that we will have stronger encryption algorithms by the time quantum cryptanalysis becomes practical and that we will know when our geopolitical rivals have that capability. But we are mistaken if we assume that

the quantum risk is not a current problem simply because quantum computing is not presently viable. We should assume that nation-state adversaries are siphoning off encrypted data today that they will unlock tomorrow when quantum cryptanalysis becomes practical. While it may seem like a stretch that an adversary would decrypt data five or ten years away, consider that today, in the year 2020, documents in the national archives related to the Kennedy Assassination nearly 60 years ago still retain redactions for current national security concerns. National secrets require long degrees of durability, especially when they contain sources and methods for the collection of intelligence. While encrypted, they still retain value over time. No matter how theoretical we may believe the capability to be, we must assume that our adversaries are already accessing our most sensitive data and communications.

More than 80 percent of all network traffic is encrypted as it travels over an untrusted network, the internet. But that protection is destined to be broken. Much of our critical data is in the cloud, accessible through collaboration platforms. In assessing the quantum risk to data in an environment, consider the sensitivity of the data not only



in terms of how important it is, but also how long it must be protected. In the graphic above, we have plotted some examples of data types in terms of importance and time of protection.

Social security numbers are plotted to the left. While we clearly never want to lose a social security number, we must be realistic given that an estimated 60 to 80 percent of social security numbers have already been compromised in data breaches. At the same time, they still serve as an identifier across a lifetime, so we place them higher on the chart.

Now contrast social security numbers with pre-release earnings data for a public company. Due to their importance prior to earnings day, they are plotted far to the right, but because of the brief time between quarter-end-close and public release, we place them near the bottom. Finally, for the reasons outlined above—the sensitivity of the content and the need to keep it confidential for an extended amount of time—national security secrets are plotted at the top right.

Systems that manage data in the top-right of the graph are the systems that need to be triaged first as new quantum-resistant technologies and products become viable. This should also help drive research priorities to understand the protocols and capabilities that are protecting secrets in the top-right of the chart.

## Quantum Research and Development

Commercially viable quantum computing, comprising quantum computing chips with many thousands of qubits and requisite software, is still many years away. Progress in the field of quantum cryptography and cryptanalysis is difficult to gauge from public news reports; however, industry investment and research advancements suggest that the overall field of quantum computing is accelerating in both the private and public sectors.

In 2017, IBM unveiled a 50-qubit computer for laboratory research<sup>12</sup> and submitted a system called “Cryptographic Suite for Algebraic Lattices, or

CRYSTALS” to the National Institute of Standards and Technology (NIST) for review and approval as a quantum resistant algorithmic system. That same year, Intel announced the development of a 17-qubit superconducting test chip,<sup>13</sup> and Microsoft announced Q Sharp, a quantum computing programming language compatible with Visual Studio.<sup>14</sup> D-Wave Systems announced general commercial availability of the D-Wave 2000Q quantum computer featuring 2,000 qubits.<sup>15</sup>

In 2018, Google announced the 72-qubit quantum chip called “Bristlecone.”<sup>16</sup> Intel began testing a silicon-based spin-qubit processor and confirmed the development of a 49-qubit superconducting test chip called “Tangle Lake.”<sup>17</sup> IonQ introduced the first commercial trapped-ion quantum computer, and QuTech successfully tested a silicon-based, 2-spin-qubit processor.<sup>18</sup>

In 2019, IBM announced the IBM Q System, the company’s first commercial quantum computer featuring a 20-qubit system,<sup>19</sup> as well as its fourteenth experimental quantum computer featuring 53 qubits.<sup>20</sup> In September, it opened an IBM quantum computation center in New York and invested in Cambridge Quantum Computing, one of the first startups to become a part of IBM’s Q Network.<sup>21</sup> In August 2019, the company announced that researchers had successfully encrypted a magnetic-tape storage drive and had plans to utilize the encryption technology across its product line.<sup>22</sup>

Also in 2019, D-Wave, the world’s first commercial supplier of quantum computers announced a preview of its next-generation quantum computing platform incorporating hardware, software, and tools to accelerate and ease the delivery of quantum computing applications.<sup>23</sup> The company’s systems are used by organizations such as NEC, Volkswagen, DENSO, Lockheed Martin, USRA, USC, Los Alamos National Laboratory, and Oak Ridge National Laboratory.<sup>24</sup>

In October 2019, Google announced that researchers working with its 53 qubit system had

achieved “quantum supremacy,” which CEO Sundar Pichai described as “a quantum computer capable of solving a problem that would take a classical computer an impractically long amount of time.”<sup>25</sup> Known as Sycamore, the system was able to calculate a proof in 3 minutes and 20 seconds that showed the numbers created by a random number generator are in fact random. Theoretically, it would take Summit, one of the world’s most powerful supercomputers, some 10,000 years to complete the same problem.<sup>26</sup>

Given the potential of quantum computing and the prevalence of cloud platforms, major cloud providers are taking the threat quantum computing may pose to their substantial businesses in the space seriously. Amazon Web Services, Google, Oracle, and others are working on both post-quantum cryptography algorithms and quantum-resistant solutions to protect their cloud offerings in the coming years.<sup>27</sup>

Private sector growth is expected beyond the cloud providers. Kenneth Research estimates that the market for global quantum computing was valued at \$89.35 million in 2016 and is projected to reach \$948.82 million by 2025, projected to grow at a compound annual growth rate of 30.02 percent from 2017 to 2025.<sup>28</sup> Gartner Research predicts that 20 percent of organizations will begin budgeting for quantum computing projects by 2023, and a survey by DigiCert found that one-third of organizations report having a Post-Quantum Cryptography (PQC) budget, and 56 percent are working on establishing a PQC budget. The same survey found that nearly 40 percent of respondents said it will be “somewhat” to “extremely” difficult to upgrade encryption to protect against quantum computer attacks.<sup>29</sup>

## Nation-State Innovation Race

Beyond the corporate world, we must assume that every major nation-state power is investing in quantum technology, in part, to read protected data throughout the public and private sectors. The

United States, Germany, Russia, India, Japan, and the European Union have increased investment in quantum research and development. What is notable is that the United States and U.S.-based corporations appear to be particularly focused on hardware platforms that will power the quantum computing revolution, whereas allies such as the EU and Japan and adversaries such as China appear to be focused more on the quantum applications that will run atop these platforms when they come of age.

- In 2018, the EU committed to spending \$1.1 billion over 20 years on quantum research and development, including a special focus on building advanced quantum key distribution (QKD) into Europe’s telecommunications networks.<sup>30</sup>
- In 2019, Russia unveiled a two-qubit quantum computer prototype,<sup>31</sup> and Germany’s Fraunhofer-Gesellschaft applied research organization announced a partnership with IBM for quantum research.<sup>32</sup>
- Japan’s Ministry of Internal Affairs and Communications submitted plans to spend \$14 billion to implement post-quantum cryptography across its own IT landscape by 2025.<sup>33</sup>
- India’s 2020 budget includes a five-year \$1.12 billion allocation to the government’s National Mission on Quantum Technologies and Applications.<sup>34</sup>
- The U.S government’s Defense Advanced Research Projects Agency (DARPA) set up the first quantum communications network in 2003 and in subsequent years has seen increased investment.<sup>35</sup>
- In 2018, the White House issued a National Strategic Overview for Quantum Information Science and launched the National Quantum Coordination Office to coordinate quantum research and development across 14 U.S. government agencies.<sup>36</sup>

- In December 2019, the Trump Administration and Congress worked together to pass into law the National Quantum Initiative Act, which commits \$1.2 billion to quantum focused efforts over five years.<sup>37</sup> This legislation also seeks to establish goals and priorities for a 10-year plan to establish the United States firmly in the world's leadership position in quantum computing. This includes the creation of a cross-government ecosystem, including:
  - National Quantum Information Science Research Centers within the Department of Energy.
  - Research and education centers in the National Science Foundation.
  - A “workshop of stakeholders” administered by NIST “to discuss the future measurement, standards, cybersecurity, and other appropriate needs for supporting the development of a robust quantum information science and technology industry in the United States.”
  - A Subcommittee on Quantum Information Science under the National Science and Technology Council.
  - A National Quantum Initiative Advisory Committee to advise the president.<sup>38</sup>

The Obama Administration invested around \$200 million per year on quantum research in a variety of areas during its eight years. The 2019 Trump Administration budget for Quantum Information Science raised annual spending to \$430 million, a number that is expected to more than double by 2022.<sup>39</sup>

The Administration's fiscal year 2021 budget provides nearly half a billion dollars for quantum technology, including \$25 million to construct a quantum internet that connects 17 national labs. Additionally, the budget allocated \$718 million for NIST to drive “industry of the future” technologies

such as quantum computing, artificial intelligence, 5G advanced communications, biotechnology, and advanced manufacturing. The budget invests over \$14 billion in Department of Defense science and technology programs, but while quantum is included in this group of strategic emerging technologies, the exact allocation for quantum investment is not specified. That said, the budget is clear in that the Office of Science will receive \$5.8 billion for early stage research, national laboratories, and construction projects, and \$237 million of this investment is specifically committed to quantum information science research.<sup>40</sup>

## The China Challenge

Geopolitical and technology thought leaders agree that the People's Republic of China (PRC) poses the greatest technological challenge to U.S. leadership in quantum computing. The Chinese government is quite public about its long-term national goal to become the global leader in critical emerging technologies, particularly those with military and commercial applications.

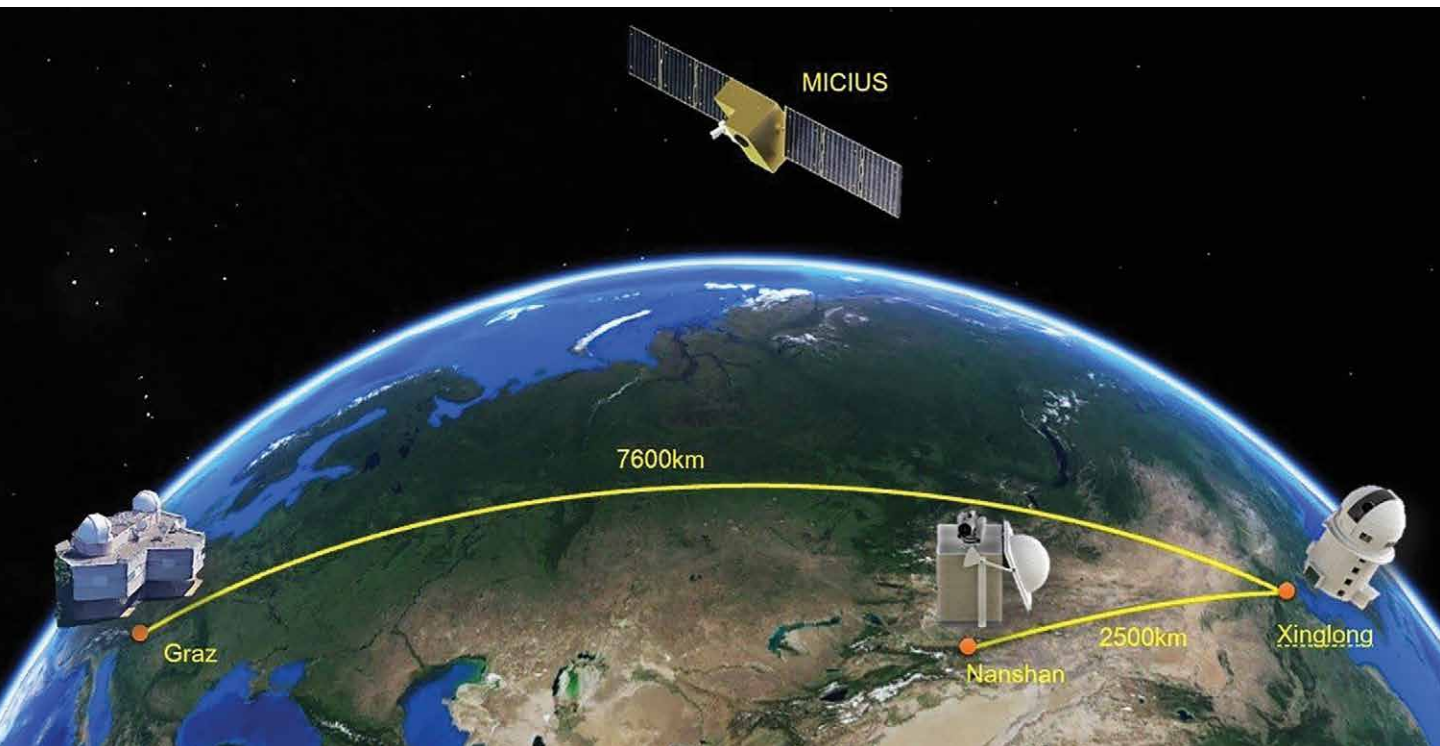
From a strategic perspective, China seeks to never again be subject to western or other foreign powers due to economic and technological inferiority. China's “century of humiliation,” the period of European and Japanese imperialism between 1839 and 1949, is just yesterday for a 4,000-year old culture with a long memory. Historians note that China was victimized by industrialized foreign powers with technologically superior militaries from the 1842 Treaty of Nanjing at the end of the First Opium War with Great Britain to the end of the Second Sino-Japanese War in 1945. The Chinese government's very public initiatives like Made in China 2025 are part of a grander national strategy to create a reality in which the country will never again be at the mercy of foreign powers.<sup>41</sup>

To this end, China has included quantum informatics as a featured component within the PRC's

13th Five-Year Plan and the Made in China 2025 plan.<sup>42</sup> In November 2015, at the 5th Plenum of the 18th Party Congress, Chinese Premier Xi Jinping specifically called out quantum communications as a critical strategic technology project that must be prioritized and achieve major breakthroughs by 2030. Xi has continued, in subsequent years, to emphasize the importance of advancing indigenous innovation in quantum communications and other critical cyber and information technologies.<sup>43</sup>

Hartmut Neven, engineering director for Google's AI Quantum team, notes that China, as a society today, is capable of steering tremendous resources to gain the world's leadership position in quantum as well as other emerging technology fields,<sup>44</sup> and recent history suggests China is willing and able to invest in emerging technologies in a big way. The total quantum budget for

China, including covert intelligence agency and military research and development budgets is not public. However, various public Chinese government investments and policy initiatives at multiple government levels and across sectors have shown a steady increase in quantum research. This leads observers to estimate that China's total spend may be in excess of \$2.5 billion per year since 2017, a sum observers point out that makes investments from the United States and other countries pale by comparison.<sup>45</sup> From 1998 to 2018, China's central and provincial governments invested an estimated \$987 million into research on quantum communication, quantum computation, and quantum metrology.<sup>46</sup> From 1998 to 2006, the National Natural Science Foundation of China (NSFC), the Chinese Academy of Science (CAS) Institute of Physics, the University of Science and Technology



Mozi, or Micius, named after the famous 5th century BCE Chinese scientist, is the first quantum communications satellite launched by China on August 16th, 2016; Illustration of the three cooperating ground stations (Graz, Nanshan, and Xinglong). (University of Science and Technology of China)

of China (USTC), the Shanxi University, and other universities received around \$10 million to pursue a variety of early stage projects.

From 2006 to 2010, China's 11<sup>th</sup> Five-Year Plan allocated an estimated \$150 million to quantum research. The Ministry of Science and Technology (MOST) and CAS launched the "Long Distance Quantum Communication" and "Key Technology Research and Verification of Quantum Experiments at Space Scale" projects to support large-scale quantum communication research. From 2011 to 2015, the nation's 12<sup>th</sup> Five-Year Plan boosted quantum research and development funding to \$490 million in areas such as quantum control (MOST), scientific research instruments and equipment development (NSFC), quantum experiments at space scale (CAS), coherent control of quantum systems and metrology physics in atomic systems (CAS), and continued work on building quantum secure communications (NDRC and CAS).

Notably the National Development and Reform Commission (NDRC), Anhui Province, Shandong Province, and CAS launched the Beijing-Shanghai Quantum Secure Communication Backbone project to accelerate industrial applications of quantum key distribution (QKD), a critical area for ensuring secure government and private sector communications.

Between 2016 and 2019, China's quantum research funding reached around \$337 million under the nation's 13<sup>th</sup> Five-Year Plan. Notable projects launched in this period include the Quantum Control and Quantum Information National Key Research and Development Project.<sup>47</sup>

As a result of these efforts, Chinese researchers have achieved some notable milestones, such as the first quantum science satellite,<sup>48</sup> a quantum resistant encrypted network connecting Beijing and Shanghai, and related developments in QKD.

Observers note that while China seeks to dominate all areas of quantum computing, its most notable accomplishments in the field to date are

focused on quantum communications rather than overall quantum computing research and development that would touch a variety of technology fields.<sup>49</sup> Patent consulting firm Patinformatics assesses which organizations are accumulating patents in critical emerging technology fields. According to the firm's 2018 report on quantum patents, Chinese organizations dominate patents on quantum applications, with nearly twice as many publications as the United States in 2017, with the applications very focused on cryptology. Since 2012, approximately 72 percent of the academic patent families published in quantum information technology are from Chinese universities, with the United States coming in a distant second place with a mere 12 percent.

The University of Science and Technology of China, the Chinese Academy of Sciences, and Beijing University have established significant portfolios associated with the hardware aspects of quantum applications that could enable China to dominate quantum cryptology and communication. Patinformatics asserts that the leading quantum computer manufacturers tend to be based in North America while the greatest accomplishments by Chinese and other Asian entities are focusing on quantum cryptology and communication.<sup>50</sup> "North American organizations may control the (quantum) computer," the report observed. "But Asian organizations may end up controlling how those machines are used."<sup>51</sup>

The annual Five-Year Plan investments might not capture the full picture of China's "all of nation" commitment to quantum research and development. The central government and regional governments are teaming to build the National Laboratory of Quantum Information Sciences in the capital of eastern Anhui province. The governments boast that the research facility will be the largest of its kind in the world, and even assert that its research will produce quantum



technologies “of immediate use” to the country’s military.<sup>52</sup> The new institution has received an initial \$1.06 billion in funding and the governments involved plan to invest an additional \$14.76 billion over the next five years.<sup>53</sup>

Other regionally funded research is taking place through the Anhui Quantum Science Industry Development Fund, Shandong Province Quantum Technology Innovation and Development Program, and an emerging quantum ecosystem in Jinan Hi-tech Zone’s “Quantum Valley”.

China’s private sector is also playing a role with internet giant Alibaba, planning to invest \$15 billion in technologies such as artificial intelligence and quantum technologies, complementary to the government’s own work.<sup>54</sup>

In addition to funding research, the PRC has also worked, through its Thousand Talents Plan, to recruit talented quantum technologists by providing incentives. As of 2018, the program had incentivized the return of around 7,000 quantum computing specialists studying or working abroad, including Pan Jianwei, known as the nation’s “father of quantum.”<sup>55</sup> Pan pursued his doctorate at the University of Vienna and conducted research at the University of Heidelberg before rallying several Chinese colleagues back to China to drive quantum research and development for his home government.<sup>56</sup>

China’s drive to lead the world in dominating the most pivotal 21<sup>st</sup> century technologies is currently unmatched by the United States. Washington is simply not investing in these technologies at the level the country invested during the Cold War to dominate the most pivotal technologies of the last century. During the Cold War, the United States invested in advanced technologies because it realized that it could not afford to lose the technology race to a hostile power like the Soviet Union. Losing that race in the most critical technologies that defined the last century and

remain critical to this day represented nothing less than an existential threat to the nation. Today, China’s “all of nation” investments in technologies such as quantum show that their leadership recognizes that the nation-state that dominates these technologies will have significant power in the 21<sup>st</sup> century in much the same way the United States dominated the last 70 years of geopolitics.

## Developing Quantum-Resistant Algorithms

The U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) is leading a selection and standardization effort for proposed quantum-resistant algorithms from academic and governing bodies around the world.<sup>57</sup> The goal of post-quantum cryptography research is the development of cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks. Of the 69 initial quantum-resistant algorithms proposed to NIST, 12 were broken or attacked within three weeks and, after three years of evaluation, NIST has managed to narrow the field of candidates to 26.

While NIST’s work in this area is promising, it must move faster and should receive greater investment by government and industry. Cooperation from across both groups is essential to developing and understanding quantum-resistant algorithms. Lack of funding for development of quantum-resistant algorithms is also part of the problem. NIST’s quantum research budget is \$30 million, just 0.0006 percent of the U.S. federal budget; too little to solve a problem that is such a serious threat to national security.

## Beyond the Math

Organizations, both public and private, must commit to starting the technical work on elements beyond just the new mathematical algorithms that will power

post-quantum cryptography. We must begin to inventory, understand, and retool the protocols and systems that will be vulnerable to quantum attacks.

### *Planning the Rollout*

Retooling our network and data protection solutions will take time; not only to develop the technology, but to roll it out throughout the world's compute and network deployments. Once replacement algorithms are complete, the implementation of related network protocols, key management, and other supporting technologies will take time, as will the integration of the algorithms into commercial products. To hasten this, organizations should commit to building post-quantum action plans that measure time and impact sensitivity so that they are ready to rapidly retool the systems protecting their data as the post-quantum ecosystem is ratified. Organizations can start prioritizing data that needs protection today, including what data is accessed or stored by vulnerable paradigms.

### *TLS 1.3.*

Additionally, organizations and technology industry partners can move their network traffic to Transport Layer Security (TLS) version 1.3, the latest generation of technology that secures computer-to-computer communications. TLS 1.3 removes RSA encryption key negotiation options and requires Diffie-Helman encryption. The main driver for this is to prevent the loss of a private RSA key which would result in the ability to decrypt all sessions based on it. The side benefit is that every session has unique Diffie-Helman key exchanges. While Diffie-Helman is not quantum safe, the move would require an adversary to break a specific session using quantum cryptanalysis on that session as compared to breaking the RSA key on the publicly available certificate. This requires adversaries to possess significantly higher compute scalability as well as the encrypted stream prior

to beginning cryptanalysis. While this mitigation does not remove the need to aggressively move to a post-quantum ecosystem, it does provide a tangible action organizations can take today.

### *More Post-Quantum Standards*

Technologists should also work to develop additional standards, protocols, and products for a post-quantum ecosystem, such as working with the Internet Engineering Task Force to support a post-quantum TLS or code-signing standards. Furthermore, once these standards come to fruition, platforms need to be plug-and-play to facilitate rapid adoption.

## **A Race We Can't Afford to Lose**

The United States and its allies are in a technology race with China and other geopolitical rivals, and quantum computing is an important front of that competition—a competition we cannot afford to lose. While quantum computing still has many challenges ahead, including the time to achieve true viability, the actions we take today will have profound impact on whether we are protected when that day comes.

There is a reasonable chance that nation-states will have this computing power in the foreseeable future. It is naïve to assume that the rest of the world will immediately become aware of the viability of pragmatic implementations of quantum cryptanalysis and take action to narrow the technology gap between nation-states.

We should be realistic and understand that the largest investors in this area are committed to achieving their objectives and supplanting U.S. technology and strategic leadership. In doing so, they can tighten their grip to better determine their own geopolitical destiny in the same way the United States has since the end of the Second World War.

Quantum is both a national security threat and a potential strategic advantage. To ensure our place in the future, we must focus on both elements today. **PRISM**

## Endnotes

<sup>1</sup>“Quantum Information Research In China”, Qiang Zhang et al 2019 *Quantum Sci. Technol.* 4 040503 and Trump Administration Fiscal Year 2021 budget outline: [https://www.whitehouse.gov/wp-content/uploads/2020/02/budget\\_fy21.pdf](https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf).

<sup>2</sup>James Gannon (2002), *“Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century”*, Washington, D.C.: Brassey’s, ISBN 978-1-57488-367-1.

<sup>3</sup>“Speech to the National Military Intelligence Association”, *Aerospace Daily*, September 25, 1983.

<sup>4</sup>F. W. Winterbotham, *“The Ultra Secret”*, Dell, August 15, 1975; Gordon Welchman, *“The Hut Six Story: Breaking the Enigma Codes”*, McGraw-Hill, March 1, 1982.

<sup>5</sup>Morgan Wright, “America’s Enigma Problem with China: The Threat of Quantum Computing”, *The Hill*, March 8, 2018.

<sup>6</sup>Brian Wang, “Quantum Annealer 10,000 times faster than classical computers by 2023”, *Next Big Future*, June 23, 2017.

<sup>7</sup>P.W. Shor, (1994). “Algorithms for quantum computation: discrete logarithms and factoring”. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press: 124–134.

<sup>8</sup>Shaun Nichols, “‘I give fusion power a higher chance of succeeding than quantum computing’ says the R in the RSA crypto-algorithm”, *The Register*, February 26, 2020.

<sup>9</sup>Numberphile, Quantum Computing and Other Extras with Ron Rivest, <https://www.youtube.com/watch?v=tX7e7CgWrvM>.

<sup>10</sup>Quantum Threat Timeline, Dr. Michele Mosca, Dr. Marco Piani, Global Risk Institute, October 19, 2019.

<sup>11</sup>Sara Peters, “Cryptographers Panel Tackles Espionage, Elections, and Blockchain”, *Dark Reading*, February 26, 2020.

<sup>12</sup>Will Knight, “IBM Raises the Bar with a 50-Qubit Quantum Computer”, *MIT Technology Review*, November 10, 2017.

<sup>13</sup>Will Knight, “Quantum Inside: Intel Manufactures an Exotic New Chip” *MIT Technology Review*, October 10, 2017.

<sup>14</sup>Peter Bright, “Microsoft makes play for next wave of computing with quantum computing toolkit”, *Ars Technica*, September 25, 2017.

<sup>15</sup>D-Wave Systems Press Release, “D-Wave Announces D-Wave 2000Q Quantum Computer and First System Order”, January 24, 2017.

<sup>16</sup>Emily Conover, “Google moves toward quantum supremacy with 72-qubit computer”, *Science News*, March 5, 2018.

<sup>17</sup>Jeremy Hsu, “CES 2018: Intel’s 49-Qubit Chip Shoots for Quantum Supremacy”, Institute of Electrical and Electronics Engineers, January 9, 2018.

<sup>18</sup>Martin Giles, “Old-fashioned silicon might be the key to building ubiquitous quantum computers”, *MIT Technology Review*, February 15, 2018.

<sup>19</sup>Frederic Lardinois, “IBM Unveils Its First Commercial Quantum Computing”, *Tech Crunch*, January 8, 2019.

<sup>20</sup>Stephen Shankland, “IBM’s New 53 Qubit Quantum Computer Is Its Biggest Yet”, *CNET*, September 18, 2019.

<sup>21</sup>“Quantum Computing: How to Invest in it and Which Companies are Leading the Way”, NASDAQ.com, February 11, 2020.

<sup>22</sup>Adam Janofsky, “Companies Explore Encryption that Withstands Quantum Computing”, *Wall Street Journal*, September 9, 2019.

<sup>23</sup>D-Wave Press Release, “D-Wave Previews Next Generation Quantum Computing Platform”, February 27, 2019.

<sup>24</sup>“Quantum Computing: How to Invest in it and Which Companies are Leading the Way”, NASDAQ.com, February 11, 2020.

<sup>25</sup>“What Our Quantum Computing Milestone Means,” Sundar Pichai, Google Blog, October 23, 2019.

<sup>26</sup>Chris Holt, “The U.S. Again Has the World’s Biggest Supercomputer”, *Engadget*, June 8, 2018.

<sup>27</sup>Alex Weibel, “Round 2 Hybrid Post-Quantum TLS Benchmarks”, *AWS Security Blog*, April 13, 2020; Barbara Darrow, “How Much Should CIOs Care About Quantum Today”, *CIO Magazine*, July 13, 2018; Jeremy Kirk, “Google Tests Post-Quantum Crypto,” *Bank Info Security*, July 11, 2016.

<sup>28</sup>“Quantum Computing Market Size Growth Opportunity and Forecast to 2025”, *Market Watch*, November 5, 2019.

<sup>29</sup>Dan Timpson, “Staying Secure in a Post-Quantum World”, *Forbes*, March 12, 2020.

<sup>30</sup>Elizabeth Gibney, “Europe plans giant billion-euro quantum technologies project”, *Nature*, April 21, 2016.

<sup>31</sup>“First Prototype of a Quantum Computer on Superconductive Materials Successfully Launched in Russia”, <https://en.misis.ru/university/news/misc/2019-10/6277/>.

<sup>32</sup>Fraunhofer Press Release, “IBM and Fraunhofer team up to promote quantum computing in Europe”, September 10, 2019.

<sup>33</sup>“Japan Aims to Put Quantum Cryptography to Practical Use”, *Japan Times*, August 24, 2019.

<sup>34</sup>“India Finally Commits to Quantum Computing, Promises \$1.12B Investment,” *The Next Web*, February 3, 2020.

<sup>35</sup>Quantum Key Distribution Network, Defense Advanced Research Projects Agency <https://www.darpa.mil/about-us/timeline/quantum-key-distribution-network>.

<sup>36</sup>“White House Launches National Quantum Coordination Office”, Government Innovators Network, March 2019.

<sup>37</sup>Tajha Chappellet-Lanier, “White House Launches National Quantum Coordination Office”, *Fedscoop*, March 4, 2019.

<sup>38</sup>Tajha Chappellet-Lanier, “President Trump launches National Quantum Initiative Advisory Committee”, *Fedscoop*, September 3, 2019.

<sup>39</sup>“Why Should I Care About Quantum Computing?”, *The Cipher Brief*, March 19, 2020.

<sup>40</sup>Trump Administration Fiscal Year 2021 budget outline: [https://www.whitehouse.gov/wp-content/uploads/2020/02/budget\\_fy21.pdf](https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf).

<sup>41</sup>Martin Jacques, *When China Rules the World: The End of the Western World and the Birth of a New Global Order* (Penguin Press, New York, NY), 2009.

<sup>42</sup>“Thirteenth Five-Year Science and Technology Military-Civil Fusion Development Special Plan” (Full Text), September 26, 2017, <http://www.aisixiang.com/data/106161.html>.

<sup>43</sup>Elsa B. Kania and John K. Costello, “Quantum Hegemony: China’s Ambitions and the Challenge to U.S. Innovation Leadership, Center for the New American Century”, September 12, 2018.

<sup>44</sup>Center for Strategic and International Studies (CSIS) speaking engagement, “American Innovation in the Quantum Future”, featuring Hartmut Neven, Engineering Director, Google AI and Quantum Team, January 20, 2020.

<sup>45</sup>Arthur Herman, “The Quantum Computing Threat to American Security”, *The Wall Street Journal*, November 10, 2019.

<sup>46</sup>“Quantum Information Research In China”, Qiang Zhang et al 2019 *Quantum Sci. Technol.* 4 040503.

<sup>47</sup>“Quantum Information Research In China”, Qiang Zhang et al 2019 *Quantum Sci. Technol.* 4 040503.

<sup>48</sup>“China launches world’s first quantum science satellite,” *Physics World*, August 16, 2016.

<sup>49</sup>Elsa B. Kania and John K. Costello, “Quantum Hegemony: China’s Ambitions and the Challenge to U.S. Innovation Leadership, Center for the New American Century”, September 12, 2018.

<sup>50</sup>Patinformatics, Quantum Information Technology (QIT): A Patent Landscape Report, 2018.

<sup>51</sup>Patinformatics, Quantum Information Technology (QIT): A Patent Landscape Report, 2018.

<sup>52</sup>“Hefei’s Construction a National Science Center from ‘Design’ to ‘Construction Map,’” *China News Network*, September 12, 2017.

<sup>53</sup>Stephen Chen, “China building world’s biggest quantum research facility,” *South China Morning Post*, September 11, 2017; and “Hefei’s Construction a National Science Center from ‘Design’ to ‘Construction Map,’” *China News Network*, September 13, 2017.

<sup>54</sup>“Alibaba to spend more than US\$15bn on technology research with launch of collaborative academy,” *South China Morning Post*, October 11, 2017.

<sup>55</sup>“China’s plan to recruit talented researchers,” *Nature*, January 17, 2018; and “China’s programme for recruiting foreign scientists comes under scrutiny,” *South China Morning Post*, November 3, 2017.

<sup>56</sup>Jeanne Whalen, “The quantum revolution is coming and Chinese scientists are at the forefront,” *The Washington Post*, August 8, 2019.

<sup>57</sup>U.S. Department of Commerce, National Institute of Standards and Technology (NIST) <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization>.

# SSQ STRATEGIC STUDIES QUARTERLY

## NEW BOOKS LIST



Hope you enjoy the SSQ listing of new books related to national security and defense. These lists for selected topics contain new releases from multiple publishers over the preceding year and a few upcoming titles.

The list will be updated semi-annually and contains linked abstracts for easy evaluation. Specific topics are below. Find them at: <https://www.airuniversity.af.edu/AU-Press/Display/Article/2308992/strategic-studies-quarterly-new-books-list/>

---

**Cyber-Technology Issues**  
**Indo-Pacific-Asia**  
**National Security-Great Power Conflict**  
**Nuclear Issues**  
**Russia-Europe Topics**  
**Space Issues**

---

While we strive to include all new books within the selected topic, some titles may be missing. If you notice an omission, please let us know:  
[StrategicStudiesQuarterly@au.af.edu](mailto:StrategicStudiesQuarterly@au.af.edu).

If you find the lists helpful, please let us know!



Airmen stationed at Nigerien Air Base 101 in Niamey, Niger, and Nigerien Air Base 201 in Agadez, support partner forces and international efforts to counter violent extremist organizations. (USAFRICOM)

# No Competition Without Presence Should the U.S. Leave Africa?”

By Katherine Zimmerman

American blood and treasure should be prioritized to secure U.S. national interests. The United States military is not the world’s police force, and where others can share the burden, the United States should add only its unique capabilities. But defending U.S. interests extends even into faraway lands, including Africa. While Africa may never be a top national security concern for the United States, a convergence of gains by state and nonstate actors alike there affect U.S. security and economic interests globally. Yet the Pentagon’s recent effort to rebalance its resources against great power competitors—especially China and Russia—after almost two decades of counterterrorism dominance places the commitment of U.S. military resources to Africa in question. Drawing down too far militarily in Africa risks losing influence on the continent to those very same state actors, erasing hard-fought counterterrorism gains, and compromising U.S. global interests.

America’s global competitors—China, Russia, and transnational terror organizations like al-Qaeda and the Islamic State—are growing in strength on the continent. Chinese investment in Africa has outpaced that of the United States for the past decade,<sup>1</sup> and corrupt Chinese practices benefit Chinese companies at the expense of Africans and fair economic competition.<sup>2</sup> Chinese security initiatives chip away at the influence of U.S.-run partner capacity building programs, and Russian military sales and business deals show renewed Kremlin interest in old Soviet stomping grounds.<sup>3</sup> Transnational Salafi-jihadi terror organizations have increasingly insinuated themselves into local conflicts, imperiling the stability of African states.

Meanwhile, European allies face their own national security challenges in Africa. Many of their interests largely align with American interests, creating an opportunity for the United States to support and partner with its allies on the continent. Some interests derive from Europe’s colonial history in Africa, the legacy of which is far from positive, however. Migration through North Africa to Europe is a key concern, especially given the current stress on European economies. Coupled with the rising strength of al-Qaeda and the Islamic State in Africa, Europe faces an increasing risk of terror cells embedding in migrant flows. France, which is conducting counterterrorism operations in West Africa, requires American support to sustain operations at the current scale.<sup>4</sup> These interests, in addition to global health concerns and promoting good governance and

---

Katherine Zimmerman is a Research Fellow at the American Enterprise Institute (AEI) and the Research Manager for AEI’s Critical Threats Project.

democratic values, mean the United States should not pull resources from Africa.

America's military investment in Africa yields wide-ranging dividends that help advance American interests from counterterrorism to democracy promotion to global health initiatives. United States Africa Command (AFRICOM) and Special Operations Command Africa (SOCAFRICA) build relationships through security cooperation and partnership training programs that are some of the most crucial U.S. relationships in Africa outside embassy walls.<sup>5</sup> They support allies and partners in counterterrorism operations, allowing non-U.S. troops to lead the ground effort. All the while, U.S. military engagements continue to promote American values and principals. Most importantly, they help to secure the theater for all other U.S. lines of effort—diplomatic, information, economic, and political—to protect and advance American interests in Africa.

The debate over U.S. resource commitments in Africa shows a fundamental misunderstanding of the competition for influence on the continent and the strategic risks that the United States will incur should it draw down its already modest military presence. A comparatively small U.S. military investment in Africa buys an outsized share of U.S. influence and crucially enables American soft power to shape the future trajectory of the continent in America's interest.

### **What's at Stake in Africa?**

In a world where spheres of influence are shifting, the lines in Africa have yet to be drawn. African countries help secure three of the world's major maritime chokepoints—the Strait of Gibraltar, the Suez Canal, and the Bab al Mandab Strait—through which one-third of global shipping moves. Chinese and Russian interests in places such as Eastern Europe and Southeast Asia are well understood, and the reasons to preserve American influence

there known. China and Russia now seek to build their influence on NATO's southern flank, and the United States has been slow to react. Public health initiatives, major development projects, democracy promotion, and more recently, counterterrorism efforts have largely comprised U.S. engagements in Africa.<sup>6</sup> The plurality of African states maintained their neutrality during the Cold War—seeking to play the powers off each other without choosing sides—and have adopted similar approaches today as the United States frames its engagements in terms of great-power competition.<sup>7</sup> U.S. engagements have not sufficiently kept pace with the changing landscape in Africa. Meanwhile, China, Russia, and Salafi-jihadi groups are seizing opportunities.

The world's fastest growing population and economies—before the coronavirus pandemic—are in Africa. Sub-Saharan Africa's population growth rate is more than twice that of South Asia.<sup>8</sup> Current projections have Africa's population doubling to 2.5 billion people by 2050, when Africa will be home to about a quarter of the world's population.<sup>9</sup> Such projections undoubtedly mask internal variations across the continent, where fertility rates vary as do levels of urbanization and ethnic diversity. Yet the expectation is that growth will occur in the urban space and the labor force will be younger.<sup>10</sup> Today, Africa's economic power remains untapped, only accounting for about 3 percent of global GDP.<sup>11</sup> If managed properly, a growing population, however, and better integration into the global economy could expand Africa's middle class, increasing the continent's total spending power.<sup>12</sup> African economies could also be primed for companies looking to diversify supply chains from China in a post-coronavirus world.<sup>13</sup>

Africa's potential economic growth and its natural resources still present ripe opportunities for trade and investment. If GDP growth had continued apace, however unlikely in the aftermath of the coronavirus pandemic, Africa would have outperformed other emerging and developing countries



(excluding China and India) and the world economy over the next few years.<sup>14</sup> American foreign direct investment in Africa—the largest single source to the continent—peaked in 2014 and flattened since, whereas Chinese investment has risen steadily.<sup>15</sup> China recognized Africa’s potential and has become its largest trading partner over the past decade. Sino-African trade fell by 14 percent in the first quarter of 2020 as the coronavirus pandemic hit, however, and may continue to shrink.<sup>16</sup> Yet China’s Belt and Road Initiative, launched in 2014, has facilitated the strengthening of Sino-African relations through infrastructure development and trade initiatives.<sup>17</sup> China is the biggest bilateral creditor to several African countries and now holds a source of leverage over those nations desperate for debt relief.<sup>18</sup>

Economics are not the only factor. Beijing has begun improving African governments’ capacity for intelligence and surveillance using emergent technologies, like facial-recognition software, that will enable those governments to protect Chinese investments and better control their own people.<sup>19</sup> The coronavirus pandemic will increase demand for this technology.<sup>20</sup> Russia, too, has sought to mitigate the impact of economic sanctions through investments in Africa—investing in mining operations and developing new export markets, particularly for Russian arms.<sup>21</sup> From a national security perspective, China or Russia successfully cornering the market on some critical reserves of minerals of which the United States is a net importer from African countries could disrupt supplies.<sup>22</sup>

Rising insecurity could undercut Africa’s economic growth, however, and the impact of the coronavirus pandemic will reverberate through African economies. The world’s most fragile states—marked by weak state legitimacy and/or capacity—are concentrated in Africa, including seven of the top ten.<sup>23</sup> They face significant challenges. The coming youth bulge will boost economic growth only if African states are able to capitalize on

it. Africa’s growing youth population will unquestionably strain demands on public goods and services; healthcare, education, and basic infrastructure.<sup>24</sup> Desertification driven by climate change will further reduce arable land, stoking local conflict between pastoral and agrarian communities.<sup>25</sup> Both the youth bulge and climate trends will contribute to internal migration patterns and drive urbanization, further taxing state infrastructure. The pull of economic opportunity drives much of Africa’s internal migration as well as migration to Europe.<sup>26</sup> Armed conflicts persist in places like the Central African Republic, the Democratic Republic of the Congo, Libya, Mali, Nigeria, Somalia, and South Sudan. Active Salafi-jihadi groups, including ones now affiliated with al-Qaeda and the Islamic State, further exacerbate the destabilizing effect of the conflicts.<sup>27</sup>

The Salafi-jihadi threat inside Africa is expanding. The ties between local Salafi-jihadi groups and transnational networks are strengthening as those groups embed further in complex conflicts. In East Africa, al-Qaeda’s largest and most active affiliate al-Shabaab leads an insurgency against the Somali government and poses a regional terror threat.<sup>28</sup> It has targeted and killed U.S. military personnel in Somalia and Kenya.<sup>29</sup> Alarming, al-Shabaab seeks more advanced attack capabilities that signal ambitions to conduct mass-casualty attacks on civilian aircraft, including trying to acquire Chinese-made, shoulder-fired anti-aircraft missiles, and possibly train pilot-terrorists emulating the 9/11 attack.<sup>30</sup> A Salafi-jihadi group newly affiliated with the Islamic State in Mozambique poses a growing insurgent threat in the country’s northeastern most province.<sup>31</sup> Using the same group name, the Islamic State has claimed attacks in the Democratic Republic of the Congo.<sup>32</sup> In North Africa, both al-Qaeda and the Islamic State retain sanctuaries. Al-Qaeda has prioritized control of trafficking routes over terror attacks whereas the Islamic State has conducted attacks in Algeria, Libya, and Tunisia.<sup>33</sup> In West Africa,

al-Qaeda and the Islamic State are pushing into neighboring states from the Sahel as they strengthen and improve their own attack capabilities.<sup>34</sup> The Islamic State is also seeking to connect its Sahel- and Nigeria-based branches.<sup>35</sup>

China and Russia each see opportunities to expand their influence in Africa through security assistance and weapons sales. The Kremlin has signed new agreements with African countries in recent years, including over 19 agreements on military-technical cooperation.<sup>36</sup> Russian private military companies (PMCs) extend the Kremlin's reach, entering countries to protect Russian investments and prop up regimes.<sup>37</sup> Russian PMCs train Central African Republic army recruits and are almost certainly behind the downing of a U.S. drone in Libya.<sup>38</sup> Chinese security assistance and arms sales are integrated into the Belt and Road Initiative. China has also bought influence through financial and military assistance to African Union peace and security initiatives, along with increasing

its contributions to UN peacekeeping missions—sprinkling members of the Chinese security forces across Africa.<sup>39</sup> China's most concerning investment has been its new military base in Djibouti, which provides the Chinese military with the ability to monitor and even interfere with U.S. military activities out of Camp Lemonnier.<sup>40</sup>

A negative feedback loop is occurring where some African states are becoming increasingly authoritarian as aggrieved populations mobilize against the state. Salafi-jihadi groups, especially in West Africa, have intentionally stoked intercommunal tensions and antigovernment sentiments to mobilize insurgencies to create opportunities to expand their influence into vulnerable communities. The heavy-handed state response, labeled as counterterrorism, punishes communities exploited by these groups and only further inflames the insurgency. The more transactional nature of Chinese and Russian engagements does little to foster good governance. Their weapons sales do not come with the same



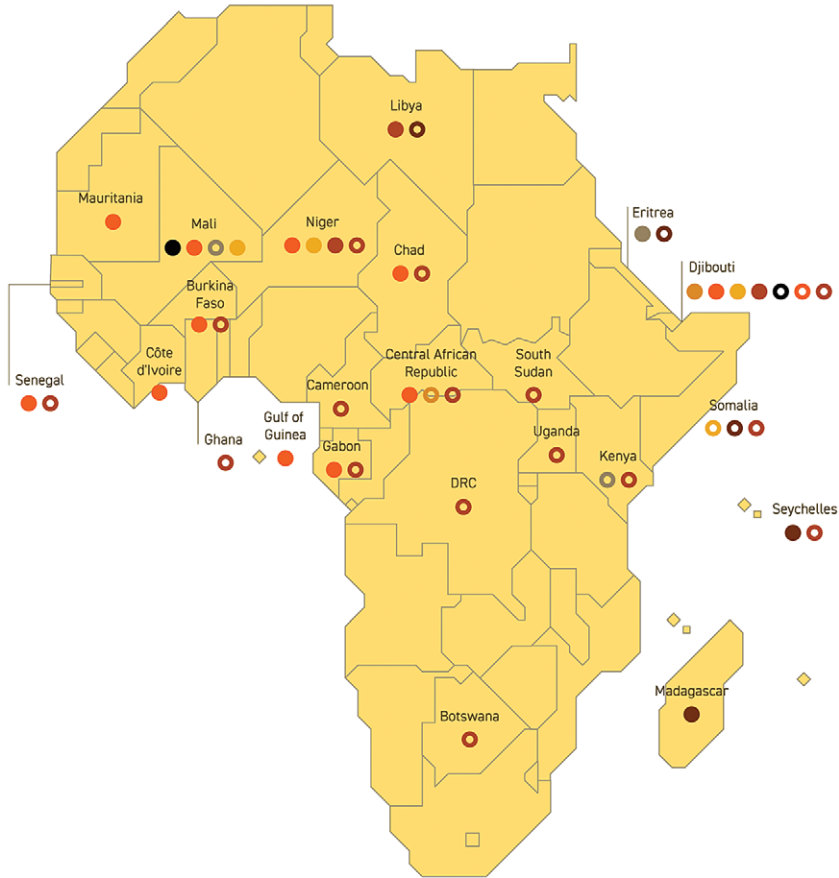
These Russian aircraft are being used to support private military companies (PMCs) sponsored by the Russian government. (Credit: U.S. Africa Command Public Affairs)

Figure 6.7

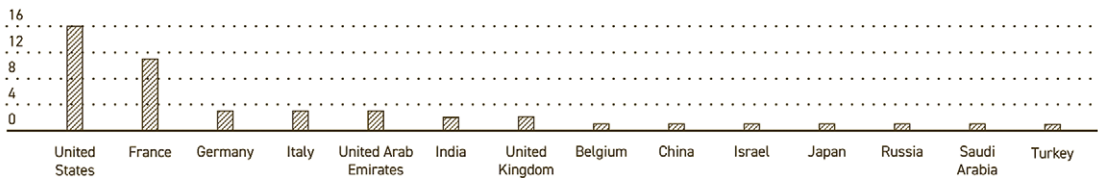
Defense partnerships: Military outposts in Africa

As commercial engagement has increased so has security collaboration, with many African countries hosting a number of European and Asian military outposts. Djibouti's location on the Red Sea makes it a particularly strategic security partner. Even so, the United States remains the partner with the most military outposts in the region, followed by France.

- Belgium
- China
- France
- Germany
- India
- Israel
- Italy
- Japan
- Russia
- Saudi Arabia
- Turkey
- United Arab Emirates
- United Kingdom
- United States



Military outposts by foreign country



Source: Andrews Atta-Asamoah, "Proceed with caution: Africa's growing foreign military presence," Institute for Security Studies, August 27, 2019.



Defense outposts, military outposts in Africa (Andrew Atta-Asamoah, Brookings Institution)

restrictions as with U.S. sales and end-use monitoring is not strictly enforced. Russian PMCs operate with shadier parts of regimes, using the relationship to advance other Russian interests, and Chinese improvements to intelligence capabilities improve the state's ability to target dissenters. Both China and Russia are strengthening dictatorships at the cost of democracy and liberal principles in Africa.<sup>41</sup>

Africa is a key theater to protecting U.S. national security interests worldwide. The United States will not win the global competition for influence with China or Russia in Africa outright, but it could face serious setbacks there. The United States must retain its influence in terrain far more critical to both of these competitors in Europe and Asia to keep its edge against them. Chinese or Russian gains in Africa, however, could start to tip the scales. The same is true for al-Qaeda and the Islamic State—neither will be defeated globally if eradicated from Africa, but their African safe havens strengthen their global networks.<sup>42</sup> Combined, these state and nonstate competitors increase volatility and enable authoritarian trends.<sup>43</sup> The United States must ensure that even as it rebalances its security resources and encourages burden-sharing with allies and partners, it invests enough to protect its interests in Africa.

## AFRICOM's Ways and Means

The Trump administration laid out its strategy to secure American interests in Africa in late 2018.<sup>44</sup> The idea of competing with China and Russia runs through the strategy, similar to the National Defense Strategy. AFRICOM updated its mission statement to reflect U.S. strategic priorities in early fall 2019, shifting its priorities toward countering malign actors.<sup>45</sup> Whereas previously strengthening partners and their capabilities came first, now countering transnational threats and malign state actors (read: China and Russia) takes precedence.

AFRICOM's current activities fall under three general categories. The first is the traditional role

that AFRICOM has played; building partnership capacity. Since its inception, AFRICOM has invested in improving African partners' security forces and defense institutions. The second category is counterterrorism operations and support activities. These include direct-action operations and support—training, advising, and assisting—to counterterrorism partners. The third category is infrastructure and logistics. AFRICOM's posture on the continent not only provides it a platform from which to conduct operations but also supports other U.S. government departments and agencies. Beyond these regular activities, AFRICOM also sustains crisis response forces in Germany, Spain, Italy, and Djibouti to react to developing crisis situations.<sup>46</sup>

### *Building Partnership Capacity*

AFRICOM works to strengthen and increase the capacity of African security forces to improve the overall security environment on the continent. Its Theater Security Cooperation Programs (TSCP) reinforce partnerships with African nations, improve their ability to respond to threats, diminish threats to U.S. interests, and help establish better security conditions to foster economic development. TSCP range in nature and include military training, capacity building, leadership development, professionalization, and humanitarian programs.<sup>47</sup> The Command also sponsors regional military exercises such as *Operations African Lion* and *Flintlock* to improve the interoperability of African forces and reinforce professionalism across the ranks.<sup>48</sup> AFRICOM also works with partners on counter-narcotics and -trafficking activities, in addition to counterterrorism.<sup>49</sup>

### *Counterterrorism Operations*

AFRICOM conducts direct-action operations and supports counterterrorism partners to degrade Salafi-jihadi groups on the continent. Nearly all of the direct-action operations are drone strikes targeting senior leaders and operatives, training

camps, or massed forces in Somalia and Libya.<sup>50</sup> U.S. counterterrorism support to African partners runs the gamut from security force assistance in the form of equipment or training to improve the capabilities of partnered forces, to conducting advise, assist, and accompany missions, to intelligence and logistics support. Embedded advisers make partners more effective and very likely improve respect for human rights norms.<sup>51</sup> AFRICOM has prioritized the East Africa theater, which hosts the Combined Joint Task Force-Horn of Africa (CJTF-HOA) at Camp Lemonnier, an operational headquarters stood up in the aftermath of the 9/11 attacks. From there, U.S. forces are countering al-Shabaab, al-Qaeda's largest and most active affiliate, and the Islamic State in Somalia.<sup>52</sup>

In East Africa, U.S. forces partner with Somali security forces and the African Union Mission in Somalia (AMISOM), and are deployed to Kenya and Djibouti to conduct and support counterterrorism as well as counterpiracy operations. The majority of U.S. forces in Africa—about 3,000 troops—are posted at Camp Lemonnier in Djibouti with CJTF-HOA, where they support counterterrorism operations in the region as well as training for partners. AFRICOM has built a specialized Somali force—the Danab Advanced Infantry Brigade—to serve as an elite counterterrorism unit within the Somali National Army (SNA).<sup>53</sup> About 500 U.S. Special Operations troops are deployed along with Danab units to advise, assist, and accompany them in operations against al-Shabaab.<sup>54</sup> AFRICOM has also provided training for AMISOM troop-contributing countries such as Burundi, Djibouti, Ethiopia, Kenya, and Uganda to improve their operational capabilities against al-Shabaab, and has the authority to assist AMISOM forces on the ground.<sup>55</sup> About 300 troops and contractors are in Kenya, where they train, advise, and share intelligence with Kenyan forces.<sup>56</sup>

In West Africa, the United States supports the G5 Sahel Joint Force, the Multinational Joint Task

Force (MNJTF), regional partners, and NATO ally France, which leads counterterrorism operations in the Sahel. About 800 to 1,400 troops are deployed in the region, most based in Niger.<sup>57</sup> AFRICOM supports the French military with strategic airlift, aerial refueling, and intelligence, surveillance, and reconnaissance (ISR). It provides bilateral support, varied in scope, to the G5 Sahel Joint Force troop-contributing countries (Burkina Faso, Chad, Mali, Mauritania, and Niger) in the form of training and equipping units.<sup>58</sup> Additionally, a small U.S. contingent works with Nigerians in the Intelligence Fusion Center to combat Boko Haram and the Islamic State's West African branch.

The current counterterrorism framing and approach will not ultimately defeat the Salafi-jihadi groups.<sup>59</sup> The strategy focuses on defeating the terror and security threats groups and individuals pose by degrading leadership, disrupting operations, and eliminating sanctuaries. The result is a securitized response that has yielded limited results, driving an argument to reduce resources further and target only those elements that pose direct threats. Overlooked are how the groups gain influence initially and expand, and the role of local conditions in creating the opportunities for Salafi-jihadi groups to strengthen.

### *Infrastructure and Logistics*

AFRICOM's posture on the continent supports a theater-wide logistics network as well as complements the posture of United States European and Central Commands. Two forward operating sites frame the continent; one in the Gulf of Guinea at St. Helena on Ascension Island, and the other off the Bab al Mandab Strait at Camp Lemonnier, Djibouti, which supports multiple combatant commands. Counterterrorism requirements largely inform the rest of AFRICOM's enduring footprint on the continent, which includes cooperative security locations in Ouagadougou, Burkina Faso; N'Djamena, Chad;

Chebelley, Djibouti; Manda Bay and Mombasa, Kenya; and Agadez and Niamey, Niger. AFRICOM added four additional locations in 2019 based on assessed threats to U.S. embassies, including Libreville, Gabon; Accra, Ghana; Dakar, Senegal; and Entebbe, Uganda. These positions, plus non-enduring contingency locations, constitute a lily pad of basing that stretches across the continent. Other U.S. agencies and departments use AFRICOM's logistics capabilities to support their programs in Africa.

### **AFRICOM's Crucial Role**

AFRICOM's resources may decrease as the Pentagon seeks to prioritize the competition with China and Russia. Yet AFRICOM already operates in a resource-constrained environment and has to make tradeoffs in terms of its posture and operations.<sup>60</sup> Resource prioritization across the geographic commands has meant AFRICOM has always operated at economy-of-force levels to some degree. Africa's geographic expanse and extreme environment along with weak infrastructure add operational difficulties, and its vastness dilutes the direct impact of U.S. military resources. The Pentagon reduced the number of personnel assigned to AFRICOM by 10 percent from about 7200 to 6500 troops as part of the 2018 Force Optimization plan.<sup>61</sup> Currently, the Pentagon is undertaking a "Blank Slate Review" of AFRICOM to inform decisions about future resourcing and align expenditures with the 2018 National Defense Strategy.<sup>62</sup> The Pentagon must weigh not only the impact on current operations and AFRICOM's own objectives but also the strategic impact on U.S. objectives outside the military's domain in Africa, which is where the true cost to the United States lies.

### *Need to be on the Field to Compete*

A steady stream of reports indicate that Secretary of Defense Mark Esper will further reduce AFRICOM's personnel, which will likely accompany additional cuts to security cooperation programming. Such

cuts will reduce the U.S. presence on the continent and create opportunities for Beijing or Moscow. Whether shifting the small amount of resources saved from Africa to another theater—Asia or Europe—will result in more than marginal gains is unclear. But the United States cannot compete in Africa if it does not have a presence.

Certainly, AFRICOM could scale back some of its security sector assistance without significantly risking American interests. AFRICOM conducts its partnership programs under a patchwork of authorities and funding streams. The operational or even strategic effect of these programs is not always clear nor is the lasting impact known. The tactical nature of some of the U.S. programs to build partnership capacity means their elimination will not be felt beyond the specific partner. The value-add of security sector assistance to reduce political violence and improve local stability remains an open question. A 2018 RAND study found that many of the U.S. training activities are one-off events rather than AFRICOM's envisioned "train-the-trainer" approach, diminishing the overall impact of the training and resulting in only temporary gains.<sup>63</sup> NATO allies with vested regional interests in Africa also conduct training and exercises with partners. Better coordination with these allies might minimize the effect of reduced U.S. programming.

Beijing's and Moscow's influence in Africa is growing, due in no small part to an effort on their end to invest time and resources in renting influence in African governments. Their efforts include military sales and security sector assistance in tandem with soft power engagements.<sup>64</sup> Both have eyed expanding their naval presence at African ports, which would support their commercial investments. AFRICOM (and the U.S. government writ large) should not try to match this move-for-move, especially since what the United States offers and what China or Russia offers are fundamentally different. Moreover, neither China nor Russia burden

themselves with ensuring that their partners follow international norms and respect human rights. The United States must never abandon its own values in an effort to squeeze out competition. But even without hope of winning the match for arms sales and security assistance against China and Russia directly, the United States must remain in the game by pursuing its own interests with African partners.

Cutting U.S. security assistance programming to the bare minimum carries costs beyond the dollars saved and absence or degradation of specific military capabilities. Some programs that might have little-to-no value in furthering security objectives may preserve U.S. influence within a country, supporting the overarching objective of advancing broader U.S. strategic aims. The programs provide a source of leverage to encourage or cajole governments that need security assistance to adopt other political or economic reforms or to support U.S. initiatives in international organizations.<sup>65</sup> U.S. security assistance programming can help pave the way for security through civilian-led initiatives. It also limits the overall influence of China or Russia by protecting against African dependence on either and keeping the option open for countries to choose aligning with the United States. China and Russia may offer faster, short-term fixes on a more transactional basis, but China's debt diplomacy and Russia's profiteering are not in countries' long-term interests. The United States must recognize that African countries will often accept whatever assistance might come their way—for many, a bad deal is better than no deal.

### *Counterterrorism Partnerships Support Multiple Priorities*

Current U.S. counterterrorism operations in Africa would be almost impossible without America's partners. They, rather than U.S. forces, have taken the lead. African Salafi-jihadi groups—al-Shabaab, Boko Haram, al-Qaeda in the Islamic Maghreb, Jama'at Nusrat al Islam wa al Muslimeen, and the Islamic

State branches—do not yet pose a direct threat to the U.S. homeland. The groups' more localized threat and less-developed capabilities resulted in far fewer U.S. resources going toward the fight against them, which in turn generated AFRICOM's light-footprint approach to the problem. Many U.S. partners would not be able to achieve what they have against local Salafi-jihadi groups without U.S. inputs. Moreover, these counterterrorism partnerships support priorities beyond just neutralizing this threat.

The effectiveness of AFRICOM's counterterrorism operations is mixed. U.S. operations have targeted the global elements of Salafi-jihadi groups to diminish the transnational threat. None of the current counterterrorism efforts is on course to defeat the local groups, however. The United States has supported partners in the fight against al-Shabaab in Somalia for over a decade. Al-Shabaab no longer controls the majority of the country or the major populated areas, but its external attack capability remains worrisome. The security forces of America's partners—Kenyan, Ugandan, Burundian, and Somali troops among others—are more capable and conduct successful ground campaigns against al-Shabaab. However, insufficient ground forces preclude further progress. U.S. counterterrorism operations in Libya have degraded the Islamic State branch to a shadow of its former self since 2016, though the group is actively seeking to reconstitute.<sup>66</sup> Finally, the U.S.-backed French-led operations in the Sahel may have slowed the expansion of and degraded the leadership network of Salafi-jihadi groups but the trajectory of violence remains discouraging. Notwithstanding their operational effectiveness, U.S. counterterrorism operations have built and strengthened intra-African relationships when the U.S. and its allies have facilitated multinational task forces and cross-border coordination that might not have been readily achieved without an external push.

Counterterrorism partnerships bolster American influence with partnered countries. They

facilitate the establishment of and reinforce relationships with African partners, serving to address immediate local security needs, while also establishing an American role and presence that competes with global actors like Russia. Scoping American counterterrorism support only to areas where Salafi-jihadi groups directly threaten the U.S. homeland alienates partners on whom America relies to pressure terrorist groups—partners who have to deal with the security challenges regardless of whether the Americans are present or not. The United States should recognize that partners' interests include eliminating the Salafi-jihadi-generated violence and insecurity in their own territory, not just the cells threatening America, and that the local Salafi-jihadi base bolsters the broader threat network.<sup>67</sup> If partners are incapable of defeating the groups, they might lift pressure and incentivize the groups to focus efforts on Americans as the “far” enemy.<sup>68</sup> Moreover, African partners might misread the withdrawal and perceive it as the United States pulling away from them.

In Libya, the withdrawal of U.S. troops after they achieved counterterrorism objectives against the local Islamic State branch eliminated any platform for future U.S. military or even diplomatic efforts. Moscow moved to fill some spaces the United States abandoned by meddling more directly in the civil war after flirting with various factions over the years. Russia has now gained a toehold on the southern Mediterranean Sea and its presence could constrain U.S. operations in Libya and threaten regional maritime interests. The U.S. diplomatic mission to Libya has been in Tunis, Tunisia, since its temporary relocation there in July 2014.<sup>69</sup> Security conditions severely constrain the movements of the U.S. ambassador to Libya and other diplomats and aid workers. AFRICOM sustained a small counterterrorism presence to combat the Islamic State until April 2019, when the troops withdrew due to the volatile environment.

By September 2019, up to about 200 Russian mercenaries linked to the Wagner Group and other PMCs deployed to bolster one faction in the Libyan Civil War.<sup>70</sup> By the end of 2019, about 800 to 1,400 Russian mercenaries were in Libya, and in May 2020, Russian military fighter aircrafts deployed to Libya—a move indicative of Moscow's backing of the PMCs and reminiscent of Russian maneuvers in Syria.<sup>71</sup> The United States reacted by considering the possible future deployment of a contingent from AFRICOM's new Security Force Assistant Brigade (SFAB) to Tunisia, though this does not directly contest the Russian position in Libya.<sup>72</sup>

Cuts to AFRICOM would likely reduce U.S. support to French operations in West Africa while leaving counterterrorism operations in East Africa relatively unaffected.<sup>73</sup> Already, resource constraints have caused AFRICOM to downgrade its counterterrorism objectives in West Africa from “degrading” to “containment.”<sup>74</sup> The French have led operations in the Sahel since 2013 and began a procurement process to regain operational independence as they boost defense spending to meet NATO treaty requirements. They are unable to sustain their current level of counterterrorism operations without U.S. intelligence and strategic airlift.<sup>75</sup> AFRICOM brings additional capabilities with its support that the French will lose; leadership, trust capital with partners, and the ability to pull together broader coalitions. The United States will in turn incur the risk that the already escalating Salafi-jihadi threat in the Sahel destabilizes the region and more dangerously, expands to transnational terror attacks. The move also undercuts America's entire counterterrorism partnership model that successive administrations have sought to generate as a replicable and sustainable effort with America's allies and partners. The French require a small investment from the United States—\$40 million annually in direct support—to operate, and in return, spend about \$700 million on their



military operations in the Sahel. Allies like France might be less willing to commit to a fight militarily if they cannot rely on critical U.S. enablers to give them a better edge on the battlefield. Moreover, the Defense Department's de-prioritization of the Sahel is at odds with the State Department's re-direction of the global coalition against the Islamic State to the Sahel as a primary theater.<sup>76</sup>

#### *A Hard-Power Platform for American Soft Power*

The U.S. military is a critical enabling factor in Africa for American diplomatic, political, economic, and development initiatives. Both the State Department and the U.S. Agency for International Development (USAID) have said that they would be able to do more in Africa with a larger military platform—and the security that comes with it.<sup>77</sup> U.S. foreign assistance programs aimed at relatively rapid stabilization and strengthening of governance capacity, along with the U.S. military's contributions, is one of America's

comparative advantages over China and Russia. Shrinking the U.S. military presence will reverberate through U.S. programs, diminishing America's soft power efforts—already strapped by funding cuts and top-level vacancies in the State Department and elsewhere. It will collapse foreign assistance programming and limit face-to-face engagements, especially given the extreme aversion to risking the lives of U.S. personnel. Many U.S. diplomats and aid workers face restraints on their movement and are limited to secure zones around such places as the U.S. embassy, a legacy of the 2012 Benghazi attack that killed U.S. Ambassador to Libya J. Christopher Stevens and three other Americans. U.S. military personnel thus have become the American face outside official embassy events and African capitals as security in areas of Africa has deteriorated, though increasingly, military personnel face restrictions in their own movements, part of the legacy of the 2017 Tongo Tongo attack that killed four U.S. soldiers in Niger.



1250 people displaced by Boko Haram violence wait for medical screenings and education during a humanitarian assistance mission led by Cameroonian soldiers and funded through the USAFRICOM Humanitarian and Civic Assistance Program. (U.S. Africa Command)

The now-tired adage that there is no development without security and no security without development rings true in Africa, and is at the heart of the necessity of a civilian-military relationship to secure U.S. interests in key theaters. In Somalia, for example, frictions between the shorter military timeline and longer political timelines has prevented the consolidation of the battlefield successes against al-Shabaab. A lack of political consensus over the local administration of territory persists, sparking conflict at times, and local security forces alone are incapable of “holding” the recaptured terrain. USAID, which has personnel embedded at AFRICOM, has been unable to expand its programming into new areas without such a hold force.<sup>78</sup> Moreover, USAID personnel are generally restricted to the embassy compound, and by the end of May 2020, USAID will only have one consultant able to leave the compound to monitor programs—a severe handicap for implementation.<sup>79</sup> The U.S. military, which trains Somali forces in southern and central Somalia, provides a secure footprint beyond the capital, Mogadishu, to extend USAID’s reach and visibility in the country, enabling the soft side of U.S. foreign policy.

Shrinking the hard-power platform for U.S. foreign policy in Africa through the reduction of the military footprint could create dangerous conditions that drive diplomats from critical areas. Libya, as noted, is increasingly harder for U.S. civilian and military personnel to visit after the military withdrew and Russian PMCs moved in, along with escalations in the Libyan Civil War. A similar draw-down in West Africa may add further constraints to the U.S. civilian presence in Mali, Niger, and Burkina Faso, which is already effectively restricted to the capitals due to insecurity and terror attacks. Rather than a sphere of U.S. influence, the United States might instead see small pockets of influence, leaving opportunities for China, Russia, or a Salafi-jihadi group to fill the gaps.

## What Should the U.S. Military Do?

The U.S. military must sustain its resources in Africa but fundamentally change its approach to do more with what it has or risk losing to its competitors. China, Russia, and the Salafi-jihadi movement are all poised to seize opportunities as they present themselves—and America’s absence will only make those occurrences more frequent. AFRICOM’s posture is not the sum of the United States in Africa but AFRICOM broadens and deepens the U.S. presence especially in critical terrain such as East Africa, the Sahel, the littoral states around the Gulf of Guinea, and elsewhere. Certainly, the Trump administration’s push to cut foreign assistance and vacancies that riddle the State Department negatively affect America’s ability to secure its interests in Africa. Global demands on limited Defense Department resources must be acknowledged, as must Secretary Esper’s effort to ensure that U.S. defense resources are correctly aligned with the foreign policy priorities of today and the future.<sup>80</sup> Yet without the platform of American hard power in Africa, American soft power will be greatly diminished. Sustaining that hard-power platform, however, cannot mean continuing with the status quo.

Counterterrorism operations in Africa do not compete directly with Chinese or Russian interests. Neither power is in Africa to counter Salafi-jihadi groups. But defeating Salafi-jihadi groups is in America’s interests and the relationships with counterterrorism partners are valuable.<sup>81</sup> The United States should not compete with China or Russia on their terms, and should therefore not cede influence unnecessarily by withdrawing from large regions of the continent. The inclination to rebalance the U.S. military posture and array forces directly against China and Russia misses the comparative value that a few thousand troops on the African continent has in furthering U.S. interests versus their value deployed into theaters where the engagement with China or Russia is more direct. Those troops

dispersed across a continent provide the platform needed to extend U.S. influence through both hard and soft power into Africa.

Inevitably, the United States will need to accept greater risk in Africa given fixed resources and developments in other theaters. Some have presented the options as binary; the United States must accept more risk on the counterterrorism front, especially in Africa, after two decades of accepting too little risk against these nonstate actors at the expense of contesting state actors. In Africa especially, U.S. military operations and programs advance multiple interests, however, including both weakening Salafi-jihadi groups and building U.S. influence. Shifting resources from counterterrorism is not as low-risk as some who cite the lack of terror attacks this past decade assume. The United States will end up tapping the very same intelligence assets that kept the terror threat low to counter Chinese and Russian ambitions. Relying, therefore, on intelligence to assess the risk of an imminent terror attack against the homeland—a key metric in resource-prioritization—assumes quality intelligence where major collection gaps are more likely. Thus, how the United States frames its approach in Africa will be important in determining what types of and how much risk it incurs.

Today, counterterrorism operations across Africa are a crucial means by which the United States competes with China and Russia. They build security partnerships that extend American influence. But they also reinforce a securitized response that has not been effective overall because the underlying conditions remain unaddressed. In West Africa, the Salafi-jihadi network is expanding and strengthening. Al-Qaeda- and Islamic State-linked groups have relative freedom of movement in the border areas, where the reach of the state is weakest, and their influence is growing within their targeted communities. In East Africa, al-Shabaab controls less terrain but still poses a terror threat within the region and seeks to extend its reach farther afield.

Only in Libya have the United States and its partners successfully degraded a group. But also, only in Libya did the United States then withdraw just to watch Russian PMCs maneuver into the space.

Secretary Esper would be better advised to drive reforms that advance multiple U.S. interests, especially diplomatic, political, and economic aims, rather than pulling resources from AFRICOM. AFRICOM should improve security assistance coordination with America's allies to optimize the distribution of this critical resource among African partners. Those partners might otherwise perceive receiving training from multiple western militaries as a sign of prestige. The United States should invest what other partners cannot or will not replicate. The Secretary must also encourage a transformation in how the U.S. military combats Salafi-jihadi groups.<sup>82</sup> Salafi-jihadi groups operate across domains. They gain influence by offering pragmatic goods or services—defense and dispute resolution, for example—in communities made vulnerable by conflict and insecurity.<sup>83</sup> The Defense Department, which has borne the cost of counterterrorism, should push the State Department to lead a coordinated soft power offensive to improve local governance and provide redress for key grievances that make Salafi-jihadi incursions welcome in many communities. Foreign assistance programs should also contest the growing authoritarian tendencies reinforced by Chinese and Russian intervention. Such an approach will require change in how the interagency develops strategy and operationalizes programming. The United States must cultivate a new landscape instead of repeatedly mowing the same grass.

The knowledge and tools needed to transform the interagency approach to counterterrorism exist. Eliminating Salafi-jihadi groups' ability to exploit local conditions by improving local communities' resiliency begins to address the underlying issues that have empowered these groups. Effective local partnerships will also be necessary. Initiatives like

the 2018 Stabilization Assistance Review and the congressionally mandated Task Force for Extremism in Fragile States, among others, developed recommendations for a strategic way forward in fragile and complex environments. The 2019 Global Fragility Act provides a framework and coordinating authorities to develop and integrate a State Department-led interagency approach.<sup>84</sup> Some military requirements to combat the groups remain, and U.S. special operations forces in Africa should continue to advise, assist, and accompany partner forces on counterterrorism missions. Yet they should also use their unique vantage point to push up intelligence to the civilian side about how Salafi-jihadi groups have gained influence on the ground (rather than simply collect on the threat network), feeding into the design of U.S. foreign assistance programming and other public diplomacy efforts.

American hard power is a crucial element of U.S. foreign policy. Without the relatively light U.S. military footprint in Africa, American soft power efforts would be stymied. Reallocating defense resources from AFRICOM to compete with Chinese and Russian influence elsewhere misses the greater marginal value of a few thousand U.S. troops in Africa compared to other theaters. To sum up the argument of this article, the minuscule dollars and troops supporting U.S. efforts in Africa accomplish much more in terms of influence and effects than their redeployment to other theaters will in the competitive global field. Reducing those assets too much will strain AFRICOM's ability to operate effectively. To increase America's bang for the buck AFRICOM must innovate and transform its counterterrorism approach in partnership with the State Department and USAID in order to achieve enduring gains against the Salafi-jihadi movement, and cultivate strong African partnerships to counter Chinese and Russian influence on the continent. **PRISM**

## Endnotes

<sup>1</sup> Panos Mourdoukoutas, "How China Beats America and Europe in Africa," *Forbes*, October 24, 2019, <https://www.forbes.com/sites/panosmourdoukoutas/2019/10/24/how-china-beats-america-and-europe-in-africa/#45a593b56937>.

<sup>2</sup> Joshua Meservey, "Chinese Corruption in Africa Undermines Beijing's Rhetoric About Friendship with the Continent," Heritage Foundation, August 8, 2018, <https://www.heritage.org/global-politics/report/chinese-corruption-africa-undermines-beijings-rhetoric-about-friendship-the>.

<sup>3</sup> Eric Schmitt, "Russia's Military Mission Creep Advances to a New Front: Africa," *New York Times*, March 31, 2019, <https://www.nytimes.com/2019/03/31/world/africa/russia-military-africa.html>.

<sup>4</sup> Katherine Zimmerman, "Why the US should spend 0.3 percent of its defense budget to prevent an African debacle," *Military Times*, March 12, 2020, <https://www.militarytimes.com/opinion/commentary/2020/03/12/why-the-us-should-spend-03-percent-of-its-defense-budget-to-prevent-an-african-debacle/>.

<sup>5</sup> Judd Devermont and Leanne Erdberg Steadman, "Defending the U.S. Military Presence in Africa for Reasons Beyond Counterterrorism," *Lawfare Blog*, May 18, 2020, <https://www.lawfareblog.com/defending-us-military-presence-africa-reasons-beyond-counterterrorism>.

<sup>6</sup> These include the African Growth and Opportunity Act (AGOA), President's Emergency Plan for AIDS Relief (PEPFAR), the Millennium Challenge Corporation (MCC), Feed the Future, and most recently, Power Africa.

<sup>7</sup> US-Ethiopian relations have improved, for example.

<sup>8</sup> The Economist, "Africa's Population will Double by 2050," March 26, 2020, <https://www.economist.com/special-report/2020/03/26/africas-population-will-double-by-2050>.

<sup>9</sup> Emi Suzuki, "World's Population Will Continue to Grow and Will Reach Nearly 10 Billion by 2050," *World Bank Blogs*, July 8, 2019, <https://blogs.worldbank.org/opendata/worlds-population-will-continue-grow-and-will-reach-nearly-10-billion-2050>.

<sup>10</sup> Jack A. Goldstone, "Africa 2050: Demographic Truth and Consequences," *Governance in an Emerging New World*, issue 119, (January 2019), <https://www.hoover.org/research/africa-2050-demographic-truth-and-consequences>.

<sup>11</sup> Colin Coleman, "This Region Will Be Worth \$5.6 Trillion Within 5 Years, But Only If It Accelerates Its Policy Reforms," *WEForum*, February 11, 2020, <https://www.weforum.org/agenda/2020/02/africa-global-growth-economics-worldwide-gdp/>.

<sup>12</sup>The Economist, “Many of Africa’s Economies are Doing Well,” March 26, 2020, <https://www.economist.com/special-report/2020/03/26/many-of-africas-economies-are-doing-well>.

<sup>13</sup>Nicholas Martin, “As Coronavirus Disrupts Supply Chains, Could Africa Profit?” Deutsche-Welle, May 14, 2020, <https://www.dw.com/en/as-coronavirus-disrupts-supply-chains-could-africa-profit/a-53435112>.

<sup>14</sup>Colin Coleman, “This Region Will Be Worth \$5.6 Trillion Within 5 Years, But Only If It Accelerates Its Policy Reforms.”

<sup>15</sup>BBC, “What are the US’s Intentions in Africa?” August 1, 2019, <https://www.bbc.com/news/world-africa-49096505>.

<sup>16</sup>Kwasi Gyamfi Asiedu, “Trade Between China and Africa Dropped 14% in the First Quarter and Could Get Worse,” Quartz Africa, April 23, 2020, <https://qz.com/africa/1844049/trade-between-china-and-africa-dropped-14-percent-in-the-first-quarter/>; and Kartik Jayaram, Omid Kassiri, and Irene Yuan Sun, “The Closest Look Yet at Chinese Economic Engagement in Africa,” McKinsey, June 2017, <https://www.mckinsey.com/featured-insights/middle-east-and-africa/the-closest-look-yet-at-chinese-economic-engagement-in-africa>.

<sup>17</sup>Paul Nantulya, “Implications for Africa from China’s One Belt One Road Strategy,” Africa Center for Strategic Studies, March 22, 2019, <https://africacenter.org/spotlight/implications-for-africa-china-one-belt-one-road-strategy/>.

<sup>18</sup>European Parliamentary Research Service, “Coronavirus in Africa: A Crisis with Multiple Impacts,” May 7, 2020, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649421/EPRS\\_BRI\(2020\)649421\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649421/EPRS_BRI(2020)649421_EN.pdf).

<sup>19</sup>Paul Nantulya, “Implications for Africa from China’s One Belt One Road Strategy.”

<sup>20</sup>For more on Chinese technology in Africa, see Steven Feldstein, “China’s Strategic Aims in Africa,” statement before the US–China Economic and Security Review Commission, May 8, 2020, [https://www.uscc.gov/sites/default/files/Feldstein\\_Testimony.pdf](https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf).

<sup>21</sup>Nataliya Bugayova, “The Kremlin’s Campaign in Africa,” Institute for the Study of War, August 23, 2019, <http://www.understandingwar.org/backgrounder/kremlins-campaign-africa>.

<sup>22</sup>US Department of Commerce, *A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals*, [https://www.commerce.gov/sites/default/files/2020-01/Critical\\_Minerals\\_Strategy\\_Final.pdf](https://www.commerce.gov/sites/default/files/2020-01/Critical_Minerals_Strategy_Final.pdf), accessed April 9, 2020; US Department of the Interior, *Mineral Commodity Summaries 2020*, US Geological Survey, January 31, 2020, <https://pubs.usgs.gov/periodicals/mcs2020/mcs2020>.

pdf; and Dean Cheng, Nicolas Loris, and Klom Kitchen, “China is a Paper Tiger on Rare Earth Minerals,” Heritage Foundation, June 13, 2019, <https://www.heritage.org/asia/report/china-paper-tiger-rare-earth-minerals>.

<sup>23</sup>Some fragile states like Ethiopia and Kenya have strengthened significantly over the past year, however. <https://fragilestatesindex.org/>.

<sup>24</sup>Julia Bello-Schünemann, Jakkie Cilliers, Zachary Donnenfeld, Ciara Aucoin, and Alex Porter, “Africa Futures: Key Trends to 2035,” Institute for Security Studies, January 1, 2017, <https://issafrica.s3.amazonaws.com/site/uploads/policybrief105.pdf>.

<sup>25</sup>Nigeria is already experiencing such conflict. Conflict Group, *Herders Against Farmers: Nigeria’s Expanding Deadly Conflict*, September 19, 2017, <https://www.crisisgroup.org/africa/west-africa/nigeria/252-herders-against-farmers-nigerias-expanding-deadly-conflict>.

<sup>26</sup>Wendy Williams, *Shifting Borders: Africa’s Displacement Crisis and Its Security Implications*, Africa Center for Strategic Studies, October 17, 2019, <https://africacenter.org/publication/shifting-borders-africas-displacement-crisis-and-its-security-implications/>; International Organization for Migration, “Migration and Migrants: Regional Dimensions and Developments.” In *World Migration Report 2020*, 49–141, <https://publications.iom.int/books/world-migration-report-2020-chapter-3>; and UN Development Programme, *Scaling Fences: Voice of Irregular African Migrants to Europe*, October 21, 2019, <https://www.undp.org/content/dam/rba/docs/Reports/UNDP-Scaling-Fences-EN-2019.pdf>.

<sup>27</sup>Displacement due to conflict is occurring widely in Africa, with Salafi-jihadi insurgencies a key contributing factor. Wendy Williams, *Shifting Borders: Africa’s Displacement Crisis and its Security Implications*, Africa Center for Strategic Studies, October 2019, <https://reliefweb.int/sites/reliefweb.int/files/resources/ARP08EN-Shifting-Borders-Africas-Displacement-Crisis-and-Its-Implications.pdf>; and Kingsley Ighboro, “Work in Progress for Africa’s Remaining Conflict Hotspots,” *Africa Renewal* (December 2019 – March 2020), <https://www.un.org/africarenewal/magazine/december-2019-march-2020/work-progress-africa%E2%80%99s-remaining-conflict-hotspots>.

<sup>28</sup>Stephen J. Townsend, *A Secure and Stable Africa is an Enduring American Interest*, statement before the Senate Armed Services Committee, January 30, 2020, [https://www.armed-services.senate.gov/imo/media/doc/Townsend\\_01-30-20.pdf](https://www.armed-services.senate.gov/imo/media/doc/Townsend_01-30-20.pdf); and James Miller, “Al-Shabaab in East Africa,” Critical Threats Project at the American Enterprise Institute, July 24, 2014, <https://www.critical-threats.org/analysis/al-shabaab-in-east-africa>.

<sup>29</sup> Department of Defense Office of Inspector General, *Lead Inspector General for East Africa and North and West Africa Counterterrorism Operations Quarterly Report to the United States Congress (October 1, 2019, through December 31, 2019)*, February 11, 2020, <https://www.dodig.mil/reports.html/Article/2080495/lead-inspector-general-for-east-africa-and-north-and-west-africa-counterterrori/>.

<sup>30</sup> Al Qaeda in the Arabian Peninsula transferred expertise to build laptop bombs to al-Shabaab by 2016, when al-Shabaab attempted to blow up a Turkish commercial airliner. Acquisition of more advanced weaponry would most probably occur through the regional arms trafficking networks. Eric Schmitt and Abdi Latif Dahir, “Al Qaeda Branch in Somalia Threatens American in East Africa—and Even the U.S.,” *New York Times*, March 21, 2020, <https://www.nytimes.com/2020/03/21/world/africa/al-qaeda-somalia-shabab.html>; and Katherine Zimmerman, “Did al-Shabaab Get a Bomb on a Plane? Or not?” AEIdeas, February 5, 2016, <https://www.aei.org/foreign-and-defense-policy/africa/did-al-shabaab-get-a-bomb-on-a-plane-or-not/>.

<sup>31</sup> Emilia Columbo, “Supporting Mozambique’s Response to the Growing Insurgent Threat in Cabo Delgado,” Center for Strategic International Studies, April 9, 2020, <https://www.csis.org/analysis/supporting-mozambiques-response-growing-insurgent-threat-cabo-delgado>.

<sup>32</sup> The Islamic State Central Africa Province operates in the Democratic Republic of the Congo (DRC) and Mozambique, rebranding the Allied Democratic Forces (ADF) in the DRC and Ansar al Sunna (also known as al-Shabaab) in Mozambique. The exact linkages between the Islamic State leadership and these local groups are not known, though a Kenya-based Islamic State financier, Waleed Ahmed Zein, worked with the ADF. UN Security Council, *Twenty-fourth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da’esh), Al-Qaida and associated individuals and entities*, July 15, 2019, <https://undocs.org/S/2019/570>; and UN Security Council, *Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da’esh), Al-Qaida and associated individuals and entities*, January 20, 2020, <https://undocs.org/S/2020/53>; and Reuters, “Financier of Islamic State Paid Money to Rebel Group in Eastern Congo: Report,” November 18, 2018, <https://www.reuters.com/article/us-congo-security/financier-of-islamic-state-paid-money-to-rebel-group-in-eastern-congo-report-idUSKCN1NK20G>.

<sup>33</sup> Thomas Joscelyn, “Islamic State Claims Rare Attack in Algeria,” Long War Journal, November 21, 2019, <https://www.longwarjournal.org/archives/2019/11/islamic-state-claims-rare-attack-in-algeria.php>; Thomas Joscelyn, “Islamic State Loyalists Fight on in Libya,” Long War Journal, May 6, 2019, <https://www.longwarjournal.org/archives/2019/05/islamic-state-loyalists-fight-on-in-libya.php>; SITE Intelligence Group, “IS Claims Credit for Suicide Bombings in Tunisian Capital,” June 27, 2019, <https://ent.siteintelgroup.com/Statements/is-claims-credit-for-suicide-bombings-in-tunisian-capital.html>; and UN Security Council, *Twenty-fifth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da’esh), Al-Qaida and associated individuals and entities*.

<sup>34</sup> Al Qaeda and the Islamic State had cooperated in the Sahel until late spring 2020, when clashes broke out between the two groups, likely over control of trafficking routes. The Islamic State’s global media has highlighted this conflict. Katherine Zimmerman, “Salafi-jihadi Ecosystem in the Sahel,” American Enterprise Institute, April 22, 2020, <https://www.aei.org/research-products/report/salafi-jihadi-ecosystem-in-the-sahel/>; and Mina al Lami, “Africa’s Sahel Becomes latest al-Qaeda-IS Battleground,” BBC Monitoring, May 11, 2020, <https://www.bbc.com/news/world-africa-52614579>.

<sup>35</sup> Katherine Zimmerman, “Salafi-jihadi Ecosystem in the Sahel.”

<sup>36</sup> Sergey Sukhankin, “The ‘Hybrid’ Role of Russian Mercenaries, PMCs, and Irregulars in Moscow’s Scramble for Africa,” Jamestown Foundation, January 10, 2020, <https://jamestown.org/the-mercenaries-behind-russian-operations-in-africa/>.

<sup>37</sup> Stephen J. Townsend, *A Secure and Stable Africa is an Enduring American Interest*.

<sup>38</sup> Russian PMCs also worked alongside Sudanese regime troops during the 2019 uprising, though their effect on developments seems to be negligible and their exact role is unclear. Stephen J. Townsend, *A Secure and Stable Africa is an Enduring American Interest*; Tim Lister, Sebastian Shukla, and Clarissa War, “Putin’s Private Army is Trying to Increase Russia’s Influence in Africa,” CNN, August 14, 2019, <https://www.cnn.com/interactive/2019/08/africa/putins-private-army-car-intl/>; and Sergey Sukhankin, “The ‘Hybrid’ Role of Russian Mercenaries, PMCs, and Irregulars in Moscow’s Scramble for Africa.”

<sup>39</sup> Crisis Group, “China Expands its Peace and Security Footprint in Africa,” October 24, 2018, <https://www.crisisgroup.org/asia/north-east-asia/china/china-expands-its-peace-and-security-footprint-africa>.

<sup>40</sup> Minor issues related to the Chinese base have already arisen: Chinese lasers injured US military pilots in Djibouti in 2018. Paul Sonne, “U.S. Accuses China of Directing Blinding Lasers at American Military Aircraft in Djibouti,” *Washington Post*, May 4, 2018, <https://www.washingtonpost.com/news/checkpoint/wp/2018/05/03/u-s-accuses-china-of-directing-blinding-lasers-at-american-military-aircraft-in-djibouti/>.

<sup>41</sup> See, for example, Andrea Kendall-Taylor, Erica Frantz, and Joseph Write, “The Digital Dictators: How Technology Strengthens Autocracy,” *Foreign Affairs* (March/April 2020), <https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators>.

<sup>42</sup> Both the Islamic State and al Qaeda trumpet the success of their local African affiliates to bolster their image globally. Al Qaeda senior leadership has benefited from al Qaeda in the Islamic Maghreb’s finances. All of the Africa-based groups have local roots and have developed transnational ties over time as the broader Salafi-jihadi network has strengthened. For example, see Figure 4 (Islamic State Branches from the Local Salafi-jihadi Vanguard,” in Katherine Zimmerman, *Beyond Counterterrorism: Defeating the Salafi-jihadi Movement*, American Enterprise Institute, October 8, 2019, <https://www.aei.org/research-products/report/beyond-counterterrorism-defeating-the-salafi-jihadi-movement/>.

<sup>43</sup> For more, see Emily Estelle’s forthcoming essay on the relationship between extremist movements and multi-sided proxy conflicts from the Critical Threats Project at the American Enterprise Institute, “Vicious Cycle: How disruptive states facilitate and exploit the rise of extremist movements,” (working title).

<sup>44</sup> The US will develop and strengthen partnerships with African government, civil society organizations, and regional institutions to reduce conflict and promote responsive governance. Prosper Africa is an initiative to encourage US-African trade and commercial ties to safeguard African economic independence from competitors such as China and Russia (which can direct state-run and semi-private companies to invest in Africa). The US encourages African nations to take responsibility for their own peace and security and will support this effort through capacity-building programs and counterterrorism operations. It also seeks to focus US foreign assistance dollars on programs that directly support US goals, including public health and education initiatives. White House, “President Donald J. Trump’s Africa Strategy Advances Prosperity, Security, and Stability,” press release, December 13, 2018, <https://www.whitehouse.gov/briefings-statements/president-donald-j-trumps-africa-strategy-advances-prosperity-security-stability/>; Nicolas Cook and Brock

R. Williams, “The Trump Administration’s Prosper Africa Initiative,” Congressional Research Service, December 12, 2019, <https://fas.org/sgp/crs/row/IF11384.pdf>; and US Department of Commerce, “Prosper Africa,” <https://www.trade.gov/prosper-africa>.

<sup>45</sup> As of October 2019, the mission statement reads: “U.S. Africa Command, with partners, counters transnational threats and malign actors, strengthens security forces and responds to crises in order to advance U.S. national interests and promote regional security, stability and prosperity.” Prior to October 2019, the mission statement read: “U.S. Africa Command, with partners, strengthens security forces, counters transnational threats, and conducts crisis response in order to advance U.S. national interests and promote regional security, stability, and prosperity.” Information accessed through the Wayback Machine.

<sup>46</sup> These rapid-response forces include the Special Purpose Marine Air Ground Task Force-Crisis Response-Africa at Moron Air Base, Spain, and Naval Air Station Sigonella, Italy; the Crisis Response Force in Baumholder, Germany; and the East Africa Response Force at Camp Lemonnier, Djibouti.

<sup>47</sup> See AFRICOM’s data page on Theater Security Cooperation Programs: <https://www.africom.mil/what-we-do/security-cooperation>.

<sup>48</sup> See AFRICOM’s data page on its regular military exercises: <https://www.africom.mil/what-we-do/exercises>.

<sup>49</sup> Both counternarcotics and countertrafficking have connections to counterterrorism because of the nexus between illicit networks and the Salafi-jihadi movement.

<sup>50</sup> A notable exception is a special operations forces raid in Libya to capture Abu Anas al Libi in 2013.

<sup>51</sup> Anecdotal reporting on improved regard for human rights norms from US special operations forces who have worked with foreign military units. The theory is that the presence of western military advisers creates a disincentive for commanders to order troops to commit human rights abuses and incentivizes commanders to hold soldiers responsible if they do commit abuses.

<sup>52</sup> The Mozambican government has deployed forces against an Islamic State-linked insurgent group with support from a private company. Tom Bowker, “Extremists step up violence in gas-rich northern Mozambique,” Associated Press, May 15, 2020, <https://apnews.com/2cdd4a08cd90094761f899187fd694fb>.

<sup>53</sup>The US began building the Danab (Lightning) Brigade in 2013. It now has 800 to 1,000 troops, short of the objective force of 3,000. Diana Stacy Correll, “AFRICOM Predicts Mission Training Somalia’s ‘Lightning Brigade’ Will Last Until 2027,” *Military Times*, March 17, 2020, <https://www.militarytimes.com/news/your-military/2020/03/17/africom-predicts-mission-training-somalias-lightning-bridgade-will-last-until-2027/>.

<sup>54</sup>Helene Cooper, Thomas Gibbons-Neff, Charlie Savage, and Eric Schmitt, “Pentagon Eyes Africa Drawdown as First Step in Global Troop Shift,” *New York Times*, December 24, 2019, <https://www.nytimes.com/2019/12/24/world/africa/esper-troops-africa-china.html>.

<sup>55</sup>Paul D. Williams, “A Navy SEAL was Killed in Somalia. Here’s What You Need to Know about U.S. Operations There.” *Washington Post*, May 8, 2017, <https://www.washingtonpost.com/news/monkey-cage/wp/2017/05/08/a-navy-seal-was-killed-in-somalia-heres-what-you-need-to-know-about-u-s-operations-there/>.

<sup>56</sup>Thomas Gibbons-Neff, Eric Schmitt, Charlie Savage, and Helene Cooper, “Chaos as Militants Overran Airfield, Killing 3 Americans in Kenya,” *New York Times*, January 22, 2020, <https://www.nytimes.com/2020/01/22/world/africa/shabab-kenya-terrorism.html>. U.S. Africa Command, “U.S. Africa Command Investigation Update: Al Shabaab Attack in Manda Bay, Kenya,” press release, February 10, 2020, <https://www.africom.mil/pressrelease/32559/us-africa-command-investigation-update-al-sha>; and Max Bearak, “2019 saw record U.S. airstrikes in Somalia. Why is al-Shabab Surging?” *Washington Post*, January 15, 2020, [https://www.washingtonpost.com/world/africa/2019-saw-record-us-airstrikes-in-somalia-why-is-al-shabab-surging/2020/01/15/be9bc808-30c2-11ea-971b-43bec3ff9860\\_story.html](https://www.washingtonpost.com/world/africa/2019-saw-record-us-airstrikes-in-somalia-why-is-al-shabab-surging/2020/01/15/be9bc808-30c2-11ea-971b-43bec3ff9860_story.html).

<sup>57</sup>Department of Defense Office of Inspector General, *Lead Inspector General for East Africa and North and West Africa Counterterrorism Operations Quarterly Report to the United States Congress (October 1, 2019, through December 31, 2019)*; Eric Schmitt, “U.S. Military Cutting Medevac Flights for Troops in West Africa,” *New York Times*, April 18, 2020, <https://www.nytimes.com/2020/04/18/world/africa/west-africa-special-operations-medevac.html>; and Ruth Maclean, “Mali’s President Exits After Being Arrested in Military Coup,” *New York Times*, August 18, 2020, <https://www.nytimes.com/2020/08/18/world/africa/mali-mutiny-coup.html>.

<sup>58</sup>The Leahy Law prohibits the Department of Defense from providing security assistance to units believed to have committed gross human rights violations, which rightly constrains how AFRICOM can engage with certain militaries and security forces in the region.

<sup>59</sup>For a full discussion on the shortcomings of the US approach to countering Salafi-jihadi groups, see Katherine Zimmerman, *Beyond Counterterrorism: Defeating the Salafi-jihadi Movement*.

<sup>60</sup>Department of Defense Office of Inspector General, *Lead Inspector General for East Africa and North and West Africa Counterterrorism Operations Quarterly Report to the United States Congress (October 1, 2019, through December 31, 2019)*.

<sup>61</sup>US Department of Defense, “Pentagon Announces Force Optimization,” press release, November 15, 2018, <https://www.defense.gov/Newsroom/Releases/Release/Article/1691538/pentagon-announces-force-optimization/>.

<sup>62</sup>A steady stream of reporting indicates that the Blank Slate Review of AFRICOM will result in a further reduction in resources, though the review is incomplete and Secretary Esper has not yet made final decisions surrounding resources. Drawing down in Africa would follow a pattern of decisions on the force posture, including the withdrawal from Afghanistan, status of forces in Iraq (expected to be a draw down), and reduction in forces posted in Germany.

<sup>63</sup>Notably, security-sector assistance has had a positive impact when peacekeeping missions are present, which should play into calculations over which programs to sustain. Stephen Watts, “Trevor Johnston, Matthew Lane, Sean Mann, Michael J. McNerney, and Andrew Brooks, *Building Security in Africa: an Evaluation of U.S. Security Sector Assistance to Africa from the Cold War to the Present*, RAND, 2018, [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RR2400/RR2447/RAND\\_RR2447.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2400/RR2447/RAND_RR2447.pdf).

<sup>64</sup>European Parliamentary Research Service, “China’s Growing Role as a Security Actor in Africa,” August 10, 2019, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642232/EPRS\\_BRI\(2019\)642232\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642232/EPRS_BRI(2019)642232_EN.pdf); and European Parliamentary Research Service, “Russia in Africa: A New Arena for Geopolitical Competition,” November 8, 2019, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642283/EPRS\\_BRI\(2019\)642283\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642283/EPRS_BRI(2019)642283_EN.pdf).

<sup>65</sup>China has used its economic influence in Africa to leverage votes at the UN other international organizations. See David H. Shinn, “China in Africa,” statement before the US-China Economic and Security Review Commission, May 8, 2020, [https://www.uscc.gov/sites/default/files/Shinn\\_Testimony.pdf](https://www.uscc.gov/sites/default/files/Shinn_Testimony.pdf).



<sup>66</sup>Sudarsan Raghavan, “Libya’s Civil War Creates Opening for ISIS Return as Counterterrorism Effort Falters,” November 24, 2019, [https://www.washingtonpost.com/world/middle-east/libyas-civil-war-creates-opening-for-isis-return-as-counterterrorism-effort-falters/2019/11/21/e78745c0-056c-11ea-9118-25d6bd37dfb1\\_story.html](https://www.washingtonpost.com/world/middle-east/libyas-civil-war-creates-opening-for-isis-return-as-counterterrorism-effort-falters/2019/11/21/e78745c0-056c-11ea-9118-25d6bd37dfb1_story.html).

<sup>67</sup>Katherine Zimmerman, *America’s Real Enemy: The Salafi-jihadi Movement*, Critical Threats Project at the American Enterprise Institute, July 18, 2017, <https://www.criticalthreats.org/analysis/americas-real-enemy-the-salafi-jihadi-movement>.

<sup>68</sup>Al Qaeda in the Arabian Peninsula (AQAP) observed that the Saleh regime was not actively prioritizing counterterrorism operations in the late 2000s and became al Qaeda’s most capable group in terms of external attacks. Al Qaeda leadership sought to prevent AQAP from pushing for Saleh’s overthrow in 2011 for fear (and rightly so) that the next regime might focus more on counterterrorism. Al Qaeda leadership has also discussed a similar relationship with the Mauritanian government, though the government contests this. (See the declassified documents from the May 2011 raid on the Osama bin Laden compound in Abbottabad, Pakistan, for more.)

<sup>69</sup>US Embassy in Libya, “U.S. Citizen Services,” <https://ly.usembassy.gov/u-s-citizen-services/>.

<sup>70</sup>Department of Defense Office of Inspector General, *Lead Inspector General for East Africa and North and West Africa Counterterrorism Operations Quarterly Report to the United States Congress (October 1, 2019, through December 31, 2019)*.

<sup>71</sup>The Economist, “Foreign Powers are Piling into Libya,” December 12, 2019, <https://www.economist.com/middle-east-and-africa/2019/12/12/foreign-powers-are-piling-into-libya>; US Africa Command, “New Evidence of Russian Aircraft Active in Libyan Airspace,” press release, June 18, 2020, <https://www.africom.mil/pressrelease/32941/new-evidence-of-russian-aircraft-active-in-li>; and US Africa Command, “Russia Deploys Military Fighter Aircraft to Libya,” press release, May 29, 2020, <https://www.africom.mil/pressrelease/32887/russia-deploys-military-fighter-aircraft-to-l>.

<sup>72</sup>US Africa Command, “AFIRCOM Commander Reaffirms Bilateral Partnership with Tunisia,” press release, May 29, 2020, <https://www.africom.mil/pressrelease/32888/africom-commander-reaffirms-bilateral-partner>.

<sup>73</sup>Author’s conversations on trends within the command with AFRICOM personnel May 2019 in Stuttgart, Germany.

<sup>74</sup>Department of Defense Office of Inspector General, *Lead Inspector General for East Africa and North and West Africa Counterterrorism Operations Quarterly Report to the United States Congress (October 1, 2019, through December 31, 2019)*.

<sup>75</sup>Katherine Zimmerman, “Why the US should spend 0.3 percent of its defense budget to prevent an African debacle.”

<sup>76</sup>Humeyra Pamuk, “U.S. Creates New Envoy Positions to Counter Rising Terrorism in the Sahel,” Reuters, March 6, 2020, <https://www.reuters.com/article/us-usa-sahel/u-s-creates-new-envoy-position-to-counter-rising-terrorism-in-sahel-idUSKBN20T2ZJ>.

<sup>77</sup>House Armed Services Committee hearing, “National Security Challenges and U.S. Military Activities in the Greater Middle East and Africa,” March 10, 2020, <https://www.youtube.com/watch?v=fw2baHfgyOU&feature=youtu.be&t=7057>.

<sup>78</sup>Department of Defense Office of Inspector General, *Lead Inspector General for East Africa and North and West Africa Counterterrorism Operations Quarterly Report to the United States Congress (October 1, 2019, through December 31, 2019)*.

<sup>79</sup>Department of Defense Office of Inspector General, *Lead Inspector General for East Africa and North and West Africa Counterterrorism Operations Quarterly Report to the United States Congress (October 1, 2019, through December 31, 2019)*.

<sup>80</sup>Beyond the scope of this argument are questions of force modernization and acquisition, training and readiness, force size, demands on US special operations forces, and now the impact of the coronavirus pandemic, among many other considerations. Like all bureaucratic organizations, the Defense Department has legacy programs and inefficiencies and has been slow to reorient under new conditions.

<sup>81</sup>Sam Wilkins, “Does American Need an Africa Strategy?” War on the Rocks, April 2, 2020, <https://warontherocks.com/2020/04/does-america-need-an-africa-strategy/>.

<sup>82</sup>For a more detailed exposition of how to transform the US approach to combating al Qaeda, the Islamic State, and other Salafi-jihadi groups, see Katherine Zimmerman, *Beyond Counterterrorism: Defeating the Salafi-jihadi Movement*.

<sup>83</sup>Katherine Zimmerman, *America’s Real Enemy: The Salafi-jihadi Movement*.

<sup>84</sup>President Donald Trump signed the Global Fragility Act of 2019 into law as part of the 2020 Appropriations Act in December 2019. The text is available in H.R. 1865: <https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-116HR1865SA-RCP116-44.PDF>.



People's Liberation Army troops prepare for a parade in September 2017 commemorating the PLA's 90th anniversary. (Defense Intelligence Agency 2019)

# China's Strategic Objectives in a Post COVID-19 World

By Benjamin Tze Ern HO<sup>1</sup>

On 1 October 2019, the People's Republic of China (PRC) celebrated its 70th birthday, thus marking another important landmark of modern China under the leadership of the Chinese Communist Party (CCP). In commemorating the event, the Chinese government held a grand military parade with some 15,000 troops, more than 160 aircraft, and 580 active weapon systems during the event, including the latest generation nuclear missile systems such as the Dongfeng-41 mobile intercontinental ballistic missile. As the *South China Morning Post* reported, citing one insider, "the parade, which aims to showcase President Xi's achievement in military modernization and reforms in both hardware and software will carry a lot of political meaning."<sup>2</sup> Given ongoing social protests in Hong Kong and problems in western societies at that time (such as Brexit talks in the UK and political opposition to President Trump in the United States) the contrast could not have been more stark: *A powerful and prosperous China celebrates its international success while many western societies fail and flounder amidst their own domestic problems.*

Nine months on (as of writing), it would seem that the COVID-19 pandemic has levelled the international mood as far as countries are able to claim unmitigated political success. Even China, despite some success in containing the virus, was careful about portraying a celebratory front in its battle against the virus. Speaking at the National People's Congress, Premier Li Keqiang noted that, "the epidemic has not yet come to an end, while the tasks we face in promoting development are immense."<sup>3</sup> At the same time, the fact that the Chinese government had spared no efforts to narrate its road to success in curbing the virus is particularly telling: *China seeks to demonstrate that its brand of governance is superior to that of the West, and consequently, it deserves a greater say in and political influence over international affairs.*

From this vantage point, I argue that a post COVID-19 global landscape is likely to witness greater intransigence, or *hardening* of Beijing's political resolve in pursuing its national interests. In addition, given the backlash and criticism it received from some western countries (particularly the United States) over its handling of the pandemic, it has generated a siege mentality among Chinese leaders, many of whom perceive an existential struggle between Beijing and Washington with the latter seen as attempting to thwart China's rise and inhibit its international influence. This article seeks to further expand on these political motifs and

---

<sup>1</sup> Benjamin Tze Ern Ho is an assistant professor with the China Programme, Institute of Defense and Strategic Studies, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore.

how they reflect China's strategic objectives over the past six years under the leadership of President Xi. Indeed, the issue of what the PRC's long-term intentions are, and elements of its grand strategy are crucial for scholars and policymakers seeking to make sense of China's international behavior. To this end, a number of important works have emerged in the past few years providing useful clues as to what Beijing's ultimate objectives might be.<sup>4</sup> This article seeks to complement the existing works by incorporating the events of the COVID-19 pandemic so as to obtain a more realistic appraisal of China. This is important for two main reasons; one, prior to COVID-19, it can be said that China under President Xi had not faced a crisis of such magnitude and it was thus difficult to assess the extent to which the CCP could claim political legitimacy by virtue of its ability to govern China. Secondly, given worsening Sino-U.S. relations (possibly at their historical lowest since the Mao-Nixon rapprochement in 1972), the stakes for Beijing's international diplomacy and claim to international political leadership could not have been greater. As Harvard's Graham Allison observed recently, Sino-U.S. relations look set to worsen and the endgame is a "lose-lose" situation.<sup>5</sup> With this backdrop, will China's strategic objectives evince greater change or continuity with the past? How will the COVID-19 pandemic and worsening relations with the United States affect China's foreign policy calculations, and more broadly, its role and place in the world? And what kind of changes will we see within China even as the CCP continues to insist that its brand of governance remains superior to western liberal democracy?

The rest of this article will proceed as follows; I will examine five major themes that have constituted important strategic objectives under President Xi. I will then attempt to relate these objectives to the events of COVID-19 and the worsening relationship with the United States. As the article will show, the COVID-19 pandemic has emboldened the

Chinese government to consider a model of "liberalism abroad and illiberalism at home" as a means to succeed in world politics. Such an approach allows the Chinese Communist Party (CCP) to both ensure that it remains unchallenged politically at home, while at the same time proffering it the opportunity to promote a foreign policy agenda which allows it to maximize its international gains while minimizing domestic risks. Finally, I conclude that these strategic imperatives pursued by the Chinese government—if dogmatically maintained—are likely to exacerbate tensions not just between China and the United States, but also between China and countries within its neighborhood, particularly in East and Southeast Asia.

## Chinese Strategic Objectives Under Xi Jinping

### *Ensuring CCP Legitimacy*

The first, and possibly the most crucial, is the need to ensure the legitimacy of the CCP to rule China. Given Chinese leaders' criticism of western democratic systems and the problems they generate, it is incumbent upon Beijing to demonstrate that its single party, authoritarian approach to governance is superior to the West. This is easier said than done given that the party consists of more than 80 million members who are far from monolithic in their ideological worldviews and political affiliations. While Xi's centralization of political power over the last few years has greatly reduced the likelihood of political opponents challenging him for power, factional politics continue to be a mainstay of the CCP's politics, and represent a grave concern to the party.<sup>6</sup>

Given the opaque character of Chinese policymaking, it is difficult to assess the precise extent to which factions within the CCP have influenced present-day Chinese politics. Nevertheless, there are two issues worth watching; one, the views of Chinese elites towards President Trump; and two,

the amount of support for President Xi following the COVID-19 pandemic. The former relates to a key strategic aspect of Sino-U.S. relations, while the latter is intimately tied to domestic conditions such as economic growth, the availability of jobs, and the overall mood in the country.

According to a recent study by Yao Lin, many Chinese liberal intellectuals fervently idolize Donald Trump and embrace the alt-right ideologies that are espoused.<sup>7</sup> Interestingly, many of these liberal intellectuals are deeply critical of the Party-state and are committed to advocating universal values and China's liberal democratization, themes which are not usually synonymous with Trump's brand of nationalistic, American-first hubristic politics.<sup>8</sup> As observed, the "traumatizing experience of Party-State totalitarianism propels Chinese liberals on an anti-CCP pilgrimage in search for sanitized and glorified imageries of western (especially American) political realities, which nurtures both their neoliberal affinity and their proclivity for a Trumpian metamorphosis."<sup>9</sup>

Notwithstanding the problems in American (and more generally western) political life, the above study suggests a growing chorus of Chinese intellectuals who are disillusioned with China's political life and are looking to the West (even as an ideal) with which to generate solutions to the perceived problems in domestic life. While China's ongoing spat with the United States continues to generate hawkish voices from Beijing, including an aggressive Wolf Warrior diplomacy, it has also paradoxically resulted in a greater affinity for western values and ideals—seeing in them a panacea for the social maladies experienced at home.

Similarly, this growing domestic discontent has been exacerbated by the COVID-19 pandemic, and the perceived mistakes made by the CCP in its bungling response during the initial outbreak. While large-scale randomized samples of citizens' sentiments are unavailable, there are several clues that suggest that all is not rosy with the CCP

internally. For instance, during the height of the virus outbreak in Wuhan, Premier Li Keqiang—instead of President Xi himself—was sent to lead a taskforce there. While Chinese public opinion over Xi's absence is difficult to gauge (given Chinese censorship), his absence was certainly notable. As Willy Lam puts it, "he has not visited places hard hit by the virus. This has been criticized in part because Xi claims to be the core of the leadership, the all-powerful leadership . . . and he doesn't have the guts to go the epidemic-stricken areas."<sup>10</sup>

From the above, I argue that at stake is Xi's personal reputation and his ability to rally the CCP around him to ensure the ongoing legitimacy of the Party to rule China. This can only be so if Chinese leaders are able to evince that its social policies and governance have the support of the majority of the Chinese people. Due to the absence of parliamentary style elections in China, this is difficult to ascertain; hence, material prosperity and economic growth remain central to legitimizing the CCP's political rule. To this end, any slowdown of the Chinese economy would pose a challenge to the mandate of the CCP. At the 13<sup>th</sup> National People's Congress this year, the Chinese government for the first time did not set a GDP target for the economy—a sign of the Chinese government's reading that the situation inside and outside China could get worse post COVID-19.

### *Widening the International Support Base*

Under President Xi, the Belt and Road Initiative (BRI) has been a central feature of Beijing's foreign policy. While a number of elements regarding the BRI remain unclear, particularly the economic viability and sustainability of BRI projects with other countries, one objective is certain; the BRI is conceived with the intention of widening China's international support base through economic statecraft.

In this respect some modest progress has been made. The first BRI forum in May 2017 saw 29 foreign heads of state and representatives from 130

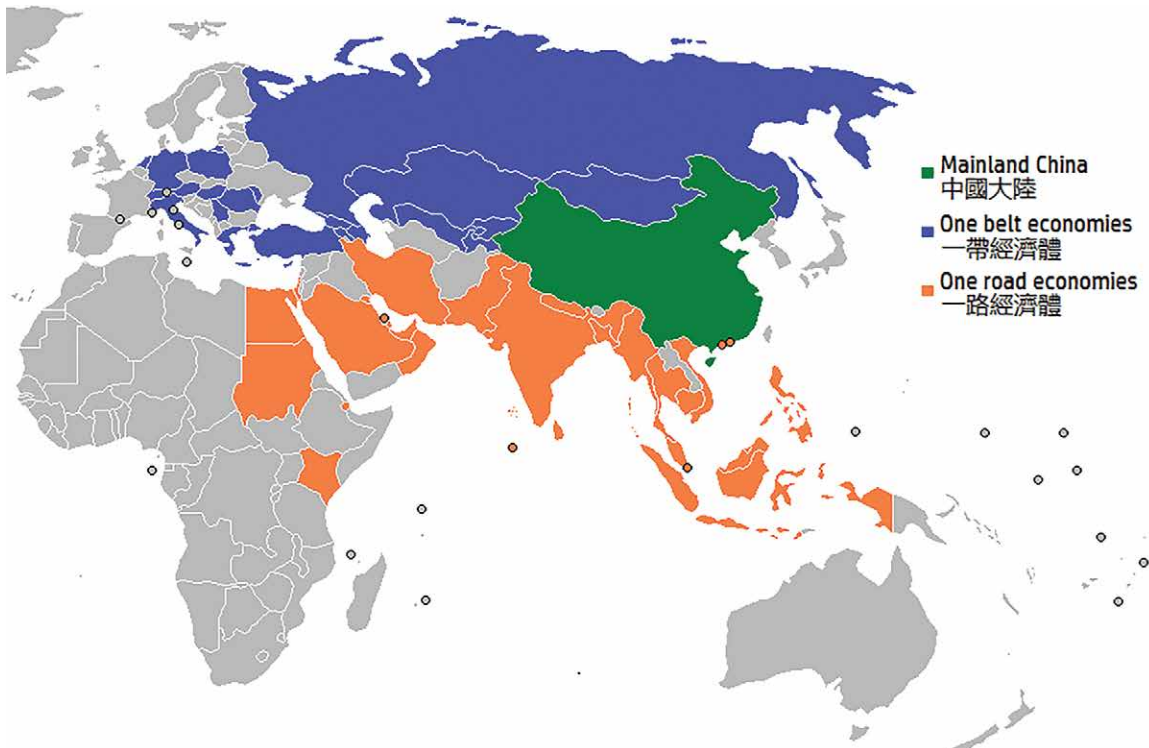
countries, while the second BRI forum in April 2019 saw an increase to 37 foreign heads of state and participation from more than 150 countries. What these numbers suggest is that China has been generally successful in using its economic statecraft to promote its political objectives. According to Baldwin, economic measures are particularly useful in helping states gain political influence for they are “likely to exert more pressure than either diplomacy or propaganda, and are less likely to evoke a violent response than military instruments.”<sup>11</sup> Seen this way, if we take economic relations between states—not as a dispassionate realm of economic activity (concerned purely with profit)—but as a derivative of wider geopolitical interests and calculations, then the political character of economic statecraft cannot be ignored.

In the case of China, the Belt and Road Initiative represents a grand strategy through

economic means;<sup>12</sup> hence, economic power is seen as a means of generating greater political influence among the countries Beijing seeks to win over into its camp. The goal of economic initiatives (like the BRI) is linked to how Chinese leaders seek to present and project Beijing’s worldview to others and to ultimately achieve China’s foreign policy and domestic goals. This “selling” of Beijing’s worldview is also closely linked to how Chinese soft power is being conceptualized and operationalized. While western iterations of soft power tend to emphasize the non-coercive aspect of soft power, and thus the stress on culture and values as instruments of soft power,<sup>13</sup> such a distinction as to whether economics ought to be seen as “hard” or “soft power” is less clear cut in China. According to one study, Chinese discourse concerning soft power is frequently expressed within its domestic context and towards



Part of China’s Belt and Road Initiative, the partially completed bridge at the Kota Batu end of the Temburong Bridge construction project in Brunei. (Peter L. Higgs)



The Belt and Road Initiative is a colossal economic trade route that is seen as a symbol of the economic dominance and ambitions of China and an example of economic superpower projection. (This file was derived from: Hong Kong Qatar Locator.png by Xxjkingdom)

domestic objectives, and also involves touting the economic success of China's development model.<sup>14</sup> Such a narrative suggests that in the Chinese mind, economic resources can be used as a source of soft power which allows China to evidence its political model and worldview to the outside world, thus rendering Beijing a model for others to emulate. This suggests that China would likely expend further efforts in the coming years to obtain greater international support for its global initiatives, especially among western countries that possess strong relations with the United States, such as the United Kingdom, Australia, and Canada.

This promotion of its international support base is also most clearly evidenced during the COVID-19 pandemic when China—following outbreaks in Europe and other parts of the world—embarked on a “mask diplomacy” in an attempt to convey its

narrative of acting as a responsible global stakeholder.<sup>15</sup> Under these auspices, Chinese public and private institutions donated masks, test kits, and other personal protection equipment to some 83 countries hard hit by the coronavirus, including European countries like Italy, Czech Republic, and Serbia, as well as several in the Middle East and Africa. According to Deputy Foreign Minister Luo Zhaohui, Beijing had done so because “China empathizes and is willing to offer what we can to countries in need,” and that it also wants to share its experience of fighting the pandemic with the rest of the world.<sup>16</sup> This demonstration of solidarity I argue is done with the goal of generating greater international goodwill and to portray China as an exceptional country, and that its political governance is different and better than the West (particularly the United States).

### *Increase International Isolation of Taiwan*

The issue of the Republic of China (ROC-Taiwan) remains a core national interest and one which no Chinese leader can be seen to make any compromise over. To this end, China—under President Xi—has been highly successful in the past few years. In 2013, Taiwan had official diplomatic relations with 22 UN member states: This number has now dwindled to 14 UN member states, with five losses coming in the past year, and two within a week in September (Solomon Islands and Kiribati). While most of these countries are small Pacific and Oceanic states and are not considered major political players internationally, their strategic locations in key maritime waters proffer Beijing increased opportunities to project international visibility while further eroding Taipei's international presence and voice.

In the coming years, it is likely that China will further intensify international pressure on Taiwan. Indeed the COVID-19 pandemic has generated significant cross-Straits dynamics suggesting that despite the Chinese government's formidable propaganda machinery, the ROC continues to present a considerable thorn in the flesh of the CCP's international branding and soft power stature. Given this backdrop of diplomatic competition, it was not surprising that both the PRC and ROC governments have been highly sensitive to each other's political maneuvers during the pandemic. This was particularly so given Taipei's considerable efforts and success in combating the virus resulting in international praise and accolades which were sharply contrasted with Beijing's early problems and subsequent criticism by a number of western countries (especially the United States). This "diplomatic tug of war"—as one study puts it—pitches both the PRC and ROC in a tussle for recognition as the representative state of "China" in international society.<sup>17</sup> As such, one might argue that both governments are involved in a "one-up game" of political brinkmanship, each trying to outdo the other in procuring

international social capital and the moral high ground to be recognized as a responsible stakeholder. There are however, some subtle differences in each countries' diplomatic messaging, as evinced by their subsequent mask diplomacy.

In early April the Chinese government offered face masks to Chinese citizens living or working in Singapore, in part to assuage concerns among its citizens there as infections in the city-state witnessed a sharp spike. This was a highly unusual move given that only Chinese citizens were given face masks (as the masks were given out at the Chinese Embassy) and the Chinese Embassy had also activated a number of its organizational contacts in Singapore to help with the mask outreach.<sup>18</sup> In addition, China's Ambassador Hong Xiaoyong also visited institutions with a high enrollment of Chinese students, including both secondary and tertiary schools. Given the lack of local reporting and the absence of official participation (on the Singaporean side), one can assume that these actions were done in a private capacity (with the tacit acknowledgement of and permission from the Singapore authorities). Shortly after this, Taiwan donated some 100,000 masks to Singapore through its Red Cross as part of Taiwan's Foreign Affairs Ministry initiative to donate 10 million masks worldwide to countries affected by the pandemic. Unlike Beijing's masks, Taipei's donation was not targeted only at its own citizens but at the broader population.<sup>19</sup> While such a donation was not part of any official diplomatic arrangements, the fact that the Prime Minister's wife expressed her gratitude to Taiwan on social media suggested that such a move was not purely a private matter, but that it had also received acknowledgement at the highest levels, even though it was not carried by the local mainstream media.<sup>20</sup> Two weeks later, China donated 600,000 masks to Singapore, an event which had representatives from both the diplomatic and political communities present.<sup>21</sup>



From the above events, I argue that the health pandemic has generated an international competition “to do good” between the PRC and ROC governments. In the case of China however, there exists a more “nationalistic” character to its deeds in which the needs of “Chinese citizens” were accorded greater emphasis and importance compared to other citizens, whereas the Taiwanese government offered its international aid within a more universal, less-selective framework.

How is this significant, and are we reading too much into such diplomatic gestures? The answer is both yes and no. To be fair, given the widespread presence of Chinese citizens it was natural that the Chinese government extended its diplomatic support to them, much in the same way many countries worldwide activated repatriation flights for their citizens during the early stages of the outbreak. But what was notable about the mask diplomacy was its emphasis on “us-them” in its initial outreach, and that Chinese citizens ought to be accorded “special privileges” or were entitled to certain benefits that go beyond what ordinary citizens in their host countries receive. This runs against diplomatic protocol (especially if a country’s ambassador is involved) and is suggestive of a broader Chinese attempt to generate influence beyond traditional diplomatic channels.<sup>22</sup> From this, it can be construed that China’s international “good deeds” are framed with a more narrow nationalistic objective in mind—a sharp contrast to the paradigm of “not letting your left hand know what your right hand is doing.”<sup>23</sup> Furthermore these actions are trained predominantly for a domestic audience, more so than the ROC, especially given the fact that many Chinese people—as observed by Singapore’s Kausikan—“understood their leaders had bungled the initial response to the outbreak in Wuhan [and] that the people bore the brunt of the mistakes and the drastic responses needed to recover from them.” Furthermore, “tightened censorship and the laudatory tone describing President Xi Jinping’s role in the

people’s struggle against COVID-19 suggests that the CCP is still insecure that it has put its mistakes to rest.”<sup>24</sup> To this end, I argue that the diplomatic efforts made by the Chinese government to showcase its contributions overseas are reflective of the attempt by the CCP to reframe the domestic narrative of the outbreak and to emphasize the Chinese state’s sparing no efforts to protect the well-being of its citizens.

### *Negate U.S. Influence in East Asia*

In the minds of many Chinese leaders and political observers, the presence of the United States in East Asia remains the biggest obstacle to China’s future prosperity and ability to project power regionally and internationally. According to Aaron Friedberg, the ultimate aim of Chinese policymakers is to win without fighting and to displace the United States as the leading power in Asia while avoiding direct confrontation.<sup>25</sup> Indeed it has been pointed out that part of China’s assertive international behavior is due in part as a result of the United States’ “pivot to Asia” strategy begun during the Obama administration, which in the eyes of Chinese observers represents a fundamental decision by Washington policymakers to contain China in order to preserve U.S. international primacy and global leadership.<sup>26</sup> Likewise the idea of a “free and open Indo-Pacific” is also viewed by the Chinese as a means to contain China’s development and ensure American international dominance.<sup>27</sup> Indeed Chinese paranoia towards the United States has intensified over the past five years, particularly following the 2017 publication of the National Security Strategy of the United States and the 2018 National Defense Strategy, both of which singled out China as America’s primary strategic competitor. As a response the 2019 Chinese White Paper summarized the overall character of the U.S. defense efforts by declaring that;

International strategic competition is on the rise. The US has adjusted its national security and defense strategies, and

adopted unilateral policies. It has provoked and intensified competition among major countries, significantly increased its defense expenditure, pushed for additional capacity in nuclear, outer space, cyber and missile defense, and undermined global strategic stability. NATO has continued its enlargement, stepped up military deployment in Central and Eastern Europe, and conducted frequent military exercises.<sup>28</sup>

From the above, China perceives a post COVID-19 world as one which will witness a shift in international power away from the West (and the United States) to Asia, and in which China is well-placed to assume a prominent position. To be certain this idea was already in circulation among Chinese policy circles, given President Xi's exhortation in 2014 of an "Asia for Asians" security cooperation structure,<sup>29</sup> and popular iterations by a number of global public intellectuals, such as Hugh White's *The China Choice* (2013), and more notably former Singapore diplomat Kishore Mahbubani's books *Has the West Lost It* (2018) and *Has China Won* (2020). What all these works hint at—in practice—is that leaders and policymakers should be prepared to confront a new international reality wherein American primacy is substantially diminished and China's influence increased. As such, it is likely that China would continue to take steps, militarily, economically and politically to further erode American presence in East Asia and Southeast Asia. All these would have significant repercussions for countries in the region, particularly in Southeast Asia where member states have traditionally practiced strategic hedging as a middle ground to navigate the complexities of great power competition between China and the United States. As observed by one Malaysian analyst of China's regional actions, "indeed, China's increasingly multifaceted maritime opportunism and coercive

presence in the disputed waters (of the South China Sea), even during the coronavirus crisis, has further deepened the weaker states' suspicions of its long-term intentions. Its increasing use of coercive means to prevent and obstruct the claimant countries' oil and gas exploration activities, together with the lack of progress on the COC (Code of Conduct) after years-long talks, further frustrated the smaller states in the region."<sup>30</sup> In other words, China's current course of actions is likely to aggravate smaller countries in Southeast Asia, a number of which are likely to pursue other institutional mechanisms (with or without the United States) to safeguard their interests that are seen to be threatened by a more assertive Chinese posture.

### *Global Rules and International Order*

It is generally perceived by Chinese leaders and political observers that the rules of the international order were made so as to preserve the interests of the West.<sup>31</sup> Given the ongoing and lively debate among western scholars over the sustainability and longevity of the existing liberal global order,<sup>32</sup> the search for alternative arrangements and theoretical frameworks to account for changes in the international system has been an intellectual holy grail of sorts for international relations scholars, both in and outside the West.<sup>33</sup>

From this vantage point, China is seen as being the flag-bearer of such a new system and one which possesses the deepest resources with which to challenge American dominance. Indeed, China's presence is ubiquitous in most if not all major global institutions and forums and Chinese representatives are now far more vocal in stating and arguing Chinese demands and interests where they arise. Furthermore, as exemplified by President Xi's proclamation of the Chinese dream and his vision of the rejuvenation of China, a far more confident China (as compared to the past) is now being portrayed on the international stage.

As such, it is likely that we will see in the coming years greater efforts by Chinese leaders and policymakers to shape international discourse about the overall distribution of global power and the rules of international order, including more assertive behavior in its foreign policy. As observed by a number of international scholars, the past decade has witnessed considerable Chinese intransigence on what it deems its core national interests, particularly in matters relating to territorial sovereignty as well as having greater say regarding the global order.<sup>34</sup> Indeed, China's Foreign Minister Wang Yi describes China's global role as one of being a "participant, facilitator and contributor,"<sup>35</sup> while Yan Xuetong writes of China as moving "from keeping a low profile to striving for achievement."<sup>36</sup>

In a study of the Chinese vision of international order, Wu Xinbo suggests that what China aspires to is a liberal partnership order including emphasizing a series of ideas such as openness, inclusiveness, cooperation, diversity, equality, multilateral institutions and rules.<sup>37</sup> Ironically, these ideas suggested by Wu are precisely the same characteristics that are often held up to be an indicator of a liberal state. If so, it would seem that China, at least where *its foreign policy is concerned, seeks to affiliate itself with patterns of international liberalism while retaining an illiberal edge to its domestic governance.*<sup>38</sup> The COVID-19 pandemic will have further convinced the Chinese government that "liberalism abroad and illiberalism at home" is the means to success in international politics. Put in practical terms, this would mean that the Chinese government is likely to express enthusiasm for international initiatives and global actions so long as these are not seen to impinge directly on its domestic front behind which it seeks to exercise absolute sovereignty. This is seen as a win-win situation for it allows the Chinese government the opportunity to obtain skills and the technical know-how to further strengthen its domestic governance while at the same time

ensuring that it is able to limit external threats to its political rule and to demonize those it views as hostile threats. Indeed, China's criticism of the United States during the pandemic includes a not-too-subtle dig at the American political system as a failure for its inability to control the virus spread within the United States, and consequently to be blamed for the worldwide explosion of the virus transmission. In a May 2020 *Global Times* article, it was said that, "Washington is widely believed to have failed its own people and the world as the country has about 4 percent of the global population, but now accounts for one-third of all cases worldwide and nearly 30 percent of the overall death toll."<sup>39</sup> This scapegoating of the United States reflects a popular mindset at work in Chinese political circles, that the *West is culpable for the problems of the world*, while China—notwithstanding its own domestic problems—is attempting to do good and thus ought to be acknowledged by the world as such.

## Conclusion

As of writing, many scholars are raising the specter of what a post COVID-19 future will be like. Related to this is the question of China's global influence and the extent to which the pandemic has amplified or diminished Beijing's international standing. As this article has argued, these five objectives—constituting core elements of China's grand strategy—are likely to be pursued, and with greater determination particularly given the sense of crisis engendered within the CCP as a result of the global pandemic. To this end, I argue that out of the above five objectives, it is likely that the Chinese government will be most sensitive to those which it considers as challenging its domestic stability and political legitimacy. The centrality of the CCP must remain paramount and any attempt to challenge or modify this (be it from domestic sources or from outside China) will result in a strong Chinese political response. At the same time, given the challenges



Taipei skyline view in 2020. The global pandemic is likely to harden Beijing's positions on matters of party legitimacy and national sovereignty, such as over Taiwan. (Credit: 毛貓大少爺 from Taipei, Taiwan)

faced by many western countries (in particular the United States) during the ongoing pandemic, the possibility of shifting postures towards China in a post-pandemic world (when that happens) cannot be ruled out. As such, one might argue that the Chinese government might adjust its policies—so long as they do not impinge on its domestic control—in response to how other countries react.

As recent examples of China's wolf diplomacy have illustrated, China's political leaders and the foreign policy community perceive a heightened western united front to undermine China's political system and constrain Beijing's rise. As a result, over the next one to three years—barring any political upheaval within the CCP—we are likely to see a

hardening of Beijing's resolve in its international behavior and the development of a siege mentality in response to the West. This would result in greater assertiveness in China's international posture, particularly in issues that it considers as core interests, such as territorial matters and the CCP's political rule. Already the Chinese government has demonstrated its willingness to sustain its diplomatic offensive amidst the coronavirus pandemic, as evidenced by its decision to enact the Hong Kong national security law, clashing with India over border disputes, and challenging other claimant states in the South China Sea. Consequently, China is unlikely to acquiesce to any external threats and challenges posed by other countries. Any attempt to make some sort of

diplomatic bargain with Beijing will be on Chinese terms and from a Chinese position of strength. Will it succeed in doing so, and are we to expect countries to play exactly the way Beijing wants? In the author's view, this is not a given, particularly if the Chinese authoritarian system continues to be perceived as an unattractive model of political governance. Moreover, China's domestic institutions and internal political dynamics will also pose problems for the Chinese government, especially if the COVID-19 pandemic results in a sustained economic downturn, thus undermining the CCP's fragile social compact with its people.<sup>40</sup> All these would have significant repercussions for China's international and domestic politics. In a post COVID-19 era, as China continues to seek greater prestige, status, and influence on the world stage, it is also likely to be more paranoid, sensitive, and susceptible to external forces on its domestic front. PRISM

## Endnotes

<sup>1</sup> The author can be contacted at [isteho@ntu.edu.sg](mailto:isteho@ntu.edu.sg).

<sup>2</sup> Chan, Minnie. "China says national day military parade won't disappoint in scale or advanced weapons," *South China Morning Post*, September 24, 2019 <https://www.scmp.com/news/china/military/article/3030206/china-says-national-day-military-parade-wont-disappoint-scale> (retrieved June 10, 2020).

<sup>3</sup> "Full text: Premier Li's speech at the third session of the 13th NPC," <https://news.cgtn.com/news/2020-05-22/Full-text-Premier-Li-s-speech-at-the-third-session-of-the-13th-NPC-QHaP1FpB8k/index.html> (retrieved June 10, 2020).

<sup>4</sup> See for instance, Brown, Kerry. *China's Dream : the Culture of Chinese Communism and the Secret Sources of Its Power*. Cambridge: Polity, 2018; Shambaugh, David L. *China's Future*. Cambridge: Polity, 2016; Gore, Lance, and Zheng Yongnian. *China Entering the Xi Jinping Era*. Abingdon, Oxon: Routledge, 2015.

<sup>5</sup> Lee, Yen Nee. "Endgame of U.S.-China rivalry is lose-lose, says Harvard professor", *CNBC*, May 26, 2020 <https://www.cnn.com/2020/05/26/endgame-of-us-china-rivalry-is-lose-lose-says-harvard-professor.html> (retrieved June 10, 2020).

<sup>6</sup> For existing studies into Chinese factional politics, see Li, Cheng. *Chinese Politics in the Xi Jinping Era : Reassessing Collective Leadership* Washington, D.C: Brookings Institution Press, 2016; Huang, Jing. *Factionalism in Chinese Communist Politics* Cambridge: Cambridge University Press, 2000.

<sup>7</sup> Lin, Yao. "Beaconism and the Trumpian Metamorphosis of Chinese Liberal Thinkers." *Journal of Contemporary China* (published May 18, 2020), DOI: 10.1080/10670564.2020.1766911.

<sup>8</sup> *Ibid.*, 2.

<sup>9</sup> *Ibid.*, 4.

<sup>10</sup> Kuo, Lily. "Taking credit, <https://www.theguardian.com/world/2020/feb/04/blame-xi-jinping-absence-coronavirus-frontline-china-crisis>, (retrieved June 10, 2020).

<sup>11</sup> Baldwin, David A. *Economic Statecraft*. Princeton, N.J.: Princeton University Press, 1985, p.110.

<sup>12</sup> For existing discussions of Chinese grand strategy, see Friedberg, Aaron L. "Globalisation and Chinese Grand Strategy." *Survival* 60, no. 1 (2018): 7-40; Ma, Lian. «Thinking of China's Grand Strategy: Chinese Perspectives.» *International Relations of the Asia-Pacific* 13, no. 1 (2013): 155-68.

<sup>13</sup> This line of thought is most popularly captured in the ideas of Joseph Nye's discussion of soft power. See, Nye, Joseph S. *Soft Power : The Means to Success in World Politics*. New York: Public Affairs, 2004.

<sup>14</sup> Li, Mingjiang. "China Debates Soft Power." *Chinese Journal of International Politics* 2, no. 2 (2008): 287-308.

<sup>15</sup> For further elaboration of the idea of China as a responsible stakeholder, see, Hoo, Tiang Boon. *China's Global Identity: Considering the Responsibilities of Great Power*. Washington, DC: Georgetown University Press, 2018.

<sup>16</sup> Zhou, Laura. "Coronavirus: why China's mask diplomacy is raising concerns in the West." *South China Morning Post*, March 28, 2020, <https://www.scmp.com/news/china/diplomacy/article/3077333/coronavirus-why-chinas-mask-diplomacy-raising-concern-west> (retrieved May 12, 2020).

<sup>17</sup> Hoo, Tiang Boon and Charles Andy. "China and Lilliputians: Small States in a Big Power's Evolving Foreign Policy." *Asian Security*, 13,2 (2017): 116-131, see 125.

<sup>18</sup> Sim, Dewey. "Coronavirus: Beijing offers Chinese nationals in Singapore face masks and support amid crisis." *South China Morning Post*, April 9, 2020, <https://www.scmp.com/week-asia/health-environment/article/3079055/coronavirus-beijing-offers-chinese-nationals-singapore> (retrieved May 18, 2020).

<sup>19</sup> Everington, Keoni. Taiwan's donation of 100,000 masks arrive in Singapore. Taiwan News, April 23, 2020, <https://www.taiwannews.com.tw/en/news/3921380> (retrieved May 18, 2020).

<sup>20</sup> There was social media speculation over the Prime Minister's wife's real feelings towards Taiwan as evidenced by a cryptic social media post she had posted regarding the Taiwanese mask donation and whether the Taiwanese government had indeed restricted Singapore from obtaining masks from its supplier in Taiwan earlier.

<sup>21</sup> See, Yong, Clement. "Coronavirus: China donates 600,000 masks to Singapore." Straits Times, May 5, 2020, <https://www.straitstimes.com/singapore/coronavirus-china-donates-600000-masks-to-singapore> (retrieved May 18, 2020).

<sup>22</sup> To this end, Singapore former top diplomat Bilahari Kausikan had highlighted against Beijing's attempts to impose its own state identity on Singapore including the use of information campaigns/operations to influence the Singapore identity. See Kausikan, Bilahari. *China is Messing with Your Mind*. Singapore: Epigram Books, 2019.

<sup>23</sup> Certainly a cynic could still insist that everything in international politics is rationally calculated and designed to serve a political purpose. I suppose this argument can be maintained and I do not disagree. However just because one might envisage a political objective in certain actions does not mean that all diplomatic actions are equally narrowly defined.

<sup>24</sup> Kausikan, Bilahari. "No, China will not get away with rewriting history." Nikkei Asian Review, March 30, 2020, <http://asia.nikkei.com/remotexs.ntu.edu.sg/Opinion/No-China-will-not-get-away-with-rewriting-history> (retrieved May 19, 2020).

<sup>25</sup> Friedberg, Aaron L. *A Contest for Supremacy: China, America, and the Struggle for Mastery in Asia* 1st ed. New York: W. W. Norton & Co., 2011.

<sup>26</sup> Zheng, Yongnian, Gang Chen, and Liang Fook Lye. *China's Foreign Policy in 2012: Responding to the US Pivot to Asia and Territorial Disputes with Neighbours* Singapore: East Asian Institute, National University of Singapore, 2012; Zhou, Fangyin. "Between Assertiveness and Self-Restraint: Understanding China's South China Sea policy." *International Affairs* 92, no. 4 (July 1, 2016): 869–890; Zhu, Zhiqun. *The US "Pivot" to Asia and Its Impact on US-China Relations* Singapore: East Asian Institute, National University of Singapore, 2012.

<sup>27</sup> Chen, Fangming. "Reviewing the Indo-Pacific strategy of the Trump administration." *International Strategic Studies* 132, no.1 (March 2019): 114-123; see also, He, Kai and Mingjiang Li. "Understanding the dynamics of the Indo-Pacific: US-China strategic competition, regional actors, and beyond." *International Affairs* Volume 96, Issue 1 (2020): 1-7.

<sup>28</sup> The State Council Information Office of the People's Republic of China. *China's National Defense in a New Era*. Beijing: Foreign Languages Press, 2019, p.3.

<sup>29</sup> Jakobson, Linda. "Reflections From China on Xi Jinping's "Asia for Asians"." *Asian Politics & Policy* 8, no. 1 (2016): 219-23.

<sup>30</sup> Kuik, Cheng-Chwee. "Hedging in post-pandemic Asia: What, How, and Why?" *The Asan Forum*, June 6, 2020, <http://www.theasanforum.org/hedging-in-post-pandemic-asia-what-how-and-why/> (retrieved June 18, 2020). For recent discussions on China's relations with Southeast Asia neighbors, see also, Choong, William. "Smaller countries in the Asia-Pacific: Mired in the Middling Middle." *ISEAS Commentary* 2020/90, July 3, 2020, <https://www.iseas.edu.sg/media/commentaries/smaller-countries-in-the-asia-pacific-mired-in-the-middling-middle/> (retrieved July 7, 2020); Marston, Hunter. "The COVID-19 pandemic pulls at the seams of Southeast Asia." *East Asia Forum*, May 9, 2020, <https://www.eastasiaforum.org/2020/05/09/the-COVID-19-pandemic-pulls-at-the-seams-of-southeast-asia/> (retrieved July 7, 2020).

<sup>31</sup> Deng, Yong. "Hegemon on the Offensive: Chinese Perspectives on U.S. Global Strategy." *Political Science Quarterly* 116, no. 3 (September 22, 2001): 343–365; Yan, Xuetong. "Chinese values vs. liberalism: what ideology will shape the international normative order." *Chinese Journal of International Politics* Vol 11, no.1, Spring (2018): 1-22.

<sup>32</sup> See, Ikenberry, G. John. *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order*. Princeton, NJ: Princeton University Press, 2011, and Mearsheimer, John J. *The Great Delusion: Liberal Dreams and International Realities*. New Haven, CT: Yale University Press, 2018 for two contrasting visions.

<sup>33</sup>Some examples include Amitav Acharya and Barry Buzan, Chih-yu Shih and Qin Yaqing. See, Acharya, Amitav. *The End of American World Order* Second edition. Cambridge: Polity Press, 2018; Behera, Navnita Chadha., Amitav Acharya, and Barry Buzan. "Looking for 'the International' Beyond the West." *Third World Quarterly*, Vol. 31, no. 5, July, 2010, 817-828; Shih, Chihi-yu. *Sinicizing International Relations : Self, Civilization, and Intellectual Politics in Subaltern East Asia* First edition. New York, NY: Palgrave Macmillan, 2013; Qin, Yaqing. *A Relational Theory of World Politics* Cambridge: Cambridge University Press, 2018.

<sup>34</sup>Friedberg, Aaron L. *A Contest for Supremacy : China, America, and the Struggle for Mastery in Asia* 1st ed. New York: W. W. Norton & Co., 2011; Liao, Nien-Chung Chang. "The Sources of China's Assertiveness: The System, Domestic Politics or Leadership Preferences?" *International Affairs* 92, no. 4 (2016): 817-33; He, Kai, and Huiyun Feng. «Debating China's Assertiveness: Taking China's Power and Interests Seriously.» *International Politics* 49, no. 5 (2012): 633-44.

<sup>35</sup>Wang, Yi. "China's role in the global and regional order: participant, facilitator and contributor", speech at Fourth World Peace Forum, Beijing, June 27, 2015, [https://www.fmprc.gov.cn/mfa\\_eng/wjb\\_663304/wjbz\\_663308/2461\\_663310/t1276595.shtml](https://www.fmprc.gov.cn/mfa_eng/wjb_663304/wjbz_663308/2461_663310/t1276595.shtml) (retrieved January 15, 2020).

<sup>36</sup>Yan, Xuetong. "From keeping a low profile to striving for achievement." *Chinese Journal of International Politics* 7:2 (2014): 153-184.

<sup>37</sup>Wu, Xinbo. "China in Search of a Liberal Partnership International Order." *International Affairs* 94, no. 5 (2018): 995-1018, see 1007.

<sup>38</sup>For a more in-depth analysis into liberal internationalism, see Beate, Jahn. "Liberal internationalism: historical trajectory and current prospects." *International Affairs* 94, 1 (2018): 43-61.

<sup>39</sup>Chen, Qingqing and Shumei Leng. "US owes world an explanation on COVID-19." *Global Times*, May 6, 2020 <https://www.globaltimes.cn/content/1187598.shtml> (retrieved June 19, 2020).

<sup>40</sup>See for instance, Shirk, Susan L. *China Fragile Superpower*. New York: Oxford University Press, 2007.



ZAMBATT V, the fifth iteration of troops from the country of Zambia to go in support of the United Nation's Multidimensional Stabilization Mission in the Central African Republic (MINUSCA), spent more than six weeks working with U.S., U.K., and French partners training and preparing for their mission to CAR." (MC2 (SW/AW) Evan Parker)



# International Competition to Provide Security Force Assistance in Africa

## Civil-Military Relations Matter<sup>1</sup>

By Jahara Matissek

Western states increasingly tackle the problem of state fragility in Africa through the delivery of security force assistance (SFA). What is SFA and why does it matter? Broadly speaking, SFA is a term used to describe the provision of military aid, advisors, and resources to a fragile state, so that the armed forces of that state can provide security in support of stability. SFA typically consists of the deployment of small numbers of military advisors and resources to a fragile or weak state to build effective armed forces.<sup>2</sup> However, such efforts are often overly technical and rarely address the political and institutional problems that create insecurity and the fragmented security organizations of that state (e.g. police, military, intelligence, etc.). Worse, in some cases, such SFA has only created the veneer of military effectiveness, known as the *Fabergé Egg* army problem; an expensively built military, but easily broken by insurgents.<sup>3</sup>

The western approach to SFA is codified in NATO doctrine, specifically Allied Joint Publication (AJP) 3.16 *Security Force Assistance*. The United States has created an organizational structure for SFA through the establishment of Security Force Assistance Brigades (SFAB). Providing SFA to weak states is an expensive endeavor, especially as done by the United States. Since 2001, the United States has provided over \$9 billion to Sub-Saharan African (SSA) countries and about \$25 billion to the five North African states.<sup>4</sup> Similarly, the European Union (EU) through its Common Security and Defence Policy (CSDP) has been spending over €100 million per year on five EU missions in Africa. Specifically, the EU is conducting civilian/political missions in Libya (2013-Present) and Niger (2012-Present), a blend of military and civilian/political training missions in Mali (2013-Present) and Somalia (2010-Present), and a pure military mission in the Central Africa Republic (2016-Present). These EU missions have cost, on average, \$10-30 million a year. Though a drop in the bucket compared to U.S. SFA efforts, the logic has been to stymie the growth of insurgency and terrorism throughout Africa.

Addressing state fragility through SFA has become popular with political leaders in many western capitals who see state weakness as conducive to insurgency, terrorism, and state collapse.<sup>5</sup> They fear the spillover from an influx of refugees coming to Europe as well as in more stable neighboring African states. Greece and Italy for example have experienced domestic turmoil and traumatic shifts (and increases) in political extremism, while the welfare systems of Botswana and South Africa are being stretched to and beyond the limit.<sup>6</sup> The

---

Dr. Jahara 'FRANKY' Matissek (Lt Col, U.S. Air Force) is an Assistant Professor, Military and Strategic Studies Department, and the Director of Research, Center for Air Power Studies, at the U.S. Air Force Academy.

*This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-20-1-0277.*

current problems of insecurity and mass migration emanating from Latin America are leading to a similar refugee crisis that has become a highly polarized and politicized issue in the United States.<sup>7</sup>

Despite the desire to provide safety and security—whatever their strategic intent might be—western SFA efforts are struggling to produce lasting outcomes in many African states (e.g. Mali, South Sudan, Somalia, etc.). Most of the failures stem from an inability to adapt assistance to the local context of civil-military relations (CMR) in each country. Contextually dependent CMR dictate how the army, police, and intelligence agencies are structured and manned. Such security architectures and the relationship to political and societal elites determine the sorts of informal relations that exist—and how much power and agency each security institution has. However, many political and military leaders in western capitals advance a technically oriented SFA approach because it is a low-risk foreign policy with the appearance of “doing something,” while committing few “boots on the ground.” Such western SFA attempts typically lack the necessary nuance because they fail to recognize the reality and actual practice of politics in a fragile state.<sup>8</sup> This failure obscures many of the structural problems leading to instability throughout Africa, especially in the Sahel where climate change collides with transnational organizational crime, economic deprivation, and political and social iniquities producing perpetual civil war dynamics.<sup>9</sup>

Great power competition further complicates matters in Africa, as China and Russia are increasingly contesting the space by providing their own economic and military aid. Such competition is occurring within a globalized economy, with a high premium on acquiring access to new consumer markets and extracting precious minerals and natural resources. According to a retired U.S. Army General, with prior foreign area officer experience in security cooperation, China and Russia conduct military aid and assistance missions for “real hard-nose politics in

pursuit of their own selfish strategic interests.” On the other hand, he contended, most U.S. military aid and advise and assist missions to African countries are for “altruistic purposes,” from improving humanitarian capabilities of African militaries, to pandemic and disaster response (e.g. Ebola, floods, etc.), to improving warfighting capability against local and regional threats (e.g. insurgents, terrorists, etc.).<sup>10</sup>

While some might rightly be skeptical of America’s altruistic intentions in Africa, one cannot ignore the reality that China, Russia, and America—and the West more broadly—present different visions for the world, to include how a state should govern and treat its citizens.<sup>11</sup> Chinese activity in Africa appears part of a grand strategy of creating a global Belt and Road Initiative, which ties Africa (and other regions) ever-closer to Beijing.<sup>12</sup> This may explain why China embraces a “comprehensive approach” to Africa, “blending trade and investment deals and cultural exchanges with arms sales, medical assistance, troops training, anti-piracy drills, and other programs.”<sup>13</sup> Russia sees opportunities for re-establishing its presence and for selling arms. While the Trump Administration lacks any clear strategy for engaging Africa and advocates “America First,” China and Russia are making inroads on the continent and in international perception.<sup>14</sup>

The question remains though; what can the West actually achieve in Africa by building host-nation military capacity (i.e. SFA) in a way that does not lead to praetorianism and other military pathologies that corrupt governance and undermine legitimacy? Moreover, can SFA facilitate democracy and human rights, and shift African countries away from authoritarianism? To answer these questions, let us consider a recently assembled multinational fighting force in the Sahel, to consider the limits of SFA and how it can be improved. Based on a contextually informed understanding of civil-military relations we can escape traditional notions of military effectiveness and better grasp the challenges of stabilization and

peacebuilding in a weak state. This would inform how the West and its partners provide military aid, assistance, and training to weak, fragile, and conflict-prone states. Success with SFA in such difficult environments requires a restructuring of the way core issues are handled by various elites.

### A G5 “Pipedream” in the Sahel?

Created by regional leaders in 2014, the G5 Sahel Joint Force was established, “as a way of taking their security into their own hands and encouraging regional development by coordinating their efforts.” Joint military operations—comprised of army personnel from Burkina Faso, Chad, Mali, Mauritania, and Niger—were initiated in 2017.<sup>15</sup> The force, expected to consist of 10,000 personnel in the near-term, has been primarily dedicated to counterterrorism (CT) operations in the Lake Chad Basin (LCB) area of Burkina Faso, Mali, and Niger. However, the overly CT-focused approach has depoliticized adversaries by labeling them as terrorists, instead of treating them as rational actors using violence to achieve certain political goals (e.g. patronage, economic rents, autonomy, etc.).<sup>16</sup> Such CT operations overlook local context and the ways in which elites conduct politics in the LCB region.

In conducting its CT mission, the G5 Sahel Joint Force often ignores the reasons some engage in criminality, insurgency, and terrorism. Underdevelopment and lack of opportunity motivate some, while weak state institutions make it easier for international terrorist and transnational criminal networks to operate and profit in these “stateless” areas.<sup>17</sup> Moreover, communal violence between various ethnic groups and identities has spiraled out of control, especially in Mali and Niger, with back-and-forth massacres perpetrated by different tribes; and the anarchy is compounded by a substantial increase in highly successful insurgent attacks and ambushes against G5 military units.<sup>18</sup> These struggles to contain and reduce the violence in the LCB region and the deteriorating situation should not come as a surprise. A 2017 analysis warned that the problem with the western SFA approach and the G5 Force was that it was an overly technical, “capacity-building approach geared to short-term success over security sector reform and lack[ed] a coordinated strategy. The Malian government [and others]...preserves the status quo and is not prepared to accept its political responsibility.”<sup>19</sup>



A billboard in Niamey (Niger) announcing a summit of Heads of State of the G5-Sahel in February 2018. (NigerTZai - Own work)

In interviews at U.S. Africa Command (AFRICOM) in 2017 the current western SFA approach of building up the G5 Sahel Alliance to deal with the unique security threats of the region, was described by one officer as essentially a “pipe-dream.” These militaries “can barely function in their own country,” he argued, “let alone be expected to safely conduct multinational operations.”<sup>20</sup> While such dismissive remarks may have seemed overly harsh at the time, the situation in the LCB region has continued to deteriorate. Even the notoriously effective Chadian armed forces had one of its bases overrun March 23, 2020, with at least 92 troops killed by Boko Haram.<sup>21</sup>

### **Competing for Influence in Africa: Damned if you Do, Even More Damned if you Don’t**

Despite international efforts to deal with insecurity in Africa through SFA, other western aid programs and investment in Africa have decreased significantly over the last decade.<sup>22</sup> These reductions in western assistance, however, have been offset by a significant increase in aid from China and Russia. This pits great powers with conflicting visions of world order and competing interests and beliefs in how Africa should look against each other. The shrinkage of western aid programs has implications:

All Africans want democracy. We all want to be like the United States. We need help with roads and infrastructure, but our governments cannot work with USAID and the World Bank. Who can the people get help from? If not China, who?<sup>23</sup>

His thoughts reflect similar sentiments, in terms of frustration of not getting the help their country needs, by dozens of foreign military personnel interviewed by the author.<sup>24</sup>

The slow withdrawal of the United States and European powers from Africa gives China and

Russia a geopolitical opportunity in the competition for resources and influence. Substantial evidence indicates that Beijing and Moscow are strategically seeking to reshape the continent in a way that reinforces authoritarianism and enables those regimes that are the most malleable, and those that are most unconscientious in extracting resources.<sup>25</sup> Their expanding influence and their strategic intent are already noticeable. China built a military base in the port of Djibouti in 2017 and Russia has signed military cooperation agreements with over 20 African states.<sup>26</sup> In addition, Russia appears bent on setting up military bases in the Central African Republic (CAR) and in the autonomous republic of Somaliland.<sup>27</sup> The return of military personnel from opposing blocs is reminiscent of the Cold War, except the 21<sup>st</sup> century is less about promoting ideologies and more about seeking reliable partners in resource extraction and consumer markets to sell to.

While China’s and Russia’s military bases in Africa appear to have benign intent for the time being—protecting the region from terrorists and defending economic and commercial interests—there is a dark side as well. China increasingly appears intent on collecting debts and guaranteeing investments. Intentional or not, China’s actions appear to constitute a *Sino-colonial* relationship with African states—and others engaged in the Belt and Road Initiative—leveraging debt-traps. China increasingly believes it can take actions—peaceful or not so peaceful—to recoup loans and investments when a country falls behind on loan payments; like Sri Lanka, which had to cede to China a 99-year lease on the Port of Hambantota, several African nations including Kenya, Uganda, and Zambia, appear on course to default, and could fall prey to similar Chinese infrastructure seizures.<sup>28</sup>

Moscow, on the other hand, sees pecuniary value in selling ammunition and weapon systems to African countries to prop up the Russian economy

and industrial base.<sup>29</sup> Leaked documents reveal Moscow's desire to turn Africa into a "Strategic Hub," and pursue political and information warfare tactics to back pro-Russian leaders and discredit their opponents.<sup>30</sup> If this was not troubling enough, the notorious Russian private military contractor, Wagner Group, with deep ties to President Putin—that works on behalf of Russian interests in eastern Ukraine and Syria—has been spotted in the CAR, Libya, Madagascar, Mozambique, and Sudan.<sup>31</sup>

While it is difficult to obtain aggregate data on purported economic and security aid from non-transparent governments like China and Russia, it does appear that the United States provides considerably more security assistance to African countries.<sup>32</sup> However, quality does not substitute for timeliness, often preventing the United States from providing assistance when and where most needed. Consider for example how the U.S. Congress slows down the processes of acquisition and implementation by the Departments of State and Defense in providing security assistance to foreign countries. The so-called Leahy rules were first imposed in the late 1990s to ensure that U.S. aid would not be implicated in gross human rights abuses. Such legislative initiative and constraint was in response to evidence directly linking American aid to Latin American security forces engaging in gross human rights violations in the 1980s.<sup>33</sup>

The rationale and intent of the Leahy amendments are quite noble in their concern for ensuring that American SFA is not used to oppress recipient country populations. However, the vetting process is overly bureaucratic and time consuming—and makes the United States appear weak and indecisive. In a 2017 interview, an Ethiopian General complained of the contrast between the American image of strength and capability and the realities of working with a slow and inept U.S. government. He had attempted to acquire mortars

for his soldiers fighting al-Shabaab in Somalia believing this was a simple request that could be quickly delivered. Unfortunately, it took approximately two years for the United States to deliver the weapons, during which time he had no choice but to acquire the needed weapons from China and Russia, taking delivery within weeks.<sup>34</sup> Nigeria had a similar experience when trying to purchase light-attack aircraft from the U.S. government for the purposes of fighting Boko Haram, with it taking over four years of political debate to finally approve the sale in 2019.<sup>35</sup>

Leahy rules requiring extensive vetting for any sort of SFA, and similar laws in most European countries seriously undercut attempts to deal with contingencies in Africa. Clumsy laws and slow administration are a significant bureaucratic impediment to achieving influence with potential partners. In order to capitalize on the potential of SFA, both in terms of influence for the United States and its allies, and enhanced capabilities for African countries, SFA requires national and international legal regimes and procedures conducive to timely delivery of aid and assistance. As great power competitors, China and Russia provide all forms of aid and military assistance readily and without restraint.

The struggle for influence creates a deeper inherent problem, namely the security assistance dilemma: The U.S. wants a dependable military ally but also wants the government and security forces to abide by democratic standards and respect for human rights. Already, America seems to be facing such a dilemma with its commitment to Saudi Arabia, in terms of arms sales and military training, as the UN has identified numerous Saudi war crimes in Yemen.<sup>36</sup> The Rapid Intervention Battalion (BIR – *Bataillon d'Intervention Rapide*) in Cameroon puts the West in a similar situation, as the BIR of approximately 4,500 elite troops has been trained by France, Israel, and the U.S. The BIR has been a highly effective force against

regional insurgents, but is responsible for attacking Anglophone villages in western Cameroon in an attempt to cleanse them.<sup>37</sup> These examples illustrate how SFA recipients can misuse their armed forces, adding only more stressors to state fragility.

At the same time, successful western competition for influence in Africa (and elsewhere) is dependent upon socialization efforts and building relations with political and military elites in these countries so that they can transition away from illiberal politics and praetorian pathologies. Thus, if we accept that the West is somewhat trapped with not being able to punish partners (e.g. cancelling SFA, etc.) in the era of great power competition—since China and Russia will fill that void—then the West must adapt expectations and make assistance contingent on reforms. Such actions would enable the recipient state to make the necessary bargains with various power brokers—fixing fragmented state and security institutions—lending itself to long-term stability and institutionalization.

## Civil-Military Relations and Partnerships

The greatest challenge for African countries dealing with insurgents and other violent non-state actors is formulating a national approach that consolidates rather than fractures the state or the society. For example, one of the less-discussed aspects of the Tuareg 2012 rebellion in Mali was the Bamako government treatment of northern ethnic Tuaregs. While struggling to integrate these nomadic peoples into the government and military, Malian President Amadou Toumani Touré provoked them by disrupting traditional power structures.<sup>38</sup> Touré began promoting the Imghad clan (led by El Hadj Ag) as the newly empowered security force of the north, undermining the historically dominant Ifoghas clan.<sup>39</sup> Touré's disruption of patronage networks by restructuring and reforming the state essentially led to the collapse of his government. The collapse

culminated with troop defections and mutiny, ultimately leading to a *coup d'état*.

While the Malian example may represent a unique case of state collapse, the challenge of balancing and reforming different parts of the state with society and the armed forces creates a dangerous triangle, which has defined the politics of most African countries since independence. This triangle consists of predatory political, societal, and military/bureaucratic elites competing with one another in a pursuit of short-term gains that undermines the long-term interests of the state as a whole.<sup>40</sup> While UN staff and western military advisors may believe they can implement and install a western system of politics and governance, such neo-colonial attempts ignore the contextualized way in which politics are conducted.<sup>41</sup> Moreover, it changes the equilibrium of politics, disrupting power centers in state and society, which in a state lacking a monopoly over violence, adds to volatility and the likelihood of civil war.

We would be well-advised to consider the strategic partnership vision promulgated by retired South African Colonel Rocklyn “Rocky” Williams. A rebel in the African National Congress (ANC), Williams fought against South African apartheid. Post-apartheid he eventually rose to the rank of Colonel in the South African National Defence Forces (SANDF). During that time he proposed a transformative vision for civil-military relations (CMR) in South Africa and elsewhere in Africa. Williams contended that with their contextually specific histories, including differing pathways to independence, each African country has unique informal power structures that heavily influence the exercise of authority and legitimacy. It was Williams' contention that the problem with CMR in most African countries is in the struggles to balance western models of objective and subjective control of the military by political leadership.<sup>42</sup> However, this tension is precisely why CMR reform is so difficult. Few African leaders see advantage in a capable military;

the armed forces become just another vestigial organ of patronage. The current political landscape in Africa demands a shift towards constructive modes of CMR that promote military professionalism, and are integrated into the decision-making processes of the state.<sup>43</sup>

Countries such as Ethiopia and Rwanda appear good candidates for the CMR model proposed by Williams. Both have built robust armed forces that rely on informal power sharing between the government, society, and even parts of the economic sector. Moreover, their current forms are informed by political ideologies formed while fighting as rebels against the previous Derg Regime of Ethiopia and genocidal Hutu Regime in Rwanda. While CMR in Ethiopia or Rwanda may appear “alien” to western military officers, their armed forces act as strategic partners and are contextually professional and effective in their respective home country processes of nation- and state-building.<sup>44</sup> The blending and blurring of lines between the government and armed forces may appear “corrupt” to many international observers, but this contextualized form of CMR has led to stability in both countries and effective

military institutions.<sup>45</sup> Indeed Ethiopia and Rwanda are capable stability providers elsewhere in Africa through UN and AU peacekeeping missions with some of the highest participation rates across the continent, and have proven to be among the most reliable and effective forces in these missions.<sup>46</sup>

These examples show that when political and military elites create partnerships, effective armed forces can be built that are not a threat. Western SFA efforts in fragile African states—and elsewhere—should increasingly build in a political element that brings CMR reforms—but that do not excessively emphasize democratization or other western values at the expense of stability.<sup>47</sup> This requires partnerships between the various branches of government, so that various actors each share the “buy-in” necessary to meet the challenges of both domestic and regional problems, conflict, and instability. Finally, and most importantly, the development of professionalism is dependent upon the dynamics of the political context. Defense institution building alongside broader developmental efforts can sustain this process by institutionalizing cooperation between numerous political and societal elites.<sup>48</sup>



Members of the Rwanda Defense Force move into formation after arriving in Bangui, Central African Republic (CAR), Jan. 16, 2014. (CPT Tom Byrd)

## Conclusion: Less Lethality, More Consolidation

Despite supposed strategic shifts in the 2017 *National Security Strategy (NSS)* to more traditional national security concerns such as great power competition with China and Russia, Africa should not be left out of the equation.<sup>49</sup> Western efforts to counter recent geopolitical inroads into Africa by China and Russia also require new forms of SFA engagement, and alternative ways of achieving development. The United States and its allies, and the UN cannot continue the old approach of trying to impose “rich-country institutions” throughout Africa, neglecting the unique histories, contexts, and cultures that inform the way authority, legitimacy, and power are organized and exercised in each state.<sup>50</sup> An interloping SFA advisor in this situation can show little innovation locked into the traditional rules of engagement, and often ends up operating in an *ad hoc* fashion primarily to protect him or herself, strategically undermining the whole point of the mission.<sup>51</sup> A summary statement by an Italian Colonel briefing his experience providing SFA in a weak state captures this problem at its worst: “Force Protection is ALWAYS the highest priority.”<sup>52</sup> Such risk-adverse approaches undermine the development of relationships with local counterparts, and decrease the likelihood of local elites collaborating with SFA advisors other than for the pursuit of their own selfish interests, such as providing false intelligence to target their rivals.<sup>53</sup>

As this article argues, the G5 Sahel Joint Force remains a pipedream in terms of addressing problems associated with under-development that have made ethnic conflict, insurgency, and criminality so enticing to so many living in the Lake Chad Basin region. Neighboring states must be encouraged by the West to take steps towards deep structural reforms, which requires a deeper level of western engagement. This requires an enduring commitment to support governments once

conflict is contained through the crucial five years of rebuilding during which civil war relapse is most likely.<sup>54</sup> Such long-term engagement by the West is crucial; decreasing western engagement only opens a power and influence vacuum for China and Russia, with many of their efforts supporting those African leaders rolling back democracy, rule of law, and human rights. Increased western emphasis on making African militaries more lethal and combat effective—in the absence of broader developmental assistance—merely masks (and reinforces) the institutional problems that lead to poor governance and weak security institutions.

Such realities in context of great power competition, and the existence of several professionalized militaries in Africa, suggests the United States and its allies can improve G5 countries and other failing states via reliable SFA proxies. This might mean the West can support and empower the militaries of Ethiopia, Rwanda, and Senegal, to act as mediating SFA providers. For instance, given Senegal’s robust institutionalization of CMR and military effectiveness since independence, the West could directly support Senegal to act as an intermediary SFA provider to G5 member states. Given Senegal’s legitimacy as having professionalized armed forces and their proximity and understanding of culture and political context in G5 countries, they could facilitate dialogue in these countries, helping reform politics and restructuring elite level agreements. Such an idea of western SFA by proxy is not without merit. The former Minister of Security of Burkina Faso, Dr. Emile Ouédraogo, suggested in 2019 that Senegal should be leading the G5 for numerous reasons.<sup>55</sup> Such a G5+1 (Senegal) idea best encompasses the focus of shifting away from overly technical western SFA and towards broader political SFA peacebuilding efforts. Senegalese military advisors, if properly supported by the West, could better facilitate CMR reforms, while enabling cooperative institutions in each G5 country. Similarly positive



impacts could be made with fragile states in Central and Eastern Africa, by the West empowering the militaries of Ethiopia and Rwanda (and other professionalized African militaries) to provide SFA as a way of avoiding the typical traps of western SFA.

The West needs broader SFA approaches to remain competitive and influential. Partnerships and peacebuilding between influential elites and other informal powerbrokers should be the hallmark of future SFA efforts.<sup>56</sup> This builds on the idea of creating contextually dependent versions of African civil-military relations that enable strategic partnerships between formal and informal actors in government, security institutions, and society. Such overlap is needed to create a shared vision and cooperation. Most importantly, it gets away from the overly technical understanding of military development in a weak state that often causes imbalances in power and a loss of trust. Helping Africans overcome state fragility requires shared ownership by elites and citizens alike across Africa and a willingness to overcome socially constructed identities.<sup>57</sup>

If the U.S. and allies continue down the path of providing SFA for the sake of CT, then the frustration of seeing such assistance creating the moral hazard of dependency or being used for repression and other abuses will likely continue. The security assistance dilemma of only providing SFA to block Chinese and Russian access is a precarious balance. Such SFA must maintain entry ramps to integrate with broader developmental programs, which requires strategic intent and resolve to confront this paradox. Tailoring such assistance means that western capitals must tailor contingent SFA in a timely and effective manner, to include a country-specific analysis of power dynamics. This enables alternative pathways of achieving contextually effective CMR reforms in a host-nation, helping socialize what an effective and professional army looks like—and the ways it can reshape the state into being more effective and professional. This all sounds easy in theory, but

the toughest part is convincing a host-nation that western commitments are long-term—and not apt to stopping due to the whims of domestic fervor over providing assistance to faraway countries they cannot locate on a map. **PRISM**

## Endnotes

<sup>1</sup> The views expressed by the author are his own and do not reflect the official views or position of the U.S. military, Department of Defense, or U.S. government. The author thanks Renanah Miles Joyce and Will Reno for article comments and Theodore McLaughlin and Lee Seymour for the invitation to present this research at the *Workshop on International Training Activities*, hosted by the Canada Research Chair on the Politics of Violence, and Center for International Peace and Security Studies (CEPSI) in Montreal, Canada, November 14-15, 2019.

<sup>2</sup> *AJP 3-16, Allied Joint Doctrine for Security Force Assistance* (London: U.K. Ministry of Defence, 2016).

<sup>3</sup> Jahara Matissek, “The crisis of American military assistance: Strategic dithering and Fabergé Egg armies,” *Defense & Security Analysis* 34, no. 3 (2018): 267-290.

<sup>4</sup> “Security Assistance Dashboard, 2001-2018, Sub-Saharan Africa and North Africa,” *Security Assistance Monitor*, 2019, <https://securityassistance.org/content/security-aid-dashboard>.

<sup>5</sup> Catherine Gegout, *Why Europe intervenes in Africa: Security prestige and the legacy of colonialism* (New York: Oxford University Press, 2018).

<sup>6</sup> Loren B. Landau, Caroline Wanjiku Kihato, and Hannah Postel, “Europe Is Making Its Migration Problem Worse: The Dangers of Aiding Autocrats,” *Foreign Affairs*, September 5, 2018, <https://www.foreignaffairs.com/articles/africa/2018-09-05/europe-making-its-migration-problem-worse>.

<sup>7</sup> “US migrant crisis: Trump seeks to curb Central America asylum claims,” *BBC*, July 16, 2019, <https://www.bbc.com/news/world-latin-america-48991301>.

<sup>8</sup> These are known as limited access orders (LAOs), where politics by elites in these weak states are negotiated via violence, bringing the economic system of sharing rents into equilibrium, whereas open access orders (OAOs) – primarily the developed world – allow everyone to compete politically and economically without the use of coercion. For more, refer to: Douglass C. North, John Joseph Wallis, Steven B. Webb, and Barry R. Weingast (eds.), *In the shadow of violence: Politics, economics, and the problems of development* (New York: Cambridge University Press, 2013).

<sup>9</sup>Buddhika Jayamaha, Jahara Matisek, William Reno, and Molly Jahn, "Changing Weather Patterns, Climate Change and Civil War Dynamics: Institutions and Conflicts in the Sahel," *Journal of Diplomacy* 20, no. 1, (Fall/Winter 2018): 70–87.

<sup>10</sup>Informal discussion with retired U.S. Army General, October 24, 2019.

<sup>11</sup>One of the biggest critics of American involvement in Africa is the investigative journalist Nick Turse who is a fellow at the *Nation Institute*, managing editor of *TomDispatch*, and a contributing writer at *The Intercept*.

<sup>12</sup>Toyo Amegnonna and Marcel Dossou, "The impact of China's one belt one road Initiative in Africa: The Evidence from Kenya," *MPRA Paper 90460*, University Library of Munich, Germany, 2018.

<sup>13</sup>Lina Benabdallah, "China-Africa military ties have deepened. Here are 4 things to know," *Washington Post: Monkey Cage*, July 6, 2018, <https://www.washingtonpost.com/news/monkey-cage/wp/2018/07/06/china-africa-military-ties-have-deepened-here-are-4-things-to-know/>.

<sup>14</sup>Reuben Brigety, "A Post-American Africa: The U.S. Is Falling Behind," *Foreign Affairs*, August 28, 2018, <https://www.foreignaffairs.com/articles/africa/2018-08-28/post-american-africa>; Cara Anna, "Russia's new focus on Africa takes advantage of US drift under Trump administration," *ABC News*, October 21, 2019, <https://abcnews.go.com/International/wireStory/russias-focus-africa-takes-advantage-us-drift-66415655>.

<sup>15</sup>"G5 Sahel Joint Force and the Sahel Alliance," *France Diplomatie: Ministry for Europe and Foreign Affairs*, February 2019, <https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/crises-and-conflicts/g5-sahel-joint-force-and-the-sahel-alliance/>.

<sup>16</sup>Natasja Rupesinghe, "The Joint Force of the G5 Sahel: An Appropriate Response to Combat Terrorism?" *Conflict Trends*, no. 2 (2018): 11-18.

<sup>17</sup>Morten Boås, *Rival priorities in the Sahel: finding the balance between security and development* (Uppsala, Sweden: Nordiska Afrikainstitutet, 2018).

<sup>18</sup>"'Continuing deterioration' leaves Mali facing critical security level: UN expert," *UN News*, December 2, 2019, <https://news.un.org/en/story/2019/12/1052531>; "G5 Sahel leaders hold crisis talks in response to deadly jihadist attack in Niger," *France 24*, December 15, 2019, <https://www.france24.com/en/20191215-g5-sahel-leaders-to-begin-crisis-talks-in-response-to-deadly-jihadist-attack-in-niger>.

<sup>19</sup>Denis M. Tull, "Mali, the G5 and security sector assistance: Political obstacles to effective cooperation," *Stiftung Wissenschaft und Politik (SWP) Comments*, 52, December 2017, German Institute for International and Security Affairs.

<sup>20</sup>Interviews, AFRICOM, Stuttgart, Germany, July 31 – August 4, 2017.

<sup>21</sup>Will Brown, "As the World Is Distracted, Boko Haram Terrorists Strike a Key Western Ally," *Foreign Policy*, April 1, 2020, <https://foreignpolicy.com/2020/04/01/boko-haram-islamist-terrorists-strike-chad-while-world-distracted-by-coronavirus/>.

<sup>22</sup>Barbara Wesel, "EU investment in Africa: Europe racing to catch up," *DW*, September 9, 2018, <https://www.dw.com/en/eu-investment-in-africa-europe-racing-to-catch-up/a-45500068>; Mfonobong Nsehe, "The Importance of Improving America's Investment Policies in Africa - An Interview with Yuri Vanetik," *Forbes*, December 17, 2019, <https://www.forbes.com/sites/mfonobongnsehe/2018/12/17/the-importance-of-improving-americas-investment-policies-in-africa-an-interview-with-yuri-vanetik/#15c388f63c7e>.

<sup>23</sup>Matthew Quintero, "If Not China, Who? Competing in Africa through Foreign Military Education," *Center for International Maritime Security*, July 23, 2019, <http://cimsec.org/if-not-china-who-competing-in-africa-through-foreign-military-education/41037>.

<sup>24</sup>Interviews with foreign military personnel from over 40 countries. 2015–2020.

<sup>25</sup>Laura Zhou, "What to know about China's ties with Africa, from aid to infrastructure," *South China Morning Post*, July 22, 2018, <https://www.scmp.com/news/china/diplomacy-defence/article/2156279/what-know-about-chinas-ties-africa-aid-infrastructure>; Eric Schmitt, "Russia's Military Mission Creep Advances to a New Front: Africa," *The New York Times*, March 31, 2019, <https://www.nytimes.com/2019/03/31/world/africa/russia-military-africa.html>.

<sup>26</sup>Jakob Hedenskog, "Russia is Stepping Up its Military Cooperation in Africa," *Swedish Defence Research Agency*, December 2018, <https://www.foi.se/rest-api/report/FOI%20MEMO%206604>.

<sup>27</sup>"Alpha Conde, Putin's middleman for Somaliland," *The Indian Ocean Newsletter*, July 19, 2019, <https://www.africaintelligence.com/ion/corridors-of-power/2019/07/19/alpha-conde-putin-s-middleman-for-somaliland,108366322-eve>; Andrew Roth, "Central African Republic considers hosting Russian military base," *The Guardian*, October 25, 2019, <https://www.theguardian.com/world/2019/oct/25/central-african-republic-russia-military-base>.

<sup>28</sup>Wilson VornDick, "Let China Fail in Africa," *The National Interest*, January 29, 2019, <https://nationalinterest.org/feature/let-china-fail-africa-42812>.

<sup>29</sup>Kester Kenn Klomegah, "Russia, Africa and the Debts," *Modern Diplomacy*, November 19, 2019, <https://modern diplomacy.eu/2019/11/19/russia-africa-and-the-debts/>.

<sup>30</sup> Luke Harding and Jason Burke, “Leaked documents reveal Russian effort to exert influence in Africa,” *The Guardian*, June 11, 2019, <https://www.theguardian.com/world/2019/jun/11/leaked-documents-reveal-russian-effort-to-exert-influence-in-africa>.

<sup>31</sup> Tim Lister, Sebastian Shukla, and Clarissa Ward, “Putin’s Private Army,” *CNN: Special Report*, September 2019, <https://edition.cnn.com/interactive/2019/08/africa/putins-private-army-car-intl/>.

<sup>32</sup> “Russia’s foreign aid re-emerges,” *Aid Data: A Research Lab at William & Mary*, April 9, 2018, <https://www.aiddata.org/blog/russias-foreign-aid-re-emerges>; “Data: Chinese Foreign Aid,” *China Africa Research Initiative*, John Hopkins: School of Advanced International Studies, 2019, <http://www.sais-cari.org/data-chinese-foreign-aid-to-africa>.

<sup>33</sup> Tanya Broder and Bernard D. Lambek, “Military Aid to Guatemala: The failure of US human rights legislation,” *Yale Journal of International Law* 13, no. 1. (1988): 111-145.

<sup>34</sup> Fieldwork and Interviews, August, Addis Abbaba, Ethiopia, August 2017.

<sup>35</sup> “Trump plans to move ahead with Nigeria plane sale – source,” *Stock Daily Dish*, December 18, 2019, <https://stockdailydish.com/trump-plans-to-move-ahead-with-nigeria-plane-sale-source/>.

<sup>36</sup> “Situation of human rights in Yemen, including violations and abuses since September 2014,” Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, A/HRC/42/CRP.1, September 3, 2019.

<sup>37</sup> “Burning Cameroon: Images you’re not meant to see,” *BBC News*, June 25, 2018, <https://www.bbc.com/news/world-africa-44561929>.

<sup>38</sup> “Country Profile: Mali, January 2005,” *Library of Congress—Federal Research Division*, 5, <https://www.loc.gov/rr/frd/cs/profiles/Mali-new.pdf>.

<sup>39</sup> Jahara Matissek, “An Effective Senegalese Military Enclave: The Armée-Nation ‘Rolls On,’” *African Security* 12, no. 1 (2019): 62-86.

<sup>40</sup> Joel S. Migdal, *Strong societies and weak states: State-society relations and state capabilities in the Third World* (Princeton, NJ: Princeton University Press, 1988).

<sup>41</sup> Alain Rouvez, Michael Coco, and Jean-Paul Paddock, *Disconsolate Empires: French, British and Belgian Military Involvement in Post-Colonial Sub-Saharan Africa* (New York: University Press of America, 1994).

<sup>42</sup> Samuel P. Huntington, *The soldier and the state: The theory and politics of civil-military relations* (Cambridge, MA: Harvard University Press, 1957).

<sup>43</sup> Rocky Williams, “Towards the creation of an African civil-military relations tradition,” *African Journal of Political Science/Revue Africaine de Science Politique* 3, no. 1 (1998): 20-41.

<sup>44</sup> Fieldwork, Ethiopia and Rwanda, August 2017; Gérard Prunier, “The Armies of the Great Lakes Countries,” *PRISM* 6, no. 4 (2018): 99-111.

<sup>45</sup> Jahara Matissek and William Reno, “Getting American Security Force Assistance Right: Political Context Matters,” *Joint Force Quarterly* 92 (2019): 65-73.

<sup>46</sup> Scott Firsing, “Thinking through the role of Africa’s militaries in peacekeeping: The cases of Nigeria, Ethiopia and Rwanda,” *South African Journal of International Affairs* 21, no. 1 (2014): 45-67.

<sup>47</sup> This proposition goes against the views of one prominent scholar that believes only westernized democratic control of armies in Africa will work. For more, see: Mathurin C. Houngnikpo, *Guarding the Guardians: Civil-military relations and democratic governance in Africa* (New York: Routledge, 2016).

<sup>48</sup> Alexandra Kerr and Michael Miklaucic (eds.), *Effective, Legitimate, Secure: Insights for Defense Institution Building* (Washington, DC: National Defense University).

<sup>49</sup> Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017).

<sup>50</sup> Kate Bridges and Michael Woolcock, *How (not) to fix problems that matter: assessing and responding to Malawi’s history of institutional reform* (New York: The World Bank, 2017).

<sup>51</sup> William Reno, “The politics of security assistance in the Horn of Africa,” *Defence Studies* 18, no. 4 (2018): 498-513.

<sup>52</sup> Italian Army Colonel, PowerPoint Briefing, Rome, Italy, September 24, 2019.

<sup>53</sup> Stathis N. Kalyvas, *The Logic of Violence in Civil War* (New York: Cambridge University Press, 2006).

<sup>54</sup> Paul Collier, *The Bottom Billion: Why the Poorest Countries are Failing and What Can Be Done About It* (New York: Oxford University Press, 2007).

<sup>55</sup> “SECURITE – Dr Emile Ouédraogo, ancien ministre burkinabè de la Sécurité : «Je ne comprends pas pourquoi le Sénégal ne fait pas partie du G5 sahel»,” *le Qoutidien*, August 28, 2019, <https://www.lequotidien.sn/secureite-dr-emile-ouedraogo-ancien-ministre-burkinabe-de-la-secureite-je-ne-comprends-pas-pourquoi-le-senegal-ne-fait-pas-partie-du-g5-sahel/>.

<sup>56</sup> Emily Knowles and Jahara Matissek, “Western Security Force Assistance in Weak States: Time for a Peacebuilding Approach,” *The RUSI Journal* 164, no. 3 (2019): 10-21.

<sup>57</sup> Amartya Sen, *Identity and Violence: The Illusion of Destiny* (New York: W. W. Norton & Company, 2007); Clayton Christensen, Efosa Ojomo, and Karen Dillon, *The Prosperity Paradox: How Innovation Can Lift Nations Out of Poverty* (New York: HarperCollins Publishers, 2019).



By 2035, 5G will enable \$13.2 trillion in global economic output, or the equivalent of adding 5 percent to global GDP.  
(Bill Oxford)

# Don't Trust Anyone

## The ABCs of Building Resilient Telecommunications Networks

By Andy Purdy, Vladimir M. Yordanov, and Yair Kler

The January issue of Prism carried an article titled “The Worst Possible Day”<sup>1</sup> that included a discussion of the implications for the United States of banning Chinese company Huawei from networks that the United States and its allies rely on for national security-related communications. A supporter of the ban, the author, Thomas Donahue, emphasized the critical importance of using equipment from trusted sources in U.S. telecom infrastructure and that of its allies. He argued that the consequences of not doing so could be catastrophic when the United States needs to project power, or convincingly threaten the use of force, such as during a military conflict. The article concluded that the United States needs to seriously consider how to assure the use of trusted alternatives to Huawei equipment, whether by supporting the development of a U.S.-based manufacturer or consortium, or spending tens of billions of dollars to acquire either or both the manufacturers Nokia and Ericsson, or investing significantly in the two Nordic firms.

We cybersecurity professionals at Huawei Technologies concur that the U.S. military and U.S. allies must have access to telecommunications networks that are available at all times, even in the worst conditions imaginable. But we disagree with Donahue’s message that Huawei must be blocked because it is headquartered in China; that companies headquartered in countries allied with the United States can be considered “trusted;” and that the “risk” from Huawei equipment cannot be mitigated. In our view, the best way to assure reliable telecommunication networks is to have a comprehensive approach to risk and resilience, which includes verifiable conformance and testing protocols. When it comes to managing risks in cyberspace, the best approach is to distrust everyone.

For the past year, as telecommunication service providers in numerous countries have begun choosing suppliers for their 5G networks, the United States government (USG) has emphatically told governments around the world that Huawei cannot be trusted to be a supplier to their 5G networks and has put heavy pressure on a number of governments to bar Huawei from 5G development. Donahue articulated his concerns somewhat more dispassionately than most, with an emphasis on what is critical from a national security perspective. He also stressed the importance to the United States and the global community of promoting greater

---

Andy Purdy is Chief Security Officer, Huawei Technologies, USA; Vladimir M. Yordanov is former Global Cybersecurity and Privacy officer, Huawei technologies; Yair Kler is Head of Solution Security – Europe, Middle East, Africa Region, Huawei Technologies.

competition among telecom equipment providers, which we agree is good for everyone.

This article attempts to explain why we believe that those who argue for the need to block Huawei and assume that Huawei's European competitors' products are worthy of trust, are wrong. Making a determination that a supplier is trustworthy based on the country in which it is headquartered is a misguided and dangerous approach. The article also describes a framework for a holistic cybersecurity strategy that ensures resilient and secure networks—including those with Huawei technology—are available to the United States and its allies, even on the worst possible day.

## Washington's Problem and Donahue's Solution

5G will have a major impact on the world economy. It will bring massive cloud-based computing power to the end-user and create new jobs by digitizing and 5G-enabling current and new industries. A 2019 study conducted by the market survey firm IHS Markit, commissioned by the U.S.-based chip and telecom equipment maker, Qualcomm, concluded that by 2035, 5G will enable \$13.2 trillion in global economic output, or the equivalent of adding 5 percent to global GDP.

Only a handful of vendors can supply end-to-end 5G equipment, and none of them is headquartered in America. The choices for 5G Radio Access Networks are limited mainly to Nokia, Ericsson, ZTE, and Samsung, but Huawei is generally acknowledged to be the leader in technological development and product range. Ericsson and Nokia are the closest runners-up.

The USG is opposed to using Huawei equipment in its networks and has put forth various reasons for its opposition, usually premised on the claim that China could imperil U.S. national security by using Huawei equipment to shut down networks, steal data, or conduct unauthorized surveillance.

Donahue focuses on what he sees as the most significant national security risk to the United States of having Huawei equipment in a key network; that on the "worst possible day"—during a military conflict or a situation when the United States must be able to use military force or deter an adversary from a hostile action—U.S. telecommunications networks, and those foreign networks that enable communications by United States and allies' assets, may not be available if they include equipment supplied by a company headquartered in China. Donahue argues that even for fiber links that withstand hostilities, data traveling over such links could be "subject to disruption if the communications must pass through equipment provided by vendors from hostile countries." Moreover, the United States might not be able to rely on communications satellites as an alternative avenue for key communications.

According to Donahue, this risk cannot be mitigated because "with 5G, the distinction between the edge and the core largely disappears." He contends that this would prevent operators from maintaining proper isolation and, as a result, vulnerabilities at the edge could directly impact and expose the core network to unmanageable risks. Therefore, in his view, it is not enough simply to ban Huawei from the core of 5G; Huawei must be banned from supplying any equipment to any part of networks that may be depended on by the United States and its allies.

Having left the telecommunications industry in the United States to the unpredictability of market forces, the U.S. no longer has a domestic equipment vendor able to provide a full range of products. Moreover, the two European vendors, Nokia and Ericsson, that Donahue presumes are "trusted," are not on strong financial footing. They lack for example, adequate ability to invest in R&D. Donahue argues that, given the strategic importance of secure communications, the U.S. government should step in and either help to fund

the development of a strong U.S. supplier or consortium-supplier, invest in telecom firms in friendly countries, or consider buying Nokia, Ericsson, or both. He concedes that this would likely cost tens of billions of dollars.

## The Problem with a “Trusted Vendor” Strategy

In Donahue’s view, Nokia and Ericsson can be trusted because they are headquartered in countries that are close U.S. allies: Huawei, conversely, cannot be trusted because its headquarters are in China—a strategic U.S. adversary. We do not argue that the two Nordic companies are not worthy of trust in a traditional sense, but strongly urge that the determination that a company is worthy of trust—and thus that its products should automatically be deemed trustworthy—should not depend solely on where the company is headquartered. A few recent cases demonstrate this reality.

In 2013, the retailer Target was attacked through a supplier of air conditioning services.<sup>2</sup> Because it was a trusted supplier, the A/C vendor had remote access credentials to parts of Target’s servers for the purpose of monitoring temperature and energy use throughout Target stores. But by tricking one of the supplier’s staff through a phishing email, hackers managed to piggy-back on the vendor’s access privileges to steal customers’ credit card data. The data breach ended up costing Target \$292 million<sup>3</sup> in compensation, legal, and other expenses. This excludes lost sales and the impact on share prices.

In 2017, hackers used TeamViewer, a software program used by IT support technicians to repair computers remotely, to breach the servers of Piriform, a company that was in the process of being acquired by cybersecurity software provider Avast. While inside the network, the attackers introduced malware into CCleaner, a widely trusted registry-cleaning tool that has been downloaded more than 2 billion times worldwide. Throughout the acquisition of Piriform,

users continued to install CCleaner on their computers. As a result, the corrupted version of the program allowed attackers to penetrate the servers of at least 11 companies, mostly in the IT sector.<sup>4</sup>

Also, in 2017, researchers identified a new type of vulnerability in Intel x86 architecture<sup>5</sup> called Meltdown, which could be exploited by adversaries to bypass computer security protocols and steal secrets processed on it. Additional research<sup>6</sup> identified new vulnerabilities, including Spectre, Spectre-NG, Foreshadow, TLBleed, and ZombieLoad, in Intel’s CPU chips. The U.S. military and many other U.S. government agencies are major users of x86-based computers, largely because Intel is widely considered a trusted vendor.

Earlier this year, the *Washington Post* published the news that Crypto AG, a Swiss manufacturer of encryption devices, was owned by the CIA and the German spy agency BND. According to the report, for decades Crypto supplied compromised equipment to more than 120 governments. Backdoors installed by BND into Crypto’s machines enabled the United States and Germany to intercept and decrypt highly classified communications from allied nations and foes alike. Buyers trusted Crypto’s gear largely owing to Switzerland’s carefully cultivated reputation for neutrality.

The common denominator in all of these incidents is that, in each case, attackers compromised the target systems through a trusted vendor. Trust that is not based on evidence is a network security design flaw.

Huawei is headquartered in Shenzhen (south-east China, next to Hong Kong), but both Nokia and Ericsson develop many of their products in China and manufacture hardware there. Ericsson operates five innovation centers in China, including one focused on 5G. Nanjing is the company’s largest manufacturing and logistics base worldwide and the location where Ericsson makes its 5G gear. Ericsson has 11,000 staff in China, roughly 5,000 of whom work in R&D.<sup>7</sup>



NOKIA is a multinational communications and information technology company founded in 1865 with substantial operations in China. (Photo by Testing / Shutterstock.com)

Similarly, Nokia co-owns its Chinese subsidiary, Nokia Shanghai Bell, together with a Chinese state-owned enterprise, China Huaxin, which holds just over 49 percent of the venture<sup>8</sup> and has the right to nominate its CEO. From 2002 to 2017, the unit’s chairman also acted as the Secretary of the Chinese Communist Party committee within the company (every company of a certain size that does business in China is required to have a Party committee).<sup>9</sup>

Were the United States to buy Nokia or Ericsson (or both), it would be acquiring firms with substantial operations in China, and large numbers of

Chinese personnel. Instead of making assumptions about trustworthiness based on where a company is headquartered, it is preferable to focus on the assurance and transparency requirements and features of all the key players, including the telecom and mobile operators, on the one hand, and the equipment (and other third-party) suppliers, on the other.

### 5G in the U.S. Military

It is commonsense that U.S. national security communications must be available—world-wide—when needed. Donahue contends that if



key communications networks are disrupted, the United States may not be able to count on the survival of communications satellites as an adequate alternative: He notes that even communications on still-operational fiber lines could be intercepted by adversaries, particularly if the equipment used was supplied by “vendors from hostile countries.”

But the Department of Defense (DOD) is enthusiastic about the use of 5G by the military, as evidenced by a paper it published last year.<sup>10</sup> The paper mentioned several security concerns but, according to the DOD, these are manageable. In the meantime, the evolving industry standards for 5G security are providing demonstrable enhancements.

We must point out the obvious limitations of 5G for use by the U.S. military. First, the U.S. military operates globally but it will be a long time before civilian 5G networks are deployed everywhere the U.S. military or its allies operate. A quick look into the GSMA<sup>11</sup> mobile economy 2019<sup>12</sup> report reveals that by 2025, only 15 percent of the world’s mobile network traffic will operate on 5G, while 25 percent of it will, of necessity, use 15- to 20-year-old 2G or 3G technologies. (2G and 3G do not satisfy even the most basic bandwidth requirements for 5G-enabled U.S. military applications.) Based on previous adoption rates of mobile technologies, it would be reasonable to estimate that it will take 5G between 20 and 30 years to reach 80 percent global coverage.

In addition, 5G networks are localized and operate within the coverage area (dictated by local circumstances of the particular state, operator, or geography). Therefore, when traffic is carried outside of state borders or between operators—for example, from a Middle Eastern country to the United States—it must traverse the global backbone and pass through various states and undersea cables, paths which are vulnerable to tampering and disruption, regardless of the vendor or equipment deployed. Thus, while some U.S. adversaries may be developing capabilities to remotely shut down

wireless networks, another option is to “cut the wire” as *The National Interest* described in a 2018 article on Russian undersea capabilities. If you have access to a submarine, this direct route would likely be easier than trying to remotely shut down a distant network by routing attacks through multiple operators and their various security controls.

Second, on the “worst day,” 5G could be unavailable in one or more of the key fields of operations. Mobile networks are vulnerable to signal jamming and GPS spoofing attacks. In late January 2020, the U.S. Navy conducted a large-scale GPS jamming exercise that covered 125,000 square miles in six U.S. states.<sup>13</sup> News reports also indicate that GPS jamming is widely used by Russia against U.S. fighter jets near Iran.<sup>14</sup> Given the range and reach of such jamming technologies and their potential impact on 5G networks national security critical communications need to have access to alternative network technologies in addition to 5G.

During a conflict, a communications network can come under attack from multiple vectors. To disable 5G networks, attackers will first select the easiest, most direct route offering the highest probability of success. Trying to hack into a 5G network that is designed to field such breaches is a comparatively harder way for an enemy to achieve the intended result.

## Security Challenges Posed by 5G

In coming years, governments, businesses, and households will increasingly depend on information and communications technologies (ICT) for essential services. Digitized industries and businesses will create new products and services that use 5G’s capability to seamlessly deliver cloud-based computing power to the user: 5G provides high speed, low latency, and the ability to support up to one million connections per square kilometer. The new network technology will be relied on to provide essential government services and manage critical infrastructure such as the



5G Repeater Tower, Mobile Phone Base Station. (Bill Oxford)

power grid, banking, aviation, telecommunications, and public transport, to cite a few examples. And apparently, as we just saw, DOD also plans to use it extensively for military-related purposes.

While the benefits will be numerous, the result of this enhanced connectivity and 5G-enabled services will be an expanded attack surface and a heightened risk of cyber breach or disruption in multiple domains. Attackers will have more potential entry points as they attempt to extract and modify data, disrupt services, and perpetrate other malicious exploits.

Such risks exist with 3G and 4G, but 5G increases their potential impact because more

critical services will depend on telecommunications technology. Harm caused by unauthorized tampering with a 5G-connected device could propagate to the rest of the network, using 5G's higher speeds and lower latency to do more damage. In a worst-case scenario, a successful attack could deal a crippling blow to a government, knock out critical infrastructure, paralyze technologies needed for healthcare, and disrupt key supply chains.

In October 2019, the European Commission published a report on the implications of 5G deployment. The report identified five types of risk, linked to the following causes:<sup>15</sup>

- Insufficient security measures
- 5G supply chain
- Third parties such as foreign governments or organized crime
- Interdependencies between 5G networks and critical systems (such as basic infrastructure or healthcare)
- Multiplication of unsecured devices linking to the 5G networks.

These risks, while formidable, have been anticipated by the industry in the collaborative standards process—not just equipment suppliers, but also network operators, device manufacturers, and software developers.

## Periphery and Core in 5G: a Distinct Separation

Donahue states that in 5G, “...the distinction between the edge and the core largely disappears,” and as a result, Huawei would have access to an entire network even if it only supplies the radio equipment. In fact, although under 5G the core and the edge move closer together in a physical sense, the virtual distinction is maintained and the standards enhance security of both, particularly the “edge.”

The distinction between the core and edge in the logical architecture of 5G is defined by 3GPP<sup>16</sup> and the European Telecommunications Standards Institute (ETSI),<sup>17</sup> and recognized by the U.S. Federal Communications Commission (FCC). In addition to the existing core, access, and transport sections of the network, this architecture introduces a new section of the network referred to as edge computing, also known as multi-access edge computing (MEC) in ETSI terminology. According to 3GPP 5G standardization documents, MEC is a disaggregated part of the core network, located closer to the access network in order to reduce network latency. It remains part of the core network and maintains clear logical separation from the access

network; and it includes dedicated interfaces as well as possible physical separation. The 5G standards process makes clear that the core and edge separation will be maintained in 5G.

The continued virtual separation of the core from the RAN and the attendant security benefits have been confirmed authoritatively. In June 2019, Professor Alf Zugenmaier (Vice Chair of the 3GPP SA<sup>3</sup><sup>18</sup>) and Professor Rahim Tafazolli<sup>19</sup> (University of Surrey), testified on the subject at a U.K. House of Commons hearing:<sup>20</sup> “The core network, as defined by the functions, may be moving out closer to the cell sites....but it is very clear what functions are core network and which are access network,” Zugenmaier said. Tafazolli added that, “there is a clear distinction between core and radio access networks wired through a unified interface, which is standardized in the 3GPP standardization.” Tafazolli further noted that, “operators have the option of buying the core from one vendor and radio access from other vendors.”

## A Holistic Risk-Mitigation Strategy for 5G Networks

Effectively managing the risk involved in 5G networks is feasible without barring suppliers and even while using equipment that is not deemed secure. The comprehensive strategy we describe below involves techniques recently endorsed and implemented by the most credible U.S. cybersecurity authorities. This holistic cybersecurity approach includes two design principles and three pillars. The two principles are trust minimization and the assumption of breach:

**Trust Minimization;** as discussed above, trust should be considered a fatal design flaw. Therefore, any security solution designed for critical infrastructure should minimize, as much as possible, the degree of trust in the underlying components, services, and personnel. Trust should be proven based on facts and should not be assumed.

**Assume Breach;**<sup>21</sup> a concept that was coined in the early 2000's<sup>22</sup> by Kirk Bailey, who suggested that organizations should build their networks based on the assumption that a well-funded adversary (e.g., a state-sponsored hacker) would be able to infiltrate any system. Bailey's proposed design principle resonated with the U.S. government. In 2016, General Michael Hayden (ret.), the former Director of the CIA and NSA, said, "Fundamentally, if somebody wants to get in, they're getting in... Accept that."<sup>23</sup>

These principles complement each other and should be the foundation for a robust risk-mitigation framework. Trust-minimization and assume-breach have successfully proven themselves under extreme, hostile conditions for the past decade. We mentioned earlier the Intel x86 vulnerabilities called Meltdown, Spectre, Spectre-NG, Foreshadow, TLBleed, and ZombieLoad. Although the vulnerabilities impacted the deepest layer of the system, that is, the hardware layer, the damage was minimal. Leading cloud service providers in the United States had generally adopted a breach-assumption approach that prevented and mitigated serious consequences.

We will now discuss three pillars of a holistic cybersecurity strategy. The first two pertain to trust minimization, while the third relates to anticipating and countering breaches.

### *Pillar I: Standardization*

Standardization is an important pillar in the cybersecurity domain. It provides a common set of guidelines, requirements, and recommendations in a transparent, verifiable, and reproducible manner. Standardization provides experts and laymen, businesses, regulators, and customers with a clear and common understanding of good versus bad. Once set, these common guidelines, requirements, and recommendations are continuously validated and verified by operators and regulators in the domain or industry covered.

The 3rd Generation Partnership Project (3GPP) is the standardization body responsible for

the development of 5G standards. Headquartered in France, it coordinates global standard-setting activities for seven national or regional telecom standards groups. Within 3GPP, the SA3 working group is dedicated to the development of security specifications. The SA3 working group includes vendors and operators from around the world. They work together to define cybersecurity enhancements and mitigations that address the risks and challenges identified through a comprehensive risk assessment.<sup>24</sup> In addition, other standardization bodies, such as the European Telecommunications Standards Institute (ETSI), develop and define the security specifications for some of the underlying technologies, such as network function virtualization (NFV),<sup>25</sup> which drive 5G.

Both 3GPP and ETSI have worked extensively on 5G security standards. 3GPP, for instance, developed security enhancements including an overall 5G security architecture, a new 5G key management scheme, enhanced radio access network (RAN) security with user plan integrity protection, network slicing security, network domain security, and management security and cryptographic algorithms.

Representatives of the U.S. government have expressed concerns about the security and reliability of 5G networks. However, scholars at prominent U.S. think tanks noted<sup>26</sup> that the United States has not actively participated at meetings where security standards are being set. Presently, European and Asian vendors account for over 95 percent of all 3GPP SA3 security-related proposals. During the last four years (2016-2019), Chinese vendors submitted over 1,600 5G security proposals alone. Conversely, during the same period, the United States only put forward a handful.

This is seemingly about to change. In May 2020, the Department of Defense (DOD) published its 5G Strategy document<sup>27</sup> acknowledging that "DOD has not engaged with the governance bodies that set mobile wireless industry standards." DOD observed

that, “to promote high-quality, protected, and reliable 5G devices and applications, the U.S. must play a lead role in shaping information and communications technology standards.”

5G standards will continuously evolve in subsequent 3GPP standards releases.<sup>28</sup> In mid-June, the Department of Commerce issued a new rule<sup>29</sup> allowing U.S. companies to work with Huawei on 5G standardization. Active involvement of the U.S. government and U.S. companies in security standardization will help to ensure that national-level security requirements are captured and reflected in the evolving standards.

### *Pillar II: Verification and Testing: Security Assurance Specifications [SCAS]*

Given the sophistication and resources of a small number of nation states and their capability to virtually implant hidden functionality in hardware and software, it is important that everyone’s products be subject to scrutiny to manage the real risk in cyberspace.

Verification and testing align with the principle of trust minimization and are therefore an essential part of a holistic, risk-mitigation strategy. Verification ensures that products and services provided by any vendor satisfy a set of well-defined requirements, thereby reducing the risk that a product behavior is inconsistent with the agreed specification, including in failure scenarios.

Security testing goes a step further by ensuring that the system security properties are not violated even under hostile and/or unpredictable conditions. Various security certification schemes have developed over the past 30 years for the evaluation of vendors’ and operators’ security posture. These include product-specific standards efforts such as ISO 15408 (Common Criteria) and GSMA/3GPP NESAS/SCAS, as well as company-level risk management schema such as ISO/IEC 270xx, ISO/IEC 28000, and ISO 22301, to name a few.

3GPP and GSMA introduced two new enhancements aimed at increasing operators’ security assurance in 5G products with transparency; SCAS—SeCurity Assurance Specifications, and NESAS—Network Equipment Security Assurance Scheme.<sup>30</sup> Together these represent a major contribution toward clear requirements and an independent testing regime for telecommunications equipment.

The work done to date by ISO, 3GPP, or GSMA should be applauded and supported, but it is essential that the collaborative effort continues forward with even broader, more robust input. Currently, operators and vendors do not have clear, comprehensive, standards-based guidance about what equipment they will be allowed to deploy in various countries around the world. 5G verification and testing is a work in progress, which needs additional collaborators.

As is the case for standards-setting, the United States has contributed little to discussions on verification and testing. Such security assurance frameworks would increase business certainty and efficiency, improve the security posture of operators and vendors, and promote transparency. On June 3, 2020 DOD announced, as part of its 5G Strategy, seven new locations for 5G testing.<sup>31 32</sup> 5G Core security experimentation will take place at Joint Base San Antonio. This development, we feel, puts the United States in a position to help drive the development, strengthening, and adoption of global security standards and testing regimes.

### *Pillar III: Multi-Level Cyber Resiliency*

In 5G networks, developing cyber-resilient systems requires the participation of all key stakeholders. The five main stakeholders in the 5G network are mobile network operators (MNOs), suppliers of services, equipment vendors, vertical industries, and governments. A multi-level cyber-resiliency strategy articulates goals for each of these stakeholders. It also identifies inter-dependencies between stakeholders at the federal and state levels (for example, when a single

network hub is shared by multiple operators, which when compromised may pose a national-level risk).

The National Institute of Standards and Technology (NIST) defines cyber resiliency as, “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”<sup>33</sup> Cyber resiliency derives from the breach-assumption design principle. It acknowledges that despite standardization and testing, system defenses will be breached. According to NIST; “modern systems are large and complex entities and as such, adversaries will always be able to find and exploit weaknesses and flaws in the systems.”

Cyber-resiliency is a realistic, rational approach that has been endorsed and advocated by some of the main agencies in the U.S. government. The U.S. Defense Science Board Task Force has stated that, “susceptibility to the advanced cyber threat by the Department of Defense is also a concern for public and private networks. Cyber resiliency is a critical factor.”<sup>34</sup>

Resiliency does not ensure full system integrity. But implemented correctly, it ensures that systems will be able to perform their most critical tasks. “From the perspective of cyber resiliency, system elements or constituent systems that are less critical to mission or business effectiveness can be sacrificed to contain a cyber-attack and maximize mission assurance,” NIST advises.

The concept of cyber resiliency is a flexible one that can be adapted to various scenarios. Every organization has different goals and priorities, so each organization has to determine what its mission-critical tasks are. This definition of priorities informs network designers of the resiliency objectives. A top objective might be, “Preclude the successful execution of an attack or the realization of adverse conditions.” But at another organization, the top priority could be, “Restore as much mission or business functionality as possible after adversity.”

To achieve their cyber-resiliency goals, network designers can choose from a wide array of proven techniques. Below are some of the techniques relevant to 5G security:

- Contextual Awareness; construct and maintain current and correct representations of the system’s security posture, revealing patterns or trends in adversary behavior.
- Analytic Monitoring; maximizes the ability to detect potentially adverse conditions and identify potential or actual damage.
- Coordinated Protection; requires an adversary to overcome multiple safeguards (i.e., implement a strategy of defense-in-depth), increasing the cost to the adversary and raising the likelihood of detection.
- Deception; hide critical assets from adversary or expose covertly tainted assets.
- Substantiated Integrity; detect attempts by an adversary to deliver compromised data, software, or hardware, as well as successful modification or fabrication.

Resources availability is one of the components of cyber-resiliency. This essentially refers to the ability to obtain critical system components even in times of crisis. The early days of the COVID-19 pandemic, when countries—even close allies—were hoarding medical supplies, served as a reminder of the importance of ensuring critical resources availability even under the most abnormal circumstances. To do this national governments need to systematically identify key components that need to be stored and for how long. For a superpower like the United States, it may in addition be appropriate to have at least some capability for strategic local manufacturing. This is the approach that is apparently being followed with Taiwan Semiconductor,<sup>35</sup> a critical supplier of electronic components, which has agreed—in principle—to build a plant in Arizona.

With a well-designed cyber-resiliency strategy, countries can be predominantly vendor-agnostic in cybersecurity terms. The United States could potentially allow any vendors, regardless of their state of origin, to be in any section of the network, including the network core. While this may sound risky to some, especially given the current political environment, this conclusion is built on analysis by world experts, as well as on a rich foundation of sound academic work.

In the next section, we look at supplier diversity. This is one of the most frequently cited elements of a cyber resiliency strategy. As we will see below, it is not primordial in importance, and it is certainly not a cure-all.

## The Pitfalls of Relying on Vendor Diversity

Politicians and the media sometimes cite supplier diversity as a silver bullet to address cybersecurity risks. It was mentioned prominently in the EU 5G toolbox released earlier this year.<sup>36</sup> In fact, supplier diversity plays a relatively minor role in cybersecurity. And if misunderstood or poorly implemented, supplier diversity can actually become a threat to network integrity.

Diversity is only one of fourteen resiliency techniques listed both by NIST and MITRE.<sup>37</sup> According to NIST, diversity encompasses six different sub-categories, including architectural diversity, design diversity, synthetic diversity, information diversity, path diversity, and of course supply chain diversity.

Diversity can enhance cyber resiliency, but it can also undermine it. In its cyber-resiliency design principles document,<sup>38</sup> MITRE noted that,

Diversity can be problematic in several ways: first, it can increase the attack surface. Rather than trying to compromise a single component and propagate across all such components, an adversary can attack any component in the set of alternatives,

looking for a path of least resistance to establish a foothold.

Second, it can increase demands on developers, system administrators, maintenance staff, and users, by forcing them to deal with multiple interfaces to equivalent components. This translates into increased lifecycle costs. (These costs have historically been acceptable in some safety-critical systems.) This can also increase the risk that inconsistencies will be introduced, particularly if the configuration alternative for the equivalent components are organized differently.

Third, diversity can be more apparent than real (e.g., multiple different implementations of the same mission functionality all running on the same underlying OS, applications which reuse software components). Thus, analysis of the architectural approach to using diversity is critical.

While we understand why supplier diversity is prominent in public discourse on 5G security, its importance must be kept in perspective.

## Network Resiliency Under Extreme Conditions

Modern military conflicts put communication networks under extreme duress. The U.S. military can resort to alternative and highly robust systems when necessary. We very briefly present some examples below.

The Defense Advanced Research Projects Agency (DARPA) has been working on mobile ad hoc networks (MANET)<sup>39</sup> since the early 1970s. These networks can be deployed in hostile environments ensuring the bandwidth requirements of U.S. forces would not be impacted by enemy threats. And low-orbit, high-speed satellite technology, such as those currently being developed by U.S. vendors,<sup>40</sup>

can be further enhanced and secured to satisfy current and future availability, confidentiality, and integrity requirements.

Resilient-system design is another tool that could be used on actual or likely battlefields. Military and intelligence agencies are proficient at building applications and services that can share information using multiple concurrent communication paths based on the networks' availability. This ensures that if network disruptions occur in one operator or in multiple operators, communication channels will still operate, even under hostile circumstances.

To enhance the resiliency and survivability of U.S. military networks and foreign networks that support the U.S. military in other countries requires investment in technology and personnel. Rather than spending tens of billions of dollars to acquire or subsidize Nokia or Ericsson, we propose that U.S. network resiliency would be better served by spending on refining and deploying technologies that can survive hostile environments, developing people who can build and operate such networks, and conducting R&D to develop better tools and protocols to achieve greater assurance.

## Conclusion

Excluding certain vendors while trusting others without assessing and addressing real cybersecurity risk, makes no sense from an economic or cybersecurity perspective. The United States is so intent on blocking Huawei from U.S. and allies' networks that it is considering alternatives that could cost tens of billions of dollars; buying or investing in Nokia or Ericsson, or both, or investing in an alternative U.S. company or consortium, or some alternative technology. Opposition to Huawei bridges the acrimonious political divide in the United States like few other contemporary issues.

Trustworthiness does not play a role in cybersecurity. What matters far more is the transparency

of telecom suppliers' operations, including whether and how they provide ongoing support to the operator after equipment is installed. Selecting a supplier should be based on the quality and reliability of its products, their demonstrable conformance to standards and best practices, as well as compliance with regulatory and contractual requirements.

Some have said candidly about Huawei that "it is not about the company, it is about the country." Given the availability of trustworthy, transparent and—as seen earlier in this article—proven risk-mitigation mechanisms, the U.S. government's decision to ban Chinese equipment vendors appears clouded by geopolitical concerns; namely China's rise economically, militarily, and technologically.

Banning vendors reduces competition and ironically increases the cybersecurity risk; the UK's Intelligence and Security Committee (ISC) stated in July 2019 that, "limiting the field to just two vendors,... would increase over-dependence and reduce competition, resulting in less resilience and lower security standards."<sup>41</sup> <sup>42</sup> We believe that global vendors play an essential role in the competitive landscape, bringing unique expertise, experience, and knowledge. Greater competition brings multiple benefits; greater innovation, lower prices, and—when well-implemented—greater resilience.

Huawei's top executives have stated that they are interested in talking with the U.S. government about how the company can address cybersecurity concerns and demonstrate that neither Huawei products nor its employees are subject to the undue influence of the Chinese (or any other) government. Huawei would discuss manufacturing in the United States,<sup>43</sup> opening Huawei to independent testing pursuant to recognized standards and best practices for telecom equipment,<sup>44</sup> or licensing Huawei's 5G technology to a U.S. company or consortium.<sup>45</sup>

If domestically fostering a vibrant technology and telecom sector is the policy of the United States, then the way forward is a tried and true one: Form



a private sector-led, public-private partnership to develop and implement a U.S. industrial technology innovation strategy. This will involve investing in R&D, providing sectoral incentives, funding university research, attracting the smartest minds in the world, and encouraging foreign investment.

It is not clear what the U.S. government will do next. But with trade tensions poised to weaken global growth, and roughly half the world's population still lacking internet access, one can hope that Washington will begin focusing on how to promote the spread of safe digital technology. **PRISM**

## Endnotes

<sup>1</sup> Thomas Donahue, "The Worst Possible Day: U.S. Telecommunications and Huawei," *PRISM* 8.3, (2019):15, [https://ndupress.ndu.edu/Portals/68/Documents/prism/prism\\_8-3/prism\\_8-3.pdf](https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3.pdf), p. 15.

<sup>2</sup> Liam Tung, "Target hackers hit air-conditioning firm first as a way in," *ZDNet*, February 6, 2014, <https://www.zdnet.com/article/target-hackers-hit-air-conditioning-firm-first-as-a-way-in/>.

<sup>3</sup> Target Annual Report, (2016): 44, [https://corporate.target.com/\\_media/targetcorp/annualreports/2016/pdfs/target-2016-annual-report.pdf](https://corporate.target.com/_media/targetcorp/annualreports/2016/pdfs/target-2016-annual-report.pdf).

<sup>4</sup> Lily Hay Newman, "Inside the Unnerving Supply Chain Attack That Corrupted CCleaner," *Wired*, April 17, 2018, <https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/>.

<sup>5</sup> x86 refers to Intel's CPU architecture developed by Intel. X86 is used in hundreds of millions of computers in the U.S. and worldwide.

<sup>6</sup> Lindsey O'Donnell, "ZombieLoad: How Intel's Latest Side Channel Bug Was Discovered and Disclosed," *Threatpost*, May 20, 2019, <https://threatpost.com/zombieload-how-intels-latest-side-channel-bug-was-discovered-and-disclosed/144849/>.

<sup>7</sup> Zhao Juntao, "President of Ericsson China: epidemic spread, global 5G demand has not been weakened," interview by Liu Yuying, March 30, 2020, <https://www.tellerreport.com/business/2020-03-30---president-of-ericsson-china--epidemic-spread--global-5g-demand-has-not-been-weakened-.SyeikYbyvU.html>.

<sup>8</sup> Nokia Corporation, *Nokia and China Huaxin sign definitive agreements for creation of new Nokia Shanghai Bell joint venture*, May 18, 2017, <https://www.nokia.com/about-us/news/releases/2017/05/18/nokia-and-china-huaxin-sign-definitive-agreements-for-creation-of-new-nokia-shanghai-bell-joint-venture/>.

<sup>9</sup> Telecoms, "Nokia and Ericsson have links to China's Communist Party," *Telecomstchnews*, August 13, 2018, <https://telecomstchnews.com/news/2018/aug/13/nokia-ericsson-china-communist-party/>.

<sup>10</sup> Defense Science Board, "Defense Applications of Fifth Generation Network Technology," June 24, 2019, <https://www.hsdl.org/?abstract&did=828623>.

<sup>11</sup> The GSM Association (GSMA) represents the interests of mobile network operators worldwide. Its members include over 750 mobile operators. Other companies active in the telecommunications industry also participate in GSMA activities.

<sup>12</sup> GSMA, "The Mobile Economy 2020" (2020), <https://www.gsma.com/r/mobileeconomy/>.

<sup>13</sup> Tom Demerly, "U.S. Navy Now Jamming GPS Over Six States and 125,000 Square Miles," *The Aviationist*, January 23, 2020, <https://theaviationist.com/2020/01/23/u-s-navy-now-jamming-gps-over-six-states-and-125000-square-miles/>.

<sup>14</sup> David Axe, "Why and How Russia Is Jamming American Fighter Jets Near Iran," *The National Interest*, January 17, 2020, <https://nationalinterest.org/blog/buzz/why-and-how-russia-jamming-american-fighter-jets-near-iran-115021>.

<sup>15</sup> European Commission and the Finnish Presidency of the Council of the EU, "Member States publish a report on EU coordinated risk assessment of 5G networks security," October 9, 2019, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_6049](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049).

<sup>16</sup> The 3rd Generation Partnership Project, better known as 3GPP, is a confederation of standards organizations which develop protocols for mobile telecommunications. 3GPP will be described in more details further down in the section on standardization.

<sup>17</sup> The European Telecommunications Standards Institute is one of the leading standard-setting organizations worldwide. Will be discussed later in this paper.

<sup>18</sup> The SA3 working group within 3GPP is dedicated to the development of security specifications.

<sup>19</sup> Tafazolli is Professor of Mobile and Satellite Communications at the University of Surrey, Director of the Institute of Communication Systems, and Director of the 5G Innovation Centre.

<sup>20</sup>The hearing focused on the U.K.'s telecommunications infrastructure. It was organized by the Science and Technology Committee of the House of Commons. Minutes available here: <http://data.parliament.uk/writenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/uk-telecommunications-infrastructure/oral/102931.html>.

<sup>21</sup>Jeffrey J. Guy, "Who coined "assumption of breach?," *Armatum Networks*, May 11, 2012, <http://armatum.com/blog/2012/who-coined-assumption-of-breach/>.

<sup>22</sup>Ernie Hayden, "Data breach protection requires new barriers," *TechTarget*, May 2013, <https://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers>.

<sup>23</sup>John Miller, "FBI fighting two-front war on growing enemy - cyber-espionage," *CBS News*, May 23, 2012, <https://www.cbsnews.com/news/fbi-fighting-two-front-war-on-growing-enemy-cyber-espionage/>.

<sup>24</sup>3GPP, "3GPP Specifications per TSG/WG," <https://www.3gpp.org/DynaReport/TSG-WG--S3.htm>.

<sup>25</sup>ETSI, "Network Functions Virtualisation (NFV)," <https://www.etsi.org/technologies/nfv>.

<sup>26</sup>Theresa Hitchens, "US Risks Losing 5G Standard Setting Battle To China, Experts Say," *Breaking Defense*, May 11, 2020, <https://breakingdefense.com/2020/05/us-risks-losing-5g-standard-setting-battle-to-china-experts-say/>.

<sup>27</sup>Department of Defense, "Department of Defense (DoD) 5G Strategy (U)," May 2, 2020, [https://www.cto.mil/wp-content/uploads/2020/05/DoD\\_5G\\_Strategy\\_May\\_2020.pdf](https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf).

<sup>28</sup>During the development of the 3GPP 5G security standards, Dr. Anand R. Prasad, then chairman of the 3GPP SA3, noted that "the reassessment of other security threats such as attacks on radio interfaces, signaling plane, user plane, masquerading, privacy, replay, bidding down, man-in-the-middle and inter-operator security issues have also been taken in to account for 5G and will lead to further security enhancements." [https://www.3gpp.org/news-events/1975-sec\\_5g](https://www.3gpp.org/news-events/1975-sec_5g).

<sup>29</sup><https://www.cnet.com/news/us-firms-now-allowed-to-work-with-huawei-on-5g-standards/>.

<sup>30</sup>SCAS is a set of security specifications for 5G equipment and NESAS defines security requirements and an assessment framework to audit the vendor's product development and lifecycle management process. Vendors would verify their products in special ISO 17025-certified, GSMA-recognized testing labs. These new security-assurance schemes provide additional validation that products adhere to the security specifications, further minimizing the need to rely on the trusted vendor approach. Various leading European regulators have been evaluating NESAS as well as other cyber-security certification schemes as potential candidates for 5G certification.

<sup>31</sup>Corinne Reichert, "US Defense Department ramps up 5G testing," *CNET*, June 4, 2020, <https://www.cnet.com/news/us-defense-ramps-up-5g-testing/>.

<sup>32</sup>Department of Defense, "DOD Names Seven Installations as Sites for Second Round of 5G Technology Testing, Experimentation," June 3, 2020, <https://www.defense.gov/Newsroom/Releases/Release/Article/2206761/dod-names-seven-installations-as-sites-for-second-round-of-5g-technology-testin/>.

<sup>33</sup>Ron Ross, "Building Cyber Resilient Systems," National Institute of Standards and Technology, <https://csrc.nist.gov/CSRC/media/Presentations/building-cyber-resilient-systems/images-media/Building-Cyber-Resiliency-MITRE-20180508.pdf>.

<sup>34</sup>Ron Ross, Victoria Pillitteri, Richard Graubart Deborah Bodeau and Rosalie McQuaid, "Developing Cyber Resilient Systems: A Systems Security Engineering Approach," National Institute of Standards and Technology, November 2019, <https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final>.

<sup>35</sup>Debby Wu and Ian King, "Taiwanese Chipmaker Plans to Build \$12 Billion Factory in Arizona," *Time*, May 15, 2020, <https://time.com/5837274/tsm-chip-plant-arizona/>.

<sup>36</sup>European Commission, "Secure 5G networks: Questions and Answers on the EU toolbox," January 29, 2020, [https://ec.europa.eu/commission/presscorner/detail/en/qanda\\_20\\_127](https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127).

<sup>37</sup>MITRE is a federally funded research and development corporation. MITRE describes its main areas of research as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience.

<sup>38</sup>Deborah Bodeau and Richard Graubart, "Cyber Resiliency Design Principles," *MITRE*, January 2017, <https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf>.

<sup>39</sup>DARPA, "DARPA Seeks Clean-Slate Ideas For Mobile Ad Hoc Networks (MANETs)," April 4, 2013, <https://www.darpa.mil/news-events/2013-04-30>.

<sup>40</sup>Kristin Cooke, "SpaceX Satellite Internet: What You Need to Know about Starlink," *Satelliteinternet*, May 8, 2020, <https://www.satelliteinternet.com/providers/starlink/>.

<sup>41</sup>Kat Hall, "Excluding Huawei from UK's 5G will harm security, MPs warn," *The Register*, July 19, 2019, [https://www.theregister.co.uk/2019/07/19/excluding\\_huawei\\_from\\_5g\\_will\\_harm\\_security\\_mps\\_warn/](https://www.theregister.co.uk/2019/07/19/excluding_huawei_from_5g_will_harm_security_mps_warn/).

<sup>42</sup>Full report: <https://www.parliament.uk/documents/other-committees/intelligence-security/Critical-National-Infrastructure-Report.pdf>.

<sup>43</sup>Reuters, "Huawei to Build First European 5G Factory in France to Soothe Western Nerves," *Voice of America*, February 27, 2020, <https://www.voanews.com/silicon-valley-technology/huawei-build-first-european-5g-factory-france-soothe-western-nerve>.

<sup>44</sup>Aurel Dragan, "Huawei opens a Center for Cyber Security Transparency in Bruxelles," *Business Review*, June 3, 2019, <https://business-review.eu/tech/huawei-opens-a-center-for-cyber-security-transparency-in-bruxelles-197636>.

<sup>45</sup>Arjun Kharpal, "Huawei's offer to license 5G tech to US firm to create an American rival is still 'on the table'," *CNBC*, February 26, 2020, <https://www.cnb.com/2020/02/26/huawei-reiterates-offer-to-license-5g-tech-to-us-firm-to-create-rival.html>.



*"As China becomes more and more powerful, it will flex its muscles and use them more."  
(Romolo Tavani via IStock)*

# Is China Expansionist?

By Kishore Mahbubani<sup>1</sup>

The Chinese soldier who pushed the Indian Colonel Santosh Babu (who tragically died) and thereby triggered the violent clash between Chinese and Indian soldiers in mid-June 2020 should be court-martialed. Both sides suffered casualties, the worst since 1975. This one push by one Chinese soldier has set back China-India relations severely, undermining all the good work that had been done over several years by Prime Minister Manmohan Singh and Premier Wen Jiabao, as well as by Prime Minister Narendra Modi and President Xi Jinping. Equally importantly, it has reinforced a growing belief, especially in the western world, that as China's economy becomes stronger and stronger, China will abandon its "peaceful rise" and behave as a militarily expansionist power. This could well happen. It would be naive to believe otherwise. However, a deep study of Chinese history and culture would also show that the continuation of a peaceful rise is equally plausible.

One key point needs to be emphasised at the outset. As China becomes more and more powerful, it will flex its muscles and use them more. This is normal great power behaviour. Indeed, the term "benevolent great power" is an oxymoron. No great power is altruistic. All great powers will pursue their national interests. So will China. However, while the goals of all great powers are similar, the methods might differ. China has become and will become more assertive. Yet it need not become more aggressive. These two words "assertive" and "aggressive" are often confused with each other. A study of the great power behaviour of America and China will illustrate the differences.

Graham Allison has wisely warned his fellow Americans to be careful in what they wish for China. He writes, "Americans enjoy lecturing Chinese to be 'more like us.' Perhaps they should be more careful what they wish for. Historically how have emerging hegemony behaved? To be more specific, how did Washington act just over a century ago when Theodore Roosevelt led the U.S. into what he was supremely confident would be an American century? [. . .] In the decade that followed his arrival in Washington, the U.S. declared war on Spain, expelling it from the Western Hemisphere and acquiring Puerto Rico, Guam, and the Philippines; threatened Germany and Britain with war unless they agreed to settle the disputes on American terms; supported an insurrection in Colombia to create a new country, Panama, in order to build a canal; and declared itself the

---

<sup>1</sup>Kishore Mahbubani is a Distinguished Fellow at the Asia Research Institute (ARI), National University of Singapore (NUS) and is a former Singaporean diplomat.

policeman of the Western Hemisphere, asserting the right to intervene whenever and wherever it judged necessary—a right it exercised nine times in the seven years of Roosevelt’s presidency alone.”<sup>2</sup>

If America’s behavior during its period of emergence as a great power conforms to the historical norm, China’s behaviour so far, defies the norm. Of the five permanent members of the UN Security Council (who represent the great powers), only one has not fought a war in forty years; China. Indeed, China has not even fired a bullet across its borders since a naval skirmish with Vietnam in 1989. The recent fighting between Chinese and Indian soldiers was brutal and savage. However, both sides adhered to their agreement not to use their firearms. Article VI of this agreement, signed in 1996, states, “Neither side shall open fire, cause bio-degradation, use hazardous chemicals, conduct blast operations or hunt with guns or explosives within two kilometers from the line of actual control.”<sup>3</sup> The strategic discipline shown by Chinese and Indian soldiers is commendable.

In contrast to China, in the last three decades, America has fought a war or been involved in military actions every year. The Congressional Research Service, an independent body, produced a study entitled, “Instances of Use of United States Armed Forces Abroad, 1798–2018.” In theory, there should have been a reduction in American interventions after the Cold War ended in 1989. This study demonstrates that in the 190 years preceding the end of the Cold War, American troops were deployed a total of 216 times, or 1.1 times per year on average. However, in the twenty-five years after the end of the Cold war, America increased its military interventions sharply and used its armed forces 152 times, or 6.1 times per year.<sup>4</sup>

John Mearsheimer has described what happened in his book, *The Great Delusion*. He writes, “With the end of the Cold War in 1989 and the collapse of the Soviet Union in 1991, the United States emerged as by far the most powerful country

on the planet. Unsurprisingly, the Clinton administration embraced liberal hegemony from the start, and the policy remained firmly intact through the Bush and Obama administrations. Not surprisingly, the United States has been involved in numerous wars during this period and has failed to achieve meaningful success in almost all of those conflicts.”<sup>5</sup> Stephen Walt adds, “U.S. military action has led directly or indirectly to the deaths of 250,000 Muslims over the past three decades (and that is a low-end estimate, not counting the deaths resulting from the sanctions against Iraq in the 1990s).”<sup>6</sup>

The big question here therefore is thus; why has China refrained from using its military in recent decades? What are the deeper roots of this pattern of behavior. Henry Kissinger has explained well why the Chinese avoid military options. He says, “[The] foundations [of China’s distinctive military theory] were laid during a period of upheaval, when ruthless struggles between rival kingdoms decimated China’s population. Reacting to this slaughter (and seeking to emerge victorious from it), Chinese thinkers developed strategic thought that placed a premium on victory through psychological advantage and preached the avoidance of direct conflict.”<sup>7</sup> Kissinger has accurately distilled the essence of the advice given by China’s master strategist Sun Tzu, who once said; “All warfare is based on deception. . . . Pretend inferiority and encourage his arrogance. . . . For to win one hundred victories is not the acme of skill. To subdue the enemy without fighting is the acme of skill.”<sup>8</sup>

If China were to try to make a case that it is inherently not a militaristic power, it would have many strong arguments to deploy. The first argument is historical. If Chinese civilization is inherently militaristic, this militaristic streak, especially the desire to conquer and subjugate other territories, would have surfaced long ago. Over the past two thousand years, China has often been the single strongest civilization in the Eurasian

landmass. If China was inherently militaristic, it would have and should have conquered territories overseas, as the European powers did. Future historians will, for example, marvel at the fact that even though Australia is geographically close to China, it was physically occupied and conquered by far more distant British forces. Indeed, had James Cook sailed directly, it would have taken him at least ninety days to reach Australia's Botany Bay, having departed from Plymouth Dockyard in August of 1768; counterfactually, were he instead to have sailed from China, he would have found himself ashore in Australia in just under thirty days.

This Chinese reluctance to conquer Australia and other overseas territories is not because China always lacked a navy. Before the Portuguese and

Spanish began the ruthless European policies of colonizing the world in the sixteenth century, the Chinese had by far the strongest navy in the world. At the start of the fifteenth century, nearly a hundred years before Christopher Columbus tried to find a route to the so-called Spice Islands, China sent out seven naval expeditions, under the remarkable leadership of Admiral Zheng He, a legendary Chinese figure. He traveled as far as Africa on ships that were far larger in size than the Portuguese or Spanish vessels: "The stars of the Chinese fleet were the treasure ships—sweeping junks, several stories high, up to 122 meters long and 50 meters wide. In fact they were about four times bigger than the 'Santa Maria,' the ship Columbus sailed to America on behalf of the Spanish crown."



Zheng He's fleet (Bruno Zaffani via Flickr)

Along the way, he did get into military battles. For example, in his voyages between 1409 and 1411, he “captured King Alagak-Konara (亞烈苦奈兒) of Ceylon and chose Yapanaina (耶巴乃那) to be the king instead,” and in his voyages between 1413 and 1415, he “captured Sekandar, (蘇幹刺) king of Sumatra (Atcheg) and then installed a new king.”<sup>9</sup>

Yet, quite remarkably, China did not conquer or occupy any overseas or distant territories. Singapore’s former foreign minister George Yeo remarked that, “throughout Chinese history, the Chinese have been averse to sending military forces far away. . . . In the 8th century, at the peak of China’s development during the Tang Dynasty, they had an army near the Fergana Valley in Central Asia, when the Abbasids were moving eastwards. They clashed. In the famous battle of Talas, the Abbasids defeated the Tang army, and the Chinese never crossed the Tianshan Mountains again in their history.”<sup>10</sup>

The relatively peaceful streak of the Han Chinese people is brought out when their behavior is compared with some of their neighbors. One of the most powerful and terrifying imperialist expansions in human history was carried out by China’s immediate neighbors in the North, the Mongols. Led by the brutal and dynamic Genghis Khan, these relatively small Mongolian tribes (far smaller in population than the Chinese people) conquered not just China but almost all of Asia, becoming, in the 13<sup>th</sup> century, the only East Asian force to threaten an invasion of Europe. Yet the more powerful Chinese empire never emulated this conquering example of its neighbors.

The Mongols conquered and ruled China itself for over a century. In an article for the Asia Society, Jean Johnson writes that, “Genghis Khan moved his troops into the quasi-Chinese Chin-ruled north China in 1211, and in 1215 they destroyed the capital city. His son Ogodei conquered all of North China by 1234 and ruled it from 1229 to 1241.

Genghis Khan’s grandson, Kublai Khan, defeated the Chinese Southern Song in 1279, and for the first time all of China was under foreign rule. In 1271 Kublai Khan named his dynasty Yuan which means ‘origin of the universe.’ The Yuan dynasty in China lasted from 1279 to 1368.”<sup>11</sup> As a result, there was massive cross-fertilization between Mongolian and Chinese culture. In this process, the Mongols could have transferred their militaristic culture into the software of Chinese civilization. Instead, the opposite happened. The Chinese progressively civilized their Mongol rulers, and while Kublai Khan fought wars with China’s neighbors, he made no effort to conquer the world like his grandfather Genghis Khan tried to do.

What was the powerful anti-military DNA of Chinese civilization that eventually infected Mongol rulers? It probably goes back to Confucius. The Chinese have long had a saying that “just as good iron is not transformed into a nail; a good man is not made into a soldier.” At several points in the Analects, Confucius cautions against people who only have the strength of soldiers. In one dialogue, Zilu said, “Does the junzi [君子] prize valor?” The Master said, “The junzi gives righteousness the topmost place. If a junzi had valor but not righteousness, he would create chaos. If a small person has valor and not righteousness, he becomes a bandit.” In another dialogue, Zilu said, “Master, if you were put in charge of the three army divisions, then whom would you wish to have with you?” The Master said, “Those who fight tigers with their bare hands, wade across rivers, and are willing to die without regret—I would not want their company. I would certainly want those who approach affairs with fearful caution and who like to lay careful plans for success.”<sup>12</sup>

In contrast to American culture, where there is a strong built-in reverence for the man in uniform, Chinese culture has revered scholars more than soldiers, even though there are military figures



who are celebrated in folklore and literature for their patriotism and loyalty. Overall, there is an even greater reverence for the man who is skilled in both, encapsulated in the idea of 文武双全 (wén wǔ shuāng quán), that is, someone who is both a fine scholar and soldier.

Still all these arguments from history will not convince many who believe that China's recent behavior has demonstrated that it has a militaristic streak, and also lies about its military intentions and actions. For example, it is widely believed that Xi Jinping reneged on his promise not to militarize the South China Sea islands. In December 2016, the Wall Street Journal reported, "For a man who stood at the White House in September 2015 and promised not to militarize the South China Sea, Xi Jinping is sure doing a lot of militarizing."<sup>13</sup> In two articles for the Washington Post, John Pomfret wrote that, "China routinely makes commitments that it does not keep. Just remember Xi's 2015 promise to then-President Barack Obama not to militarize the islands it created in the South China Sea,"<sup>14</sup> and again that Xi "broke his promises to President Barack Obama not to militarize the seven Chinese-made islands in the South China Sea."<sup>15</sup> The Economist was perhaps the most forthright in its accusation of Xi's broken promise, declaring in April 2018, "Less than three years ago, Xi Jinping stood with Barack Obama in the Rose Garden at the White House and lied through his teeth. [. . .] China absolutely did not, Mr. Xi purred, 'intend to pursue militarisation' on its islands."<sup>16</sup>

If Xi had indeed made such a promise and reneged, it would only go to confirm a widespread belief in the West that China has become aggressive and expansionist. It would also confirm a belief that the Chinese are being perfidious and deceptive when they claim that China will rise peacefully. So what is true?

Few Americans can claim to know China as well as Ambassador Stapleton Roy. Born in China,

a fluent Mandarin speaker, Roy also served as the American ambassador to China from 1991 to 1995 and has stayed exceptionally well informed on U.S.-China relations. He explained what happened: In a joint press conference with President Obama on September 25, 2015, Xi Jinping had proposed a more reasonable approach on the South China Sea. Xi had supported full and effective implementation of the 2002 Declaration on the Conduct of Parties in the South China Sea, signed by China and all ten ASEAN members; had called for early conclusion of the China-ASEAN consultations on a Code of Conduct for the South China Sea; and had added that China had no intention of militarizing the Spratlys, where it had engaged in massive reclamation work on the reefs and shoals it occupied. Roy said that Obama missed an opportunity to capitalize on this reasonable proposal. Instead, the U.S. Navy stepped up its naval patrols. China responded by proceeding with militarization. In short, Xi did not renege on a promise. His offer was effectively spurned by the U.S. Navy.

While there is no question that China has restrained itself from militarily "aggressive" behaviour, it is also clear that China has become more "assertive" as it emerges as a new great power, using non-military means to project its power. When Norway conferred the Nobel Peace Prize to Chinese dissident Liu Xiaobo in 2010, Norway was put in diplomatic cold storage. Ties were cut. When the Australian Prime Minister called for an independent inquiry into the causes of COVID-19 in April 2020, China froze the imports of Australian barley. The use of economic means to pressure smaller countries is normal great power behaviour. The United States cut off World Bank loans to poor Ethiopia when it made the mistake of repaying high-interest loans to American banks. France punishes its former colonies in Africa when they fail to heed the wisdom of Paris.

It's also true that Chinese diplomacy has become assertive with the younger "wolf warrior"

diplomats issuing sharper statements and rebuttals. This has triggered a backlash. Yet, they are only shooting off sharp words, not bullets. As the old English proverb says, “sticks and stones may break my bones but words will never break me.” A world where pointed words replace bullets is a safer world.

Like other great powers, China is selective when it comes to conforming to international law. It respects the UN Convention on the Law of the Sea but walked away from the decision of the Law of the Sea Tribunal on the South China Sea. The United States also walked away from the World Court in 1986 when it decreed that the U.S. support for the Sandinistas in Nicaragua violated international law, including “not to use force against another State,” “not to intervene in its affairs,” “not to violate its sovereignty,” and “not to interrupt peaceful maritime commerce.”<sup>17</sup> The U.S. Ambassador to the UN then called the court a “semi-legal, semi-judicial, semi-political body, which nations sometimes accept and sometimes don’t.”<sup>18</sup>

There is one area where China takes a fierce stand: It will not brook any interference in its internal affairs. Hence, it will reject all foreign criticisms of its treatment of Uighurs or Hong Kong. So far, China has restrained its military responses to Hong Kong, unlike Prime Minister Jawaharlal Nehru of India, who reacted to personal appeals from President John F. Kennedy and Prime Minister Harold MacMillan by invading Goa. On the Uighurs, China’s position is technically correct under international law. The British government used a similar argument when the UN tried to investigate British crimes in Northern Ireland. The then British Foreign Secretary, Michael Stewart, told the UN that this would amount to interference in the internal affairs of the UK. This also explains why not a single Islamic state supported the western countries when they wrote a letter to the UN criticizing China’s treatment of the Uighurs. The record shows that only the West, which represents 12 percent of the world’s population, has been critical

of China’s internal behaviour. The remaining 88 percent have not joined this western crusade.

To explain the continued western suspicions of China, let me add a slightly provocative but historically accurate note. There is one deep-seated reason for the strong suspicions that western minds have about China. There has been buried deep in the unconscious of the western psyche an inchoate but real fear of the “yellow peril.” Since it is buried deep in the unconscious, it seldom surfaces. When senior American policymakers make their decisions on China, they can say with all sincerity that they are driven by rational, not emotional, considerations. Yet, to an external observer, it is manifestly clear that America’s reactions to China’s rise are influenced by deep emotional reactions, too. Just as individual human beings have difficulty unearthing the unconscious motives that drive our behavior, countries and civilizations also have difficulty unearthing their unconscious impulses.

It is a fact that the yellow peril has lain buried in western civilization for centuries. Napoleon famously alluded to it when he said, “Let China sleep; when she awakes she will shake the world.” Why did Napoleon refer to China and not to India, an equally large and populous civilization? Because no hordes of Indians had threatened or ravaged European capitals. By contrast, hordes of Mongols, a “yellow race,” had appeared at Europe’s doorstep in the thirteenth century. As Noreen Giffney recounts, “in 1235, Mongol armies invaded Eastern Europe and the Rus’ principalities between 1236 and 1242. [. . .] The Mongol onslaught was followed by a swift and mysterious withdrawal to the surprise and relief of westerners.”<sup>19</sup>

The latent fear of the yellow peril surfaces from time to time in literature and art. As a child living in a British colony, I read the popular Fu Manchu novels. They left a deep impression on me. Subconsciously, I began to believe that the personification of evil in human society came in the form of a

slant-eyed yellow man devoid of moral scruples. If I, as a non-westerner, could internalize this ethnic caricature, I suspect that these subconscious fears have also affected the reactions of American policymakers to the rise of China.

The strong anti-China mood that has swept through Washington, DC, may in part be the result of rational dissatisfaction with some of China's policies, probably as a result of the fear of China's unfamiliar culture, but also in part from deeper emotional undercurrents. As the former U.S. ambassador Chas Freeman has observed, "in their views of China, many Americans now appear subconsciously to have combined images of the insidious Dr. Fu Manchu, Japan's unnerving 1980s challenge to U.S. industrial and financial primacy, and a sense of existential

threat analogous to the Sino-phobia that inspired the Anti-Coolie and Chinese Exclusion Acts."<sup>20</sup>

Given the psychological reality of this yellow peril undercurrent, American people need to question how much their reactions to China's rise result from hard-headed rational analysis and how much is a result of deep discomfort with the success of a non-Caucasian civilization. We may never know the real answer, as these struggles between reason and emotion are playing out in subconscious terrains. Still, we should thank Kiron Skinner, a former Director of Policy Planning in the State Department of the Trump Administration, for alluding to the fact that such subconscious dimensions are at play here. As she said in her testimony before Congress, "It's the first time that we will have a great power



A large temporary monument in Tiananmen Square marking the 90th anniversary of the Chinese Communist Party. (Haha169 via Wikimedia Commons)

competitor that is not Caucasian.” The time has come for an honest discussion of the “yellow peril” dimension in U.S.-China relations. The best way to deal with our subconscious fears is to surface them and deal with them.

China’s re-emergence as a great power should not have come as a surprise. From the years 1 to 1820, the two largest economies were always those of China and India. Their return to great power status was perfectly natural. However, the speed of China’s return has been unnatural. Its speed of return is off the charts. In 1980, its economy, in purchasing power parity (PPP) terms was one-tenth the size of America. By 2014, it had become larger.

As its economy grew, so too did its defense budget. China today is a much stronger military power. The balance of power vis-à-vis America has shifted drastically. It has also spent its defense budget relatively wisely. China is focused on using the strategies adopted by a weaker military power engaged in asymmetric warfare. China spends its budget on sophisticated land-based missiles that could make U.S. aircraft carrier battle groups utterly ineffective. An aircraft carrier may cost \$13 billion to build. China’s DF-26 ballistic missile, which the Chinese media claims is capable of sinking an aircraft carrier, costs a few hundred thousand dollars. New technology is also helping China to defend itself against aircraft carriers. Professor Timothy Colton of Harvard University told me that aircraft carriers become “sitting ducks” when they face the threat of hypersonic missiles, which are maneuverable and fly at tremendous speed, at varying altitudes.

The discomfort about China’s reemergence as a major military power is perfectly understandable. China has clearly emerged as a more formidable military competitor. However, the long history of China suggests that China will be very careful about using its military capabilities. The recent tragic episode on the China-India border would have only reinforced the Chinese belief that the use of military force

as a first option is unwise. The real competition between America and China will be in the economic and social fields. The main reason why America successfully defeated the mighty Soviet Union without fighting a war with it is that the American economy outperformed the Soviet economy. The threat by President Ronald Reagan to outspend the Soviet Union in military expenditures eventually convinced Soviet Premier Mikhail Gorbachev to sue for peace. Could the same happen between America and China? Or could the opposite happen? Most projections show that within a decade or two, China will have a larger economy in nominal market terms. Should America change its strategy when it becomes the number two economy in the world? Or should it do so beforehand? Equally, should it heed this famous advice of President Dwight Eisenhower? As he told the American Society of Newspaper Editors, “every gun that is made, every warship launched, every rocket fired signifies, in the final sense, a theft from those who hunger and are not fed, those who are cold and are not clothed.”<sup>21</sup>

There is absolutely no doubt that China will emerge as a formidable geopolitical competitor of the United States. It would be wise to plan for this outcome. Yet, as George Kennan wisely advised at the beginning of the titanic contest against the Soviet Union, the outcome of the contest would not be determined by the competition in the military realm. Instead, he said that the outcome would be determined by the ability of America to “create among the peoples of the world generally the impression of a country which knows what it wants, which is coping successfully with the problems of its internal life and with the responsibilities of a world power, and what has a spiritual vitality capable of holding its own among the major ideological currents of the time.”<sup>22</sup>

Kennan’s emphasis on “spiritual vitality” is even more relevant in the ongoing geopolitical contest with China. It is this dimension that will determine the outcome of the contest against China, not the

military dimension. Since China has the world's oldest civilisation, the only civilisation to have recovered from four major shocks in its history, it would be a serious mistake for an American policy-maker to underestimate the strength and resilience of Chinese civilisation in the peaceful contest that will take place between the two powers. PRISM

## Endnotes

<sup>1</sup> Kishore Mahbubani, is the author of the book, *Has China Won?* (Public Affairs, 2020). This essay contains excerpts from *Has China Won?*

<sup>2</sup> Graham Allison, *Destined for War: Can American and China escape Thucydides's Trap?* New York: Houghton Mifflin Harcourt, 2017.

<sup>3</sup> "Agreement Between the Government of the Republic of India and the Government of the People's Republic of China on Confidence-Building Measures in the Military Field Along the Line of Actual Control in the India-China Border Areas," November 29, 1996, [https://peacemaker.un.org/sites/peacemaker.un.org/files/CN%20IN\\_961129\\_Agreement%20between%20China%20and%20India.pdf](https://peacemaker.un.org/sites/peacemaker.un.org/files/CN%20IN_961129_Agreement%20between%20China%20and%20India.pdf).

<sup>4</sup> Congressional Research Service, "Instances of Use of United States Armed Forces Abroad, 1798–2018," December 28, 2018, <https://www.hsdl.org/?view&did=819747>.

<sup>5</sup> John J. Mearsheimer, *The Great Delusion: Liberal dreams and international realities*, New Haven: Yale University Press, 2018.

<sup>6</sup> Stephen M. Walt, "The Myth of American Exceptionalism," *Foreign Policy*, October 11, 2011, <https://foreignpolicy.com/2011/10/11/the-myth-of-american-exceptionalism/>.

<sup>7</sup> Henry Kissinger, *On China*, New York: Penguin, 2011, 25.

<sup>8</sup> *ibid.*

<sup>9</sup> Andreas Lorenz, "Hero of the High Seas," *Der Spiegel*, August 29, 2005, <https://www.spiegel.de/international/spiegel/china-s-christopher-columbus-hero-of-the-high-seas-a-372474-2.html>.

<sup>10</sup> George Yeo, "A Continuing Rise of China," *Business Times* (Singapore), October 30, 2019, <https://www.businesstimes.com.sg/opinion/thinkchina/a-continuing-rise-of-china>.

<sup>11</sup> Jean Johnson, "The Mongol Dynasty," *Asia Society*, <https://asiasociety.org/education/mongol-dynasty>.

<sup>12</sup> Confucius, "The Analects of Confucius," trans. Robert Eno, 2015, <https://chinatxt.sitehost.iu.edu/Resources.html>.

<sup>13</sup> Thomas Shugart, "China Arms Its Great Wall of Sand," *Wall Street Journal*, December 15, 2016, <https://www.wsj.com/articles/china-arms-its-great-wall-of-sand-1481848109>.

<sup>14</sup> John Pomfret, "A China-U.S. Truce on Trade Only Scratches the Surface of a Broader Conflict," *Washington Post*, December 3, 2018, [https://www.washingtonpost.com/opinions/2018/12/03/china-us-truce-trade-only-scratches-surface-broader-conflict/?utm\\_term=.0e6e9a186448](https://www.washingtonpost.com/opinions/2018/12/03/china-us-truce-trade-only-scratches-surface-broader-conflict/?utm_term=.0e6e9a186448).

<sup>15</sup> John Pomfret, "How the World's Resistance to China Caught Xi Jinping Off Guard," *Washington Post*, December 21, 2018, [https://www.washingtonpost.com/opinions/2018/12/21/how-worlds-resistance-china-caught-xi-jinping-off-guard/?utm\\_term=.105ab7ca5227](https://www.washingtonpost.com/opinions/2018/12/21/how-worlds-resistance-china-caught-xi-jinping-off-guard/?utm_term=.105ab7ca5227).

<sup>16</sup> "China Has Militarised the South China Sea and Got Away with It," *The Economist*, June 21, 2018, <https://www.economist.com/asia/2018/06/21/china-has-militarised-the-south-china-sea-and-got-away-with-it>.

<sup>17</sup> "CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA," *International Court of Justice*, 27 June 1986, <https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf>.

<sup>18</sup> Graham Allison, "Heresy to say great powers don't bow to tribunals on Law of the Sea?" *Straits Times*, 16 July 2016, <https://www.straitstimes.com/opinion/heresy-to-say-great-powers-dont-bow-to-international-courts>.

<sup>19</sup> Noreen Giffney, "Monstrous Mongols," *Postmedieval: A Journal of Medieval Cultural Studies* 3, no. 2, (May 2012): 227–245.

<sup>20</sup> Chas W. Freeman Jr., "On Hostile Coexistence with China," May 3, 2019, <https://chasfreeman.net/on-hostile-coexistence-with-china/>.

<sup>21</sup> Dwight D. Eisenhower, "The Chance for Peace," Washington D.C., April 16, 1953, [http://www.edchange.org/multicultural/speeches/ike\\_chance\\_for\\_peace.html](http://www.edchange.org/multicultural/speeches/ike_chance_for_peace.html).

<sup>22</sup> George Kennan (X), "The Sources of Soviet Conduct," *Foreign Affairs*, July 1947.

An Interview with

# General Joseph Votel, USA (Ret)

President and CEO of Business Executives for National Security (BENS), and former Commander of U.S. Central Command (USCENTCOM) and U.S. Special Operations Command (USSOCOM)

**We have now been fighting in Central Asia for almost 20 years with significant cost in blood and treasure. What have we accomplished there?**

First and foremost, we have largely blunted the platform that was used to attack our country on 9/11, and our military operations there have ensured that the area cannot be used as a location from which to attack our citizens or our homeland. We certainly have accomplished that. I think we have also provided the opportunity for the Afghan people to move forward in their own way; to exercise self-rule, for example. It has certainly been a very difficult path and it will continue to be as we move forward. It is not an easy situation, but I think we have provided the opportunity for them to become a more stable part of the Central Asian scene, and hopefully not be a platform from which terrorist organizations or other elements of instability can continue to impact the people of Afghanistan or others in the region.

**Can you envision a Saigon-like collapse of the Afghan government after we depart?**

I don't think that I would predict something like that. I think what we are seeing is about what we expected. It is very complex; what might be called Afghan-hard, and it is always going to be. It will be very important for us to continue to provide support—moral and otherwise—throughout this entire process. There were some good reasons behind President Trump's decision to withdraw troops and begin to decrease our presence on the ground, and get the burden back on the Afghans where it needs to be. But there are things that we continue to do at the allowable troop levels to continue to assist the Afghans as they move forward. Military support is going to be an important aspect of that. But as important as the military aspect is, at least of equal importance is the political support. I understand Ambassador Khalilzad is back in Afghanistan again this week. The diplomatic effort is going to have to continue if we are going to see this through to a conclusion that supports our national interests.

---

This interview was conducted by PRISM Editor-in-Chief Michael Miklaucic on 22 May, 2020

**By reducing troop levels—down to the allowable levels—are we ceding influence in the region to Russia and China?**

Our troops are principally in Afghanistan; they are not broadly dispersed throughout the region. Russia and China will continue to pursue their own interests. China will focus principally on the economic aspect and we see that playing out in Pakistan with the China-Pakistan economic corridor. Russia has concerns in the northern parts of central Asia including terrorist threats, so that may be a factor, but I don't know that we are going to be replaced in the region. It is important to recognize that Central and South Asia are important areas to us: We have to maintain a level of presence, a level of relationships, a level of reliability as partners there that does continue to provide influence for the United States. That will be important in the long term.

**Having commanded both the Special Operations Command (SOCOM) and Central Command (CENTCOM) what can you say about the current state of the global war on terrorism?**

It continues. SOCOM Commander General Richard Clarke recently discussing his priorities emphasized up front that the continuing effort combatting extremism is his priority. It will continue to be. We have to continue to focus on this. We are in a different strategic situation now than we were in 2001. Now we are confronted with great power competition, and we certainly have to pay attention to that, as that competition is going to be existential to us. But terrorism has impacted us over the decades as well. The best way of addressing terrorism is to continue putting pressure on terrorist leadership and their networks and helping our partners develop their own capabilities to address terrorism. Whether it is our own direct pressure or whether it is through working with partners or enabling partners to keep pressure on these networks and drive them—and drive them down—we will have to continue to do

that. So, while we necessarily have to focus on great power competition, we are also going to have to continue to deal with the terrorism.

**In the 20 years that we were focused on the global counter-terrorism mission, did we take our eye off the ball with respect to traditional great power competition?**

I think an argument can be made for that. The large numbers of troops rotating into Iraq and Afghanistan for long periods of time significantly consumed resources and readiness. We put all of our investments and efforts into trying to make sure—appropriately—that the people on the ground had what they needed. And during that time, we saw Russia and China continue to move forward in their own national pursuits, watching what we were doing and learning from it, and using the time while we were engaged in these counter-terrorism wars to improve their own capabilities and influence. There is no doubt that they took advantage of that. Did we lose sight of the ball on that? I do not think that is the case, yet. We have to be serious about it, we have to get focused back on it, and I think that is the object of the National Defense Strategy; trying to maintain a competitive advantage against great power competitors.

**The National Security Strategy and the National Defense Strategy indeed both identify great power rivals as the most significant threat to U.S. security. Do you agree that the current pivot from the Near East and counterterrorism to great power competition is timely?**

I do, and as the CENTCOM commander, I testified before Congress to that fact on several occasions. We have to look at our interests and decide what are existential threats to us. I do think a rising China and a nuclear capable Russia that is revanchist in its actions right now pose very serious threats to America. We have to pay attention to that. And the military element of power has to make certain that

we can contribute to meet the challenge, alongside our diplomatic, informational, and economic elements of national power. But at the same time, we also need to make sure we deal with a full range of threats, such as the rogue regime in Iran that continues to perpetrate friction in the Middle East, and North Korea. But bearing everything in mind, the pivot to great power competition is the right one.

**Can you describe a plausible scenario in which U.S. forces and either Chinese or Russian forces actually engage in direct combat?**

I do not really see that on the horizon right now. That would not be in our interest nor in their interest either. What I do see is conflicts playing out in what we refer to as the “gray zone.” In the physical spaces and places where we compete for influence and for partnerships, different actors try to pursue their own interests and objectives. This is where the competition could play out much more indirectly—militarily, economically, and ideologically. I think that is much more likely than a direct confrontation at this point. Certainly, direct confrontation is always a possibility. But the risks are very great and we should do everything we can to avoid that. I think that we will definitely see this playing out more in the gray zone than we will in direct engagement.

**How can the United States best counter Russian and Chinese gray zone aggression—what some refer to as hybrid warfare or conflict short of war. What is the best response?**

Our best response is making sure that we bring all the elements of our power together to create the most positive and long-lasting influence and partnerships that we can. I firmly believe that it is important that when we look at the list of countries that line up with the United States and our Western Allies, and we look at the countries that line up with China or Russia, we always want to make sure that our list is longer. And we do that by being good

military partners. We do that by having strong and robust security cooperation programs. We do that by having strong diplomatic and economic ties. We do that by sharing our values.

At CENTCOM, one of the most important programs was a program that brought foreign military officers to our schools in the United States. It doesn't cost very much; we were only spending about \$19 million per year on it in my last year in command. What that program does is bring people into our schools, gives them an opportunity to get to know our country: Their families live in our communities and they almost always leave with an overwhelmingly positive view of the United States. That's the type of thing that we need to do to ensure that we have strong, long, enduring relationships. Traveling around the Middle East as the CENTCOM commander and even as the SOCOM commander, it was always very evident to me that people wanted to be aligned with the United States, and that they want to be on our side. We have to reinforce that by our actions.

**One of our comparative advantages vis-à-vis either Russia or China is our robust global alliance and partner network. What should we be doing now to strengthen and reinforce that network?**

It is vitally important that we continue to be as reliable as we can be. Former Secretary Mattis used to remind us of this: It is good to be operationally unpredictable—create an element of surprise operationally—but strategically, we have to be predictable. Our partners have to be able to rely on us in the long term. We don't want them questioning our commitment. What we have to do is look at the relationships that we have and find ways to strengthen them. They are not all perfect. A very strong case has been made by President Trump and others that the NATO allies definitely need to pay their way for their own defense. We cannot care more about their defense than they do, frankly. We must put the right kind of pressure on them to step up. But what



is most important is to recognize that where we have had our greatest successes is when we have brought our allies and partners along. My most recent experience with the coalition to defeat ISIS put together by my predecessors—that I had the opportunity to work with in a 79-nation coalition—is a great example. Those are the times when we will be most successful. We must do this. We must make sure we share technology with them, and should look at how we might better share information with them. There are practical things we can do to improve our relationships with allies and partners as well. What I think is first and foremost is to recognize that our way of competing, our way of protecting ourselves, is really through strong partnerships. We have to put actions behind our words militarily, economically, diplomatically, and informationally: We must make sure that we are prioritizing our relationships.

**In your experience commanding CENTCOM, do you think we were successful in bringing all of those elements of national power together? If you remember, back in the early 2000s, there was a lot of enthusiasm and talk about integrated whole-of-government responses and inter-agency collaboration. Has the United States been very good at interagency collaboration and the whole-of-government responses that you describe?**

We have had moments when we have done a good job, but in general, we struggle with this. We started off our discussion today talking about Afghanistan and I think Afghanistan is a good example of where we have leaned very heavily on the military to carry a large part of the mission. I am not trying to denigrate our diplomats; they do fantastic work, but the civilian component needs to be robust and sustained. And being able to sustain the civilian effort is always a challenge. As I was leaving CENTCOM fourteen months ago, out of twenty countries in the region—eighteen with which we had diplomatic relationships at the time—in only seven did we have

a confirmed ambassador. The chargés are excellent, they are great professionals, but there is a difference. We should be sending a strong message of commitment by sending people that have the confidence of the President and the full backing of our Congress to be our principal representatives in these countries. This I think is really important.

**Another thing that Secretary Mattis said was “If you don’t fund the State Department fully, then I need to buy more ammunition.” What should we be doing in addition to appointing ambassadors? What else might we do to fortify the State Department and USAID?**

My experience working with people in that department and that agency has generally been very positive. They are great Americans who care about what they are doing, who are very focused on their missions. But we must allow our diplomats to get out of the embassies and be out more often. We have placed a lot of limitations on them. Certainly, situations like Benghazi have had a chilling effect on our diplomats getting out and being with people that they need to be with in order to make the very biggest impact that they can. And these things must be taken into consideration. There is an effort, sponsored by the American Academy of Diplomacy, to encourage review of the Congressional requirements in situations or incidents with our embassies or diplomats or our overseas USAID staff that really inhibit their ability to get out and do the things that we need done. They are overly onerous and work against our interests. We have to take a look at this; it’s not enough just for the military to be outside the wire. In many cases, the military is not the best choice to be the only face our host nation partners see. The best choice might, in fact, be USAID, or our diplomats. I think back to some of the provincial reconstruction teams in Afghanistan in the 2007-2008 timeframe; these were extraordinary efforts where we had diplomats living out in the local

communities, directly interfacing every day with local Afghan leadership, and it was a good approach. We have to inculcate that culture again of letting our people out into the communities.

**That would align with Ambassador Ryan Crocker's idea of an expeditionary diplomatic corps.**

I have heard him speak about that and I think it is definitely a worthwhile idea. If you look back into American history, you will see examples when diplomats stepped forward and created great opportunities for us to advance our interests. It is important especially in what has become a highly complex world, and one that is dominated by competition; competition for influence, competition for ideas, and competition for control. And so, for us to try to preserve the way of life that we have had we have to look at this very seriously.

**I agree completely. You cannot sit in the capital and hope to have a major influence on a country.**

Ambassador Ronald Newman (President of the American Academy of Diplomacy) and I have been discussing this. The process that is initiated by Congress when an incident happens overseas is a very thorough review process but is very much top-driven. Ambassador Newman's idea was if the Department of State or USAID had a process similar to what the Department of Defense has for significant incidents it would have a less suppressive effect in terms of trying to get back out into the field. I really support that.

**We spent years and hundreds of millions of dollars supporting the Afghan and Iraqi militaries, which have not performed particularly well when they've been in direct combat. What does that say for our current efforts to work by, with, and through, and to develop partner capacity with our security force assistance brigades and security cooperation?**

That is an excellent discussion point. I would say though that even in those cases not all our efforts

to institutionalize professionalism were failures. If you look at an organization like the counter-terrorism service in Iraq; as the Iraqi army evaporated around it in the midst of the Islamic State onslaught, the counter-terrorism service held together, and it became the nucleus of the rebuilt Iraqi army that ultimately defeated ISIS. Along with the broad international coalition that was supporting them they really took the fight to ISIL. So, there have been some examples of success, but I take your point on that.

The observation that comes out of this is that when we step into these situations, we have to step into them with our eyes wide open. One of the very smart things we did when we went back into Iraq in 2014 and Syria shortly thereafter in trying to defeat ISIS was that as we identified our partners on the ground, we did not try to reorganize them, try to over-professionalize them or institutionalize them any more than was absolutely essential for the task at hand. We helped the Iraqi army retrain itself, recoup its capabilities, and then helped them as they orchestrated a fairly complex campaign plan; but we did not try to overtly change their structure.

Across the border in Syria, we took the YPG (Kurdish People's Protection Units) with the Syrian Democratic Forces and the other Arab militias as they were. We did not try to reorganize them. We used them for the capabilities they had and tried to enable and reinforce their natural strengths. The Kurds were extraordinarily good leaders and they had a great understanding of the situation. Of course, the Arab militias had great local understanding as well. We focused on that instead of trying to reorganize them into something that looked similar to us. This is a good lesson for us long-term.

As the SOCOM commander, I looked at a number of the programs we have had with special operations partners around the world and I think you will see that that approach has paid off. While militaries will be in various states of readiness, often the special operations forces are of pretty high

quality, adhere to the rule of law, and are very reliable forces for their country. We have taken a very deliberate approach to this, not trying to over-organize them and trying to build on the inherent strengths of our partners.

**Over the course of your career, how would you characterize the evolution or any changes in the concepts or the character of war and the concepts of victory and defeat?**

The concept of war and the nature of battle have been significantly impacted by speed and information, and certainly by technology that has changed our ideas about what we do, the way that we have pursued things, and our understanding of our challenges and opportunities.

We sit on the cusp of artificial intelligence-enabled activities and operations. This is a watershed point for us that we have been building to over a number of years and is going to have a dramatic impact on how we move forward. In many cases, those who dominate these technologies will be the ones writing the rules that will prevail over the long term. This is very critical. I mean to include in this the whole suite of emerging cyber technologies. These represent something uniquely different than anything we have experienced in the past. While we have exquisite intelligence collection capabilities, often the information out there in the open sphere is as important to us as classified information; but the volume of it is so great and our ability to mine through it and understand it is still greatly challenged. That said, as we saw in Raqqah and in West Mosul, war can still be very brutal. These were brutal, brutal fights against a very savvy and technically-enabled terrorist army (information-wise). When it came down to the end of fighting in many urban areas, it was very gruesome building-to-building combat. So, the basic nature of war remains brutal but it is now dramatically influenced by these emerging technologies.

As to the concept of victory, that has become more complex to understand. One of the things that we often spoke about at SOCOM, as well as at CENTCOM, was the need to rethink what winning means in this environment. Winning will not necessarily look the same as it did in the past; a parade, a very clear and distinct signing of surrender or some clear indication that hostilities are over, and that one side has prevailed over the other. In many ways, it will be more about preserving our interests, preserving decision space moving forward, maintaining relationships going forward, and being able to sustain a level of pressure on adversaries that prevents them from rising or from prevailing in a competition with us. The definition of what winning in this very complex environment means has changed; winning matters, but winning looks quite different than what we might have thought about it in the past.

**What specific emerging technology does he see as the most critical for the U.S. to prioritize, and why?**

I think artificial intelligence coupled with 5G communications capability should be our priority. This has the potential to make extraordinary advances for our nation and for our partners. It is essential for the United States and her partners to master this technology first so that we can ensure the rules that guide the global use of these technologies are fashioned in a lawful and ethical manner. In the wrong hands, like the Chinese, this could have an extraordinarily bad effect on us.

**Can you briefly describe the main elements of a strategy that will best manage our evolving relationship with China and avoid war?**

First and foremost are deep and trusting relationships with our partners in the region and around the globe—militarily, diplomatically and economically. Second would be an approach that holds China accountable for its actions—whether that is their failure to properly warn the world of the COVID-19

virus or the predatory lending arrangements they are pursuing globally. Third would be making sure our strategy is not just about military strength. We have to compete across the spectrum. We need to leverage our strength in innovation, entrepreneurship,

and American business. Finally, we have to lead. We cannot do this by ourselves, and we have always been at our best when we have been leading others because that is not only in our interest but in fact the interests of peace-loving people around the world.

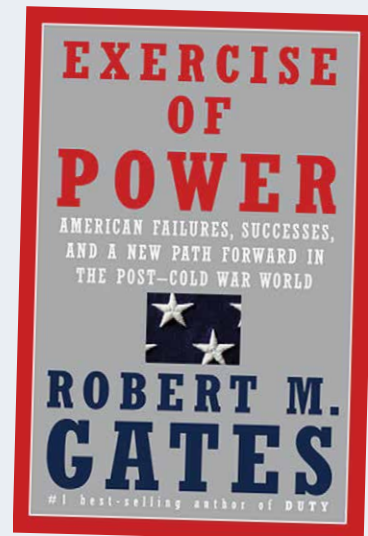
**Exercise of Power:  
American Failures, Successes, and a  
New Path Forward in the Post-Cold  
War World**

By Robert Gates  
Knopf Double Day Publishing Group, 2020  
464 pp. \$29.95  
Hardcover ISBN: 9781524731885  
Ebook ISBN: 9781524731892

Reviewed By Admiral James Stavridis, USN  
(Ret)

I first met Secretary Gates in the summer of 2006, when he was President of Texas A&M and had been invited to the Pentagon to meet with my boss, Secretary of Defense Don Rumsfeld. I was a newly selected 3-star Vice Admiral, and knew all about him, of course, as a career CIA officer who went on to lead the Agency before retiring and heading into academe, first as Dean of the Bush School and then as President at Texas A&M. When he came into my small office outside the vast Secretary of Defense office, I started to usher him in immediately, but he spent several minutes asking me about myself, how long I had been with Secretary Rumsfeld, where I had been before my current job. It was friendly and engaging conversation, but you could feel that spymaster's gaze sizing you up and filing the conversation away. I thought to myself, I would like to work for him someday—never considering it would happen. I sure wasn't going to get out of the Navy and move to Texas.

Little did I know that in a matter of months Secretary Rumsfeld would depart and I would find myself working directly for Secretary of Defense



Bob Gates for the next seven years. Indeed, just before Gates took over, I headed down to Miami to be Commander of the United States Southern Command. Three years later, after considering sending me to the Pacific, Gates chose me to be the first (and, so far, only) Navy Admiral to serve as Supreme Allied Commander of NATO. My four years there were consumed with Afghanistan, Libya, the Balkans, piracy off the coast of Africa, the gradual destruction of Syria, and NATO reform. Gates was the best of bosses, demanding but sensible, good humored even in tense situations, and always quick with a quip or a word of encouragement over a Grey Goose vodka as the day wound down. There is no one in whose judgment I repose more trust, nor anyone whose character I more admire.

None of that would surprise any reader who has paid attention to the career of Bob Gates, especially if they have read his excellent memoir of those days, "Duty," or his subsequent book on leadership, "A Passion for Leadership." But in his new book, "Exercise of Power," we see a new and sweeping vision that is only hinted at in his earlier writings,

---

Admiral James Stavridis, USN (Ret) is a retired United States Navy admiral, currently an Operating Executive with The Carlyle Group and Chair of the Board of Counselors at McLarty Associates. In August 2018, he stepped down as Dean of the Fletcher School of Law and Diplomacy at Tufts University.

---

as good as they were. In his new book, he presents a complex yet unified theory of how America can best conduct itself in the world, drawing smoothly on the many crises in which Gates found himself engaged—in multiple tours not only at the CIA but on the National Security Council staff as well. No one but Bob Gates could write this book, and it comes at a particularly timely moment as Americans broadly question our role in the world.

He begins with a short but compelling overview of the tools of power, typically providing anecdotes from his experiences as to how they can best be used; military, economic, diplomatic, cyber (good to see this as a “stand-alone” tool, which it is most assuredly), development, communications, intelligence, cultural, ideological, private sector, religion, etc. I think of these as almost Clausewitzian-style “principles of power” for the 21st century. Of particular power is his idea that the sum is truly greater than the parts—as is the music of a symphony far greater than any single instrument. And Gates is quick to acknowledge that as a nation we are vastly overweight in our reliance on the military instrument, and underweight on all the others, and in their integration. If the U.S. government were in fact a symphony, you could think of a stage with a massive, amplified, and pounding set of drums taking up nearly three quarters of the stage—that would be the military. In the corner, a tiny group of other instruments squeak along, barely discernible—that would be the rest of the interagency.

To back up his thesis, the bulk of the book is essentially a collection of set pieces that lay out the good, the bad, and the really ugly international scenarios in which America has engaged in the post-Cold War world. The very few “good” outcomes are the first Gulf War pushing back Saddam Hussein’s invasion of Kuwait, then leaving; Colombia and the suppression of the Marxist-narco terrorist group, the FARC; and (somewhat) the Balkans, where two interventions have created at least a modest level of

peace (compared to the raging wars that followed the dissolution of the old Yugoslavia). The long list of “bad” and “really ugly” outcomes are well known at this point; Somalia, where Black Hawk Down pushed us out; Haiti, where the bad luck always seems to overcome our best of intentions; Iraq, especially the poorly executed attempt to completely democratize it and dispense with the armed forces; Afghanistan and the over extension and failed adventure with nation building; Syria and the failure to enforce a red-line; and Libya, where a NATO “success” turned to ashes as all the intervening states sprinted for the exits after Qaddafi’s death and the resulting chaos that continues to reign. I lived Libya (and several others) with Secretary Gates and everything he consistently advocated—moderation of ambition, realistic expectations, recognition of the limitation of our military power, a desire for sensible long-term engagement—is on display in this volume as a cautionary tale.

One of the “money” chapters in the book is toward the end, and it deals with how the United States should approach the challenges of our relationship with China. We need to be neither foolish about where China is headed (and in a devastating list of quotes, Secretary Gates lays out just how wrong every previous administration has been in its optimism), nor unnecessarily confrontational. I would say the approach Bob Gates lays out is about right; confront where we must, but cooperate where we can. Finding the balance will be challenging, but this book helps lay out guide posts to doing so. Taken with the rest of the volume, it affords policymakers a powerful guide to how to approach the conundrum that is China.

No book is perfect, and there is to my eye a very surprising omission; any commentary on the now three-year old Trump administration and its growing tendency to simply withdraw from the world. While I would not expect Secretary Gates to drag his arguments down into the morass of

---

day-to-day politics, we could have hoped for a clear rejection of the Trumpian worldview, which can ultimately be boiled down to two words; “get out.” Rejecting international engagement is different than buying into a money pit of commitment to fixing broken states. The Trump Doctrine, such as it is, seems to consist of; rejecting alliances, cutting international aid, building economic and physical borders around our nation, reducing the budgets of our international tools other than the military, and pulling out of international treaties (Trans-Pacific Partnership, Paris Climate Accords, INF, Open Skies, WHO, on and on).

The tragedy is that we’ve tried that already—in the 1920s and 1930s. We rejected the League of Nations, built trade barriers (the Hawley-Smoot Tariffs), and spurned any sort of engagement in the world. How did that turn out? We broke the global economy (the Great Depression) and you can drop a plumb line to the rise of fascism and the Second

World War. Secretary Gates effectively lays out the right course for the nation to steer; an effective inter-agency process (a symphony of action far greater than the sum of the parts), international engagement, but with a clear-eyed view of the advantages and limitations of our partners, and an increasing reliance on communication, culture, and the private sector—our super powers in the USA—but only when we choose to use them, and can effectively “live them” in front of the unblinking glare of international media.

This is a powerful, clearly written and ultimately woken book on how America must approach the world. We are far from becoming a defeated or a declining power—but without the prescription that Secretary Gates lays out in “Exercise of Power,” we might become one. The good news is that we can continue to be a force for good in the world, and ensure our nation prospers as well—if we heed good advice like this.

---

## The Return of the Russian Leviathan

By Sergei Medvedev

Translated by Stephen Dalziel

Polity, December 2019

Hardcover ISBN: 978509536047, \$74.95, 250

pp.

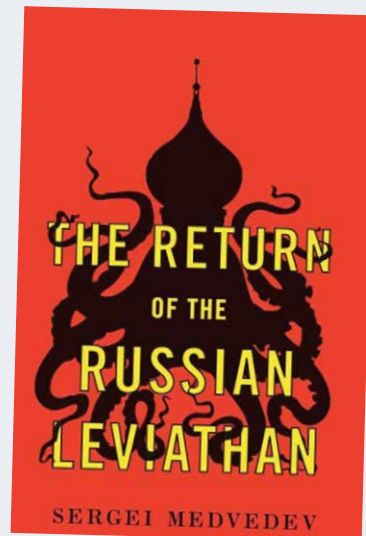
Paperback ISBN: 9781509536054, \$24.95

Reviewed by John Herbst

Sergei Medvedev, Professor in the Faculty of Social Sciences at Moscow's Higher School of Economics, is a fox; a thoroughly modern, or perhaps I should say, post-modern fox. Isaiah Berlin would understand. The British historian of ideas wrote a paradigmatic essay on Russian literature, "The Hedgehog and the Fox," in which he contrasted Tolstoy the fox, with Dostoevsky the hedgehog. As Berlin explained, the hedgehog knows one big thing, but the fox knows many things.

At first glance, Medvedev's recent book, "The Return of the Russian Leviathan" might seem to be the work of a hedgehog, because it addresses one very large topic, Russia and the reemergence after a brief interlude of its traditional authoritarian style of rule. But while he holds tightly and correctly to that large theme, his sensibility is foxy. And the book is no systematic study of authoritarianism in Russia, its similarities with Soviet totalitarianism and Czarist despotism, and its unique Putin flourishes.

Instead, it is an illuminating and at times brilliant series of short essays on different aspects on Russian life. The book is grouped loosely into four parts; the war for space, the war for symbols, the war for the body, and the war for memory. These categories are somewhat abstract and Medvedev's writings diffuse, so that some key themes appear throughout the book.



And what are those key themes? Medvedev believes that for Russia to thrive, it must accommodate itself to the modern, global order and economy. He sees that Russia under Putin has moved in the opposite direction. In the early 2000s, while pursuing increasingly repressive policies at home, Putin did not misbehave internationally; but that all changed with his 2014 seizure and annexation of Crimea, which ended "a 25-year project of normalization and adaptation to the global world." Medvedev's analysis is on target, although I would pre-date Putin's challenge to the global order back to his Munich Security speech in February 2007, the cyber-attack on Estonia that summer, and his August 2008 war on Georgia.

Medvedev sees Kremlin economic policies determined by the preferences of its leadership and their cronies, not national interests nor the interests of the Russian people. This is particularly evident in the oil and gas sector, responsible for 60 percent of Russian export earnings, which has enriched Putin and his inner circle and which provides resources for the Kremlin's patronage system. In Medvedev's eyes, the Kremlin's domestic and foreign policies have led

---

John E. Herbst is Director of the Atlantic Council's Eurasia Center and was the United States Ambassador to Ukraine (2003-2006) and Uzbekistan (2000-2003).



---

to stagnation and repression at home, and isolation abroad. Medvedev's big picture thoughts are sound, and well understood by the real opposition in Russia, and sober analysts in the West.

But the great added value of this book is his look at the cultural factors that helped produce these policies and the way that these factors influence many different aspects of Russian life. He provides clear guidance up front in his fourth essay, "Crimea as a Territory of the Subconscious." He writes that to understand why Putin decided to turn away from world order and seize Crimea, one need not consult American statesmen/scholars Kissinger or Brzezinski, but rather Fyodor Dostoevsky, or 19<sup>th</sup> century pan-Slavist Nikolay Danilevsky, both of whom saw Russia as essentially different from the West.

Medvedev, however, is no historical determinist. This choice was not inevitable, even if it restored an established pattern in Russian culture and tradition. Instead it was simply the decision of an "Orthodox (i.e. Russian Orthodox) Chekhist" Putin, who was also influenced by the monarchist emigre thinker Ivan Ilyin, who advocated a Christian fascist Russia.

Looking at the first years of Putin's presidency, Medvedev observes that Russia seemed to be on a very different trajectory. During that period the Russian economy grew quickly thanks to rising hydrocarbon prices, sound macroeconomic policies and cooperation with the West. But even then there was grumbling about the "geopolitical defeat" Russia suffered with the end of the Cold War, and the "plundering" of Russia by global liberalism and its Russian accomplices. These themes became ever more prominent that decade and came to dominate Russian media as tensions with the West flared after the Kremlin began its war against Ukraine.

Another major theme for Medvedev is the Kremlin's reliance on "trolling" or disinformation as a governing tool. This topic, of course, has received substantial attention in the West, which has focused

on Putin's use of it as a weapon, for instance, to hide Moscow's role in Donbas, or to promote BREXIT, or to interfere in western elections. But Medvedev offers a different optic. He sees it as essential to Putin's success in governing Russia in the wake of his failed policies: "With the absence of political will and strategic thinking, and with a shrinking resource base, trolling represents the thoughts and main method of state policy." Indeed, he writes, for some years now, the whole of Russia, including President Putin, has tended to live in a TV serial, "a parallel reality."

An important part of this is Putin's revival of the Soviet practice of orchestrating public outrage. While Putin took control of the major television stations early in his tenure as President, the small station Dozhd (Rain) remains independent. To contain the possible impact of its reporting, the Kremlin organizes "Veterans of Novgorod Offended by the Programmes of the Dozhd television channel."

As one of the books section headings make clear—"The War for Symbols"—the Kremlin places great emphasis on symbols. They are part of the effort to control the narrative about what is happening in Russia and elsewhere. The ongoing, largely fact-free effort to tar the Ukrainian government and society as fascist is one key battleground. But perhaps even more fundamental is the refusal to come to grips with the horrors of Soviet rule. Putin famously decried the dissolution of the Soviet Union as the greatest tragedy of the 20<sup>th</sup> century; and he remains proud of his service in the KGB, one of the most repressive organizations in human history.

Medvedev notes that a modern, liberal Germany could never have emerged without a reckoning with its Nazi past and rues the failure of Putin's Russia to do the same. There is no officially recognized historical memory of enormous evils the Soviet regime inflicted on its population. Medvedev mentions the unrealized hope of literary critic Marietta Chudakova that the writings of Aleksandr Solzhenitsyn, Vassiliy Grossman, and

---

Varela Shalamov would serve as a substitute for the Nuremberg Trials in teaching the Russian people about the horrors of the Soviet past; but concludes that to stick such a lesson needs “concrete” memorials—museums and exhibitions as in Germany. And such memorials are not on the agenda of a regime devoted to the memory of the achievements of its Soviet and Czarist predecessors.

Medvedev reminds us that 19<sup>th</sup> century philosopher Piotr Chadaev was right when he said Russia has no history, but “lives only in the present.” In other words, the past is endlessly malleable to serve the interests of current rulers. But Medvedev also explains that it is perhaps natural for the Russian people to avoid looking at the horrors of the forced collectivization and purges. He sees a “pain taboo” in Russia. “Suffering is something internalized which people try to deal with inside themselves....It is not normal to talk about pain in Russia.” Kremlin preferences and the avoidance of a public discussion of pain explains the strong criticism in Russia of Svetlana Alexievich, the Belarusian writer who won a Nobel Prize in 2015 for her grainy and unsparing portrayals of the horrors of the Soviet period.

Medvedev the fox throws out many more insights in this volume. To mention just two more,

he explains the prosaic ways that the Kremlin’s militaristic foreign policy and its patronage system reinforce each other. Putin returned intercontinental ballistic missiles to the Kremlin’s victory parades in 2008; and the appearance of these missiles causes \$25-50 million in damage to Moscow’s roads each year, which means more profits for Putin’s cronies, who repair the streets.

Medvedev also notes that while political thought in Russia is closely monitored and restricted, there is one exception; the study of geopolitics. Classic Western geopolitical thinkers like Halford Mackinder and Alfred Mahan are not just readily available in Russia, but receive substantial attention, especially from Russia’s foremost geopolitician, the extremist thinker Aleksandr Dugin. And this suits the President of Russia, who has included Dugin in at least one of his trips abroad, because the geopoliticians talk of the natural competition between the landpowers of Eurasia (Russia) and seapowers (the UK before and now the United States).

There is a lot more in this book—such as Medvedev’s commentary on Russian films—that offers valuable clues into Russian life for even seasoned Russia-hands. Highly recommended, but watch out for the author’s detours into magical realism.

---

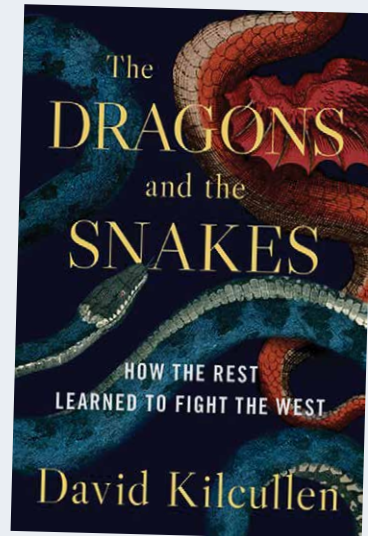
## The Dragons and the Snakes: How the Rest Learned to Fight the West

By David Kilcullen  
Oxford University Press, March 2020  
336pp. \$27.95  
ISBN: 9780190265687

Reviewed by Carter Malkasian

Every few years David Kilcullen publishes an insightful book that inspires new thinking in the U.S. armed forces and becomes a standard reference for all manner of strategies, operational plans, and concepts. The Australian anthropologist, former army officer, and conflict zone observer has a unique talent for capturing global dynamics in warfare and explaining them to a wide audience. In 2009, it was *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*. In 2013, it was *Out of the Mountains: The Coming Age of the Urban Guerrilla*. His newest, *The Dragons and the Snakes: How the Rest Learned to Fight the West*, repeats the feat in a timely book for the re-emerging multipolar world.

*The Dragons and the Snakes* is about how Russia and China (“dragons”) have developed new methods and technologies for fighting the United States and its allies while terrorist adversaries and rogue states (“snakes”) have evolved since 2001. Kilcullen is highly conversant in new technologies and able to show convincingly how GPS, smartphones, autonomous systems, and the internet have been exploited by adversaries to great lethality. His main takeaway is that, “the high-tech, high-precision, high-cost suite of networked systems that won the Gulf War so



quickly and brought Western powers such unprecedented battlefield dominance in the quarter century since then—is no longer working,” and that we must adapt or face decline.

Kilcullen devotes significant space to exploring what has become known as the “gray zone”—the variety of subversive, hybrid, and clandestine techniques, both military and non-military, that have been used to defeat or undermine Western partners and allies without going to war. He contends that the United States and the West have an extraordinarily narrow notion of war as a conventional, force-on-force contest of arms among combat units on the battlefield. Conflict in the gray zone between peace and open war is often also described as “competition short of armed conflict” and is often paired with Russia’s “little green men” (Russian contractors or special forces posing as a third party) or China’s maritime militia (which pose as fishermen to exert Chinese claims in the South China Sea). The gray zone also has conceptual links to hybrid warfare—the use of conventional and unconventional tactics by an adversary, exemplified by the tactics of Hezbollah.

---

Carter Malkasian is a Research Analyst at the Center for Naval Analyses. From 2015 to 2019 he was a senior advisor to General Joseph Dunford, Chairman of the Joint Chiefs of Staff.

---

The great contribution of *The Dragons and the Snakes* lies in Kilcullen's rich yet succinct chapters on Russia and China. On Russia, Kilcullen describes how paramilitary forces, contractors, cyber operations, political subversion, and information campaigns surf "the threshold of detectability, sometimes subliminal...at other times breaking fully into the open to seize an advantage or consolidate gains before an adversary can react." Borrowing a term from anthropology for people on undefined thresholds in society or culture, Kilcullen dubs this "liminal warfare." Kilcullen walks the reader through Russian military operations since 1991 (highlighted by an informative description of the 2008 war in Georgia), the ideas of geopolitical theorist Aleksander Dugin, and General Valeriy Gerasimov's influential writings (the famous "Gerasimov Doctrine") on "indirect and asymmetric methods" and undeclared war for "achieving political-military goals." The danger from the Russians is "a sudden strike so ambiguous that we may still not be sure it is really happening, even in the moment."

On China, Kilcullen describes how the Chinese employ a broad range of armed and non-armed tools to coerce an adversary during what the West views as peacetime. The Chinese, Kilcullen argues, do not distinguish between states of war and peace. They seek to dismantle Western influence as if they are at war. Foreign assistance, financial disruption, currency manipulation, cyber operations, information operations, criminal activities, and stealing technology substitute for armed conflict. There are no geographical limits. Kilcullen describes this Chinese form of gray zone activity as "conceptual envelopment." Again, Kilcullen is at his best walking the reader through the details of post-1991 events, reforms, and thinking, such as the Chinese perception of U.S. technological superiority demonstrated in the Gulf War, the Taiwan Strait Crisis, and Qiao Liang and Wang Xiangsui's book on unrestricted

warfare. Whereas the key danger from Russia is the sudden ambiguous strike, the key danger from China is the gradual expansion of non-kinetic operations against warlike goals such that we do not realize what is happening until it is too late.

To cope with these strategies and declining economic power, Kilcullen advises that the United States and the West should adopt a Byzantine approach—the Byzantine Empire having been the rearguard of Western civilization as the West may now be the rearguard of democracy. He recommends that we develop new military models while copying those of adversaries; expand use of non-conventional and non-kinetic techniques; maintain an edge in critical technologies; turn adversaries against each other; use soft power to create internal challenges for them at home; and above all strengthen our own economies and polities. Kilcullen sees a Byzantine approach as drawn out over decades. In short, we would develop gray zone methods of our own—both offensive and defensive.

Kilcullen's most profound observation by far is that these new methods of warfare raise the chances for misunderstanding, security dilemmas, and open war. The U.S. and Chinese perceptions of each other, Kilcullen notes, are fundamentally flawed. Both sides misread the intent and exaggerate the threats coming from the other. Neither are unitary actors; incidental and uncoordinated actions by parts of the whole can be misconstrued as an aggressive grand strategy. Each can perceive threat when there is none: "An illusion—an apparent pattern, existing only in the eyes of Western observers, that Chinese strategists would not recognize in themselves, just as we would not recognize their perception of us." Conceptual envelopment magnifies the problem. Each side knows the other is conducting operations toward warlike aims. In turn, both are inclined to view all actions, even innocent ones, as part of a larger plot, breeding "the danger of miscalculation, of

---

talking ourselves into war with adversaries—or of strategists misinterpreting each other’s actions and thereby provoking an escalatory security dilemma that ends in the war of the century.” Kilcullen excludes Russia from this penetrating observation but I have to think it applies to Russia and liminal warfare as well.

I have spent a good bit of time working on gray zone matters over the past five years. To my mind, *The Dragons and the Snakes* is the best single piece out there—concise, well-written, and nuanced. It is both a timely introduction to the topic for the unfamiliar and a source of new discoveries and insights for the expert; an important book during changing times.



Save the Date for the 7<sup>th</sup> Annual

# **CYBER BEACON CONFERENCE**

on Thursday, the 3<sup>rd</sup> of December 2020

**Disruption in an Era of Great Power Competition:  
*Pandemic, Infodemic, Space, Cyberspace, and Beyond***

Hosted Virtually by the  
College of Information and Cyberspace  
“Our Nation’s Information and Cyberspace War College”  
- Limited Space Available -

[cic.ndu.edu](http://cic.ndu.edu)

### **SUBSCRIPTIONS**

Keep up to date with global and national security affairs, including sources, effects, and responses to international insecurity, global policy and development, state-building and reconstruction, counterinsurgency, and lessons learned. To request, cancel or modify your subscription, contact the *PRISM* editorial staff at <prism@ndu.edu>. Please include your preferred mailing address and desired number of copies in your message.

