

# SSQ STRATEGIC STUDIES QUARTERLY

---

FALL 2021

VOL. 15, NO. 3

---

## FEATURE ARTICLE

### **The Technologies and International Politics of Genetic Warfare**

Yelena Biberman

---

### **An Overlooked Aid to Arms Control: US Nuclear Modernization**

Matthew R. Costlow

---

### **Strategic Imperative: A Competitive Framework for US-Sino Relations**

CAPT Michael P. Ferguson, USA

---

### **The Remote Sensing Revolution Threat**

LTC Brad Townsend, USA

---

### **Arctic Space Strategy: The US and Norwegian Common Interest and Strategic Effort**

Lt Col Kjetil Bjørkum, Royal Norwegian Air Force

---

### **Comprehensive Security Approach in Response to Russian Hybrid Warfare**

Lt Col Tuukka Elonheimo, Finnish Air Force

---

---

# SSQ STRATEGIC STUDIES QUARTERLY

---

**Chief of Staff, US Air Force**

Gen Charles Q. Brown, Jr., USAF

**Chief of Space Operations, US Space Force**

Gen John W. Raymond, USSF

**Commander, Air Education and Training Command**

Lt Gen Marshall B. Webb, USAF

**Commander and President, Air University**

Lt Gen James B. Hecker, USAF

**Director, Academic Services**

Mehmed Ali, PhD

**Director, Air University Press**

Mehmed Ali, PhD

---

**Editor**

Dr. Victor Mbodouma

**Managing Editor**

Jeanne K. Shamburger

**Print Specialist**

Megan N. Hoehn

**Illustrator**

Daniel M. Armstrong

---

***Advisers***

Gen Michael P. C. Carns, USAF, Retired

James W. Forsyth, PhD

Christina Goulter, PhD

Christopher J. Bowie, PhD

Jay P. Kesan, PhD

Charlotte Ku, PhD

Martin C. Libicki, PhD

***Contributing Editors***

David C. Benson, PhD

Mark J. Conversino, PhD

Kelly A. Grieco, PhD

Michael R. Kraig, PhD

Dawn C. Murphy, PhD

David D. Palkki, PhD

Nicholas M. Sambaluk, PhD

Evelyn D. Watkins-Bean, PhD

Wendy Whitman Cobb, PhD



<https://www.af.mil/>



<https://www.spaceforce.mil/>



<https://www.aetc.af.mil/>



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

# STRATEGIC STUDIES QUARTERLY

An Air Force–Sponsored Strategic Forum on  
National and International Security

Fall 2021

VOL. 15, NO. 3

## FOREWORD

### 3 Foreword

Victor Mbodouma

## FEATURE ARTICLE

### 6 The Technologies and International Politics of Genetic Warfare

Yelena Biberman

## PERSPECTIVES

### 34 An Overlooked Aid to Arms Control: US Nuclear Modernization

Matthew R. Costlow

### 48 Strategic Imperative: A Competitive Framework for US-Sino Relations

CAPT Michael P. Ferguson, USA

### 69 The Remote Sensing Revolution Threat

LTC Brad Townsend, USA

## PARAVION

### 88 Arctic Space Strategy: The US and Norwegian Common Interest and Strategic Effort

Lt Col Kjetil Bjørkum, Royal Norwegian Air Force

### 113 Comprehensive Security Approach in Response to Russian Hybrid Warfare

Lt Col Tuukka Elonheimo, Finnish Air Force

## BOOK REVIEWS

- 138 *The Russian Understanding of War: Blurring the Lines between War and Peace*  
by Oscar Jonsson  
Reviewed by Capt Jayson M. Warren, USAF
- 140 *Rebranding China: Contested Status Signaling in the Changing Global Order*  
by Xiaoyu Pu  
Reviewed by Dr. David A. Anderson
- 142 *Russia Abroad: Driving Regional Fracture in Post-Communist Eurasia and Beyond*  
edited by Anna Ohanyan  
Reviewed by LTC Andrew Forney, USA

## FOREWORD

Is the US nuclear strategic deterrent fully adequate to dissuade today's new threats, such as modernization and expansion of nonstrategic nuclear weapons, hybrid warfare, cyber and terrorist attacks, and other subversive, provocative, revisionist, and hegemonistic activities from China, Russia, and other adversaries?

Answering that question is not simple. Nevertheless, the fact that adversaries are aggressively and fearlessly implementing those threats can signal that America's nuclear forces, while still directed toward averting aggression and preserving peace, may no longer be the adequate deterrents of hostile behavior they once were.

The US and allied states are increasingly concerned about these emerging threats and the challenges they pose to US and international security. These apprehensions have reignited debates about the role of nuclear weapons in the US and NATO deterrent strategies. Many in the US have proposed modernizing the US nuclear triad, extending its life service, and modernizing nuclear-capable aircraft. Ground Based Strategic Deterrent (GBSD) missiles are under development to replace Minuteman III missiles. Still, whether these efforts will address and deter today's threats remains to be seen.

Tackling the question of the role of nuclear weapons in the nuclear deterrent strategy, articles in this edition take a hard, fresh look at the weaknesses in the US nuclear deterrent strategy and explore novel, concrete tactical and operational venues the US and allies could use to strengthen existing nuclear arsenals and address and confront today's threats.

In "The Technologies and International Politics of Genetic Warfare," Dr. Yelena Biberman discusses the eventuality of genetic warfare thanks to the weaponization, delivery, and precision of biological weapons made possible by innovations in synthetic biology, artificial intelligence, and nanotechnology. Since genetic weapons may have the same deterrent effects as nuclear weapons, they represent a viable deterrent source for nuclear states such as the United States that may now include them in their deterrent strategy and develop and use them covertly or openly as strategic, tactical, and psychological deterrents.

However, the list of nuclear states and terroristic, genocidal, and apocalyptic regimes and non-state actors that may use genetic and nuclear weapons is growing. Thus, there is an urgent need for the US to expand its arms control efforts beyond China and Russia and include all types of nuclear weapons. In "An Overlooked Aid to Arms Control: US Nuclear Modernization," Matthew R. Costlow proposes that the US modernize its nuclear programs to induce states to agree to come to the negotiating

table but also to provide US diplomacy with an additional viable option to incentivize states to comply with an arms control agreement. The idea of modernized nuclear weapons triggers fear of a counteraction threat should these states choose to violate the agreement.

To engage the adversaries meaningfully, the US must continue to value competition as a strategic tool. CAPT Michael P. Ferguson, USA, in “Strategic Imperative: A Competitive Framework for US-Sino Relations,” warns that renouncing the conceptual framework of competition can result in unfruitful policies shaping against rogue and revisionist powers like the Chinese Communist Party. That is, if the US does not stick to the conceptual framework of competition, it may not have a strategic imperative to prevent adversaries from achieving their strategic objectives at the expense of US values and national security interests.

Today’s security threats are multifaceted and evolving. In “The Remote Sensing Revolution Threat,” LTC Brad Townsend, USA, identifies remote sensing (using satellites to image objects on the ground) as a serious threat to US national security and assesses weaknesses in existing US approaches to its management. He proposes a comprehensive approach that includes novel diplomatic procedures and increased regulatory control measures to accompany future active military means of addressing this emerging, ubiquitous threat. Possessing this technology and managing it appropriately will guarantee an overwhelming military advantage for the US security strategy to leverage while denying that capability to adversaries.

Since adversaries’ threats pose challenges to the US and its allies, this fall issue includes a new section—*Par Avion* (by airmail)—featuring articles with international perspectives on US national security strategy. These articles offer international insights on how the US can strengthen its deterrent strategy while working collaboratively with allied states.

In “Arctic Space Strategy: The US and Norwegian Common Interest and Strategic Effort,” Lt Col Kjetil Bjørkum from the Norwegian Air Force discusses the increased significance of the Arctic in the context of strategic competition. He lays out the challenges of the Arctic and areas where the US and Norway could cooperate for mutual benefits and for deflecting the Chinese and Russian presence.

A worrisome and complex threat to the US and its allies is Russian hybrid warfare—the use of conventional military force supported by irregular and cyber warfare tactics. In “Comprehensive Security Approach in Response to Russian Hybrid Warfare,” Lt Col Tuuka Elonheimo from the Finnish Air Force explains the broader concept of Russian hybrid

warfare. He argues that these Russian warfare methods are a serious threat to Western democracies, unity, and decision-making ability and provides preventive measures including increasing comprehensive security, cooperation, situational awareness, preparedness, and resilience.

We welcome your feedback on this issue and hope it promotes discussion and further exploration of these areas. You can comment at <https://www.airuniversity.af.edu/SSQ/> by clicking the “Comment on Article” button at the end of each article, on Facebook at <https://www.facebook.com/StrategicStudiesQuarterly>, and Twitter at <https://twitter.com/SSQJournal>. Contact the editor at [StrategicStudiesQuarterly@au.af.edu](mailto:StrategicStudiesQuarterly@au.af.edu).

**Victor Mbodouma**  
Editor in Chief, SSQ

# The Technologies and International Politics of Genetic Warfare

YELENA BIBERMAN

## Abstract

This article considers the prospect and potential of genetic warfare. Drawing on expert interviews and fieldwork, it begins by detailing how the recent and anticipated innovations in synthetic biology, artificial intelligence, and nanotechnology solve the weaponization, delivery, and precision problems that had previously made biological weapons impractical. The article then considers how states and non-state actors may develop and use genetic weapons, with a focus on the problem of secrecy. Underlying whether to reveal or conceal genetic war capability is a trade-off between strategic surprise and deterrence. Actors requiring deterrence are likely to reveal genetic military capability. With the only rivaling source of deterrence being nuclear weapons, nonnuclear states and non-state actors are more likely to make public their genetic weapons capability than nuclear states. The question of whether to use genetic weapons covertly or openly also entails a trade-off. Covert use confers strategic and tactical benefits, whereas the benefits of unrestricted use are primarily psychological. Terroristic, genocidal, and apocalyptic regimes and non-state actors may use genetic weapons openly, but most would likely opt for covert genetic warfare.

\*\*\*\*\*

Is the genome becoming a new domain of warfare? Innovations in synthetic biology, artificial intelligence (AI), and nanotechnology are hastening the prospect of human evolution catching up with shifting cultural preferences.<sup>1</sup> The capacity to modify itself by environmental demands may enable the so-called *Homo deus* to survive and thrive despite the many possible impediments.<sup>2</sup> However, the revolutionary technologies may also usher in human extinction.

In making his case for reelection in 2012, Vladimir Putin predicted that nuclear weapons would, over the next half a century, become eclipsed by “fundamentally new instruments for achieving political and strategic goals.”<sup>3</sup> The future of warfare, he said, is “based on new physical principles,” including “genetic” science. The new weapons would be “as effective as nuclear,” but



“more ‘acceptable’ from the political and military perspective.”<sup>4</sup> Then came a construction boom at over two dozen institutes that had previously comprised the USSR’s biological and chemical weapons establishment.<sup>5</sup>

The US security establishment is also beginning to take the promises and perils of the biotechnology revolution seriously, and there have been calls for a national strategy.<sup>6</sup> The US intelligence community’s (IC) 2016 worldwide threat assessment singled out genome editing: “Research in genome editing conducted by countries with different regulatory or ethical standards than those of Western countries probably increases the risk of the creation of potentially harmful biological agents or products.”<sup>7</sup> The IC predicted, however, that researchers will “continue to encounter challenges to achieve the desired outcome of their genome modifications, in part because of the technical limitations that are inherent in available genome editing systems.”<sup>8</sup>

The Imperiale Framework—developed by the National Academies of Sciences, Engineering, and Medicine in 2018 at the behest of the US Department of Defense—offers the latest, most complete assessment of the hierarchy of probable biological threats. It begins by noting that the scientific advances of the past two decades have expanded what is possible in creating new weapons while also making them more quickly available and more widely accessible.<sup>9</sup> The Imperiale Framework identifies three capabilities warranting the most concern at present: recreating known pathogenic viruses, making existing bacteria more dangerous, and making harmful biochemicals via *in situ* synthesis. The first two rely on technology that is easy to use and highly accessible; the novelty of the third makes preventing and recognizing an attack particularly difficult.<sup>10</sup>

This article explores the prospect and potential of genetic weapons, or genetically engineered bioweapons. It begins by surveying the recent technological developments that make genetic weapons possible. These include vital advancements in synthetic biology, AI, bioinformatics, nanotechnology, and robotics. These advancements make genetic weapons potentially at least as dangerous as nuclear but as accessible as cyber weapons.

It then considers how states and non-state actors may develop and use genetic weapons, specifically regarding secrecy. The recent COVID-19 pandemic triggered fears and high-level, questionable accusations of covert biological warfare.<sup>11</sup> The response suggests that even if the worry is unwarranted in the COVID-19 case, questions about the covert capability and use of bioengineered weapons are likely to surface in policy, politics, and popular culture over the decades to come. Regarding genetic weapons capability, this article proposes that the choice to reveal or conceal involves

a trade-off between strategic surprise capability and deterrence. Consequently, actors seeking to deter rivals—be it from an offensive attack or retaliation—would likely reveal genetic military capability. Such is especially the case when these actors do not already possess the only rivaling source of deterrence: nuclear weapons. Nonnuclear states and non-state actors would, therefore, be most likely to make public their genetic weapons capability. The actors most likely to conceal it are nuclear states.

The question of whether to use genetic weapons covertly or openly also entails a trade-off. Covert use confers strategic and tactical benefits, such as tactical surprise, plausible deniability, and versatility. The benefits of unrestricted use are primarily psychological and symbolic.<sup>12</sup> Consequently, those seeking genetic weapons' psychological or symbolic benefits would be most likely to use genetic weapons openly. This category comprises terroristic, genocidal, and apocalyptic regimes and non-state actors.<sup>13</sup> Others would likely opt for covert use.

### **Technologies of Genetic Warfare**

Biological weapons have been dubbed “a failed military innovation.”<sup>14</sup> The United States and USSR researched and produced them during the Cold War but did not use them.<sup>15</sup> With a few horrific exceptions, modern states have not turned biological agents into weapons of choice.<sup>16</sup>

Experts widely regard biological weapons as “inefficient, unpredictable, and more likely to harm their users than their intended targets.”<sup>17</sup> Effective use requires overcoming three sets of obstacles. The first is that of weaponization or turning a biological agent into a working weapon. Here arise questions of availability, infectivity, casualty effectiveness, immunization, and therapy.<sup>18</sup> That is, is the agent capable of producing an infection that would interfere with the target's normal activities in the desired way and against which the target is defenseless?

The second set of obstacles concerns the agent's delivery. Here arise questions of resistance, epidemicity, and detection. How will the agent reach the target? Can it maintain its virulence outside of the lab by withstanding destructive environmental conditions, such as the ultraviolet radiation of sunlight? Will it mutate? How will it spread from host to host?

Finally, there is the question of precision. Biological weapons have seen minimal modern battle mainly because they are indiscriminate, affecting all exposed to them.<sup>19</sup> Targeting and blowback (“retroactivity”) are as critical as those of weaponizability and delivery. Could the biological agent be used selectively against a specific target? Could it backfire against those using it?

Some have been understandably circumspect about the potential of the recent advances in biotechnology to cause serious threats. For example, Sonia Ben Ouaghran-Gormley highlights unpredictability as a significant problem in processing and handling any biomaterials, which “evolve, are prone to developing new properties, and are sensitive to environmental and handling uncertainties.”<sup>20</sup> Weapons relying on biomaterials will, she argues, always be “captive to the complexity of living systems, and despite the progress made in understanding their functions and composition, the process of creating and maintaining viable organisms still retains a great deal of mystery.”<sup>21</sup> The complexity of living systems can be both a challenge and a potential benefit to keeping organisms viable. The recent experience with the mutating coronavirus has demonstrated what Charles Darwin observed in *Origin of Species* (and Jeff Goldblum reaffirmed in *Jurassic Park*): life finds a way. A virus that can survive contact with the human immune system can better mutate to avoid the immune response. Among the other challenges to progress previously identified in the literature are software development and management of large data sets, and social and economic factors, such as organizational pathologies and market failures.<sup>22</sup> The National Academy of Sciences lists several bottlenecks to synthetic biology-enabled capability, but it also predicts that some of them “will likely widen and some barriers will be overcome.”<sup>23</sup> In other words, science finds a way.

The following explains how emerging technologies are enabling state and non-state actors to overcome the traditional impediments to biological warfare. It identifies some of the existing challenges and the breakthroughs that suggest that overcoming these challenges is only a matter of time.

### ***Weaponizability***

Biological weapons do not require genetic engineering. However, the new techniques for changing an organism’s genetic makeup open the possibility “to develop—either deliberately or accidentally—pathogens with enhanced transmissibility or lethality, including entirely new kinds of biological agents and toxins.”<sup>24</sup> Neither engineering existing living organisms nor creating novel ones would be possible, however, without the “super-exponential growth” in genomic data generation over the past decade due to advances in sequencing technologies, bioinformatics, and artificial intelligence.<sup>25</sup>

The global leader in DNA sequencing is China. In 2010, BGI (formerly the Beijing Genomics Institute and now a Shenzhen-based firm) purchased 128 of the world’s fastest sequencing machines, gaining more than half the

global capacity for decoding DNA.<sup>26</sup> Its stated goal is to sequence the genomes of one million people, one million plants and animals, and one million microbial ecosystems.<sup>27</sup> Other successful sequencing companies include Beijing-based Novogene, founded in 2011 by a former BGI executive.

Genomics research is characterized by a culture of open access sharing of large-scale DNA sequence data, a legacy of the Human Genome Project.<sup>28</sup> The exponentially increasing volume of genomic data is prompting initiatives to make the data more accessible.<sup>29</sup> Even data storage is being pursued genetically. In a study published in 2017, researchers efficiently encoded onto a speck of DNA information such as an entire computer operating system, a film, a \$50 Amazon gift card, and a computer virus and then successfully retrieved all the digital content. The process is still costly, but the study revealed that “DNA has the potential to provide large-capacity information storage”—millions of megabytes of information could be stored in a single gram of DNA.<sup>30</sup>

Making the plethora of genomic data legible is AI, which uses computer systems to do what previously required human intelligence.<sup>31</sup> For example, the artificial neurons of a group of algorithms known as “deep learning” make accessible to humans vast and complex data sets.<sup>32</sup> The tools and techniques for the analysis, storage, and distribution of genomic data (i.e., bioinformatics), especially when combined with artificial intelligence, also enable simulation that could be used to optimize genomic weaponization.

In 2015, CRISPR (clustered regularly interspaced short palindromic repeats) ushered a “huge revolution” in gene editing by “effectively democratiz[ing] the technology so that everyone is using it.”<sup>33</sup> It is now allowing researchers to cheaply and quickly change the DNA of almost any organism, including human.<sup>34</sup> The CRISPR technique relies on a class of enzymes (called “Cas” for “CRISPR-associated,” Cas9 in particular) that uses a guide RNA molecule to pinpoint its target DNA that then edits the DNA to disrupt genes or to insert desired sequences. Researchers typically need to order only the RNA fragment, as the other components can be bought off the shelf. The total cost of gene editing is as little as \$30, and the technique is even taught in middle-school science classes.<sup>35</sup> CRISPR’s affordability, availability, and ease of use increase the prospects of its misuse “not only by a malicious actor but also through accident.”<sup>36</sup>

Technologies such as CRISPR are, as the US intelligence community’s 2016 worldwide threat assessment put it, “almost always dual-use” and “diffuse rapidly around the globe.”<sup>37</sup> And research is gradually overcoming its technical limitations. In 2015, the first human embryos were genetically engineered using CRISPR.<sup>38</sup> Efficiency was low, some cells were altered

while others were not within the same embryo, and “off-target” mutations were observed. However, in just two years, these problems were largely overcome. Scientists repaired a severe disease-causing mutation by successfully editing genes in human embryos. In the ensuing embryos, all cells were mutation-free, and there was no evidence of off-target mutations.<sup>39</sup>

In 2020, the United States turned to CRISPR to battle the SARS-CoV-2 coronavirus causing the COVID-19 disease. The Food and Drug Administration granted its first “emergency-use” approval for a coronavirus test involving CRISPR, selected for its ability to detect (and signal with fluorescent glow) SARS-CoV-2 genetic material from a nose, mouth, or throat swab in about an hour.<sup>40</sup>

The CRISPR approach is relatively simple and widely accessible, but applying it successfully to accomplish a specific change in an organism is still a work in progress. An analogy is word processing on a computer. It is easy to edit a document but very difficult to generate a novel. The latter still takes unique expertise and experience.<sup>41</sup> It is not easy to obtain, maintain, and successfully propagate living organisms. It is harder still to figure out what DNA to change and how to accomplish a specific change in the function of an organism. The CRISPERed human embryos edited out genetic diseases, but it took decades to identify the exact genetic mutations causing them. They were all relatively simple genetic mutations and disorders. Most biological traits have a more complex genetic basis. Even if a simple pathogen is selected and made more virulent or weaponized, it is still challenging to scale up production and mass produce.

Genetic editing is not the only route to weaponization, however. An infectious agent can be synthesized. Its DNA can be created from scratch using chemical precursors and then inserted into a host cell where it can “come alive.”<sup>42</sup> In 2002, a team of researchers from the State University of New York at Stony Brook synthesized an artificial poliovirus from scratch.<sup>43</sup> They obtained the virus’s genetic sequence online; ordered small, tailor-made DNA sequences; and combined them to reconstruct the complete viral genome. They then added a chemical cocktail to bring the synthesized DNA to life. Such a method could synthesize other viruses with similarly short DNA sequences, such as Ebola.

The field of synthetic biology, which involves “selectively altering the genes of organisms to make them do things that they would not do in their original, natural, untouched state,” is advancing rapidly.<sup>44</sup> It essentially treats biological systems as computers—as “programmable manufacturing systems”—by “making small changes in their genetic software” to “effect big changes in their output.”<sup>45</sup> A variety of genetic engineering strategies are

now available to “increase control” over genetic interactions, such as pleiotropy (a single gene having more than one, seemingly unrelated, effect).<sup>46</sup>

## *Delivery*

In 1963, the CIA tried to assassinate Cuban leader Fidel Castro with biological weapons. The unwitting assassin was American lawyer James Donovan (notably played by Tom Hanks in the Oscar-nominated movie *Bridge of Spies*). Donovan was conducting the first-ever secret negotiations with Castro and planning to give him a scuba diving suit as a confidence builder. The CIA planned to contaminate the scuba suit and the accompanying breathing apparatus with Madura foot fungus (causing a chronic skin infection) and tuberculosis bacteria. However, the plot was shelved when an agency insider alerted Donovan to possible CIA tampering.<sup>47</sup>

Arranging for a biological warfare agent to be absorbed through (or injected into) the target’s skin is, as the case of Castro shows, a logistical nightmare. Even if such a delivery method may be effectively used for assassination, it is unlikely to be used to cause mass casualties.

Biological warfare agents can be disseminated in several other ways. Aerosol sprays disperse airborne germs as fine particles. However, they require the target to breathe a sufficient quantity of the particles into the lungs. Many toxins lose their toxicity when aerosolized as well as when the aerosol cloud enters the atmosphere. A sudden change in wind direction may also impair the entire operation. On four separate occasions, the Japanese religious cult Aum Shinrikyo (“Supreme Truth”), notorious for its 1995 nerve gas attack, attempted to spray a bacterial agent over Tokyo. Despite its “impressive resources, dedicated personnel, and high motivation,” none of the efforts succeeded, illustrating that it is “far more difficult to carry out a deadly bioterrorism attack than has sometimes been portrayed.”<sup>48</sup> Aum carried out its attacks during the summer, with sunlight and smog likely degrading the bacterial agent. One of the attacks was during a rainy month, so the aerosolized particles were likely washed out of the air.<sup>49</sup>

Another bioweapons delivery mechanism is explosives, whether artillery, missiles, or detonated bombs. The explosives method is even less effective than aerosols because the blast destroys about 95 percent of the disease-causing agent. Deadly agents can also be put into food or water. The logistics are a significant limiting factor here as well. Contaminating a city’s water supplies, for example, requires “an unrealistically large” amount of an agent.<sup>50</sup>

Delivery problems have made biological weapons tactically unappealing.<sup>51</sup> Effective delivery requires the deadly agent to reach its target. Doing so requires a robust agent and a reliable delivery mechanism. New technologies are enabling both.

Most bacterial and viral agents struggle to maintain their virulence when confronted with common environmental factors, such as sunlight and humidity, and high temperatures or radical temperature changes. They also evolve and mutate. Genetic instability is typical for microorganisms. With increased transmissibility often comes reduced virulence. Production of virus molecules involves passage through host organisms. As the virus is not subject to any evolutionary pressure to maintain virulence during this scaling-up process, it tends to accumulate mutations that generate an attenuated strain. Similarly, bacteria cultured in laboratories tend to lose virulence.<sup>52</sup>

Gene editing and synthetic biology research are making strides in overcoming the problem of genetic instability. A study published in 2019 presented a new system, CRISPR-BEST. It created mutations in actinomycetes (bacteria that produce a wide variety of industrially and medically relevant compounds) without creating genetic instability and forcing them to rearrange and even delete large parts of their chromosomes.<sup>53</sup> Synthetic biology is also increasingly embracing genetic instability rather than trying to suppress or compensate for it. With improved understanding, it is expected to design devices that incorporate genetic instability as a parameter.<sup>54</sup> Such devices would be “a true frontier in biological engineering.”<sup>55</sup>

When it comes to delivery, nanotechnology can prevail where aerosols, explosives, and in-person methods falter. Nanotechnology exploits the behavior of materials ranging from 1 to 100 nanometers, visible only through the most powerful microscopes.<sup>56</sup> In their suggestions for a new NATO Strategic Concept, a group of experts (led by former US secretary of state Madeleine Albright) identified nanotechnology as a “potentially disruptive development” that could “transform the technological battlefield.”<sup>57</sup>

Nanotechnology offers new delivery possibilities for biological and genetic weapons. In the future, nano-carriers and capsules may transport small toxins, such as ricin or microbe subunits (e.g., the lethal factor of anthrax), across otherwise impermeable cell membranes and the blood-brain barrier. Bioagents’ targeted delivery with nanoparticles is likely to increase effectiveness and, thus, require less of the agent.<sup>58</sup> Nanotechnology could also enable controlling biological weapons once they enter the body.<sup>59</sup>

Speculative literature predicts the production of nanoscale robots that would enter the body and penetrate cells, causing them to act similarly to

the effects of a biological or chemical weapon.<sup>60</sup> Experts also speculate that, in the future, “insect-like” nanobots could be programmed to inject toxins into humans.<sup>61</sup> No scuba gear required.

The field of synthetic biology encompasses hybrid technology that combines living and nonliving elements.<sup>62</sup> Biological organisms can be enhanced with nanotechnology, or nanotechnology (e.g., nanobots) can be enhanced with biological elements. This includes technology-enhanced organisms (or viruses) at one end of the spectrum and biologically-enhanced machines at the other end. Somewhere in the middle, an organism crosses the line between living and nonliving. The latter would not have the inherent capacity to mutate, reproduce, and evolve.

Combining genetically engineered DNA using CRISPR and nanotechnology-based vectors for packaging and delivery could help overcome the inherent liabilities of natural biological weapons. It would make them more durable, efficient, and precise. Since they would not be alive and would not evolve, their behavior would be much more predictable and amenable to engineering than living agents would be. Synthetic biology could be used to create “smart germs” that combine the biological functions of DNA with synthetic manufacturing, delivery, and targeting systems that include hybrid biological and synthetic mechanisms. An example might be a nanoscale microchip that is ingested or breathed in, activated by a specific host, that uses a microfluidic chip and engineered DNA to absorb reagents from the host’s body and manufacture a specific toxin or pathogen.

## ***Precision***

Could a weaponized biological agent be delivered to the intended target and affect only that target? This is the problem of precision, and, like the problems of weaponizability and delivery, it had made biological weapons unreliable. New technologies allow precise or selective targeting by tailoring deadly agents specifically for a given group or individual.

The idea of using genetic information to target specific groups with biological or chemical weapons was first publicly aired in 1970 in *Military Review*, the US Army’s professional journal. The article considers the prospect of weaponizing genetic differences—specifically in the activities of enzymes—between different ethnic groups. That is, certain groups may be more vulnerable than others to a given naturally occurring agent.<sup>63</sup> Written before the age of genetic engineering and biotechnology, the article drastically underestimates what is possible.



There are far more genetic similarities between individuals and human populations than differences. However, differences exist. This is not because social categories like ethnicity or race are biological but because populations differ in the frequencies of some alleles (i.e., marker alleles) they carry. The differences are a product of microevolution as the human species spread around the globe and adapted to living in different environments.<sup>64</sup> A case in point is the adaptation to malaria through a high frequency of sickle cell anemia found in populations in West Africa.<sup>65</sup>

Over time, natural selection spreads across human populations' genetic variants, granting resistance to particular infectious diseases. These genetic variants leave "distinctive, detectable patterns of genetic variation in the human genome."<sup>66</sup> Also, they "may singly or in combination distinguish the members of one social group (an 'ethnic' group) from another."<sup>67</sup>

Toxin resistance may be among the genetic differences that could be exploited militarily. In a study published in 2011, researchers exposed anthrax bacterium cells from people of African, Asian, European, and North American descent (whose tissues were taken for a freely available genome database). Most of the cells fell to the assaults. However, cells from three people of European descent required hundreds or even thousands more times as much anthrax toxin to kill them. The researchers traced the broad range in anthrax sensitivity to regulating a specific gene (CMG2), which codes for a protein that controls anthrax's ability to access human cells.<sup>68</sup>

Another source of genetic variation is in the noncoding regions of the human genome. The technique of genetic fingerprinting, which dates back to the mid-1980s, can be used to identify regions in the noncoding DNA with a high rate of mutation—the so-called minisatellites. The minisatellites arise from mistakes in replication, and their unique patterns can be used to identify specific individuals. They can also be used to identify groups, as patterns of variation between individuals "is characteristic of a particular group and differs from group to group."<sup>69</sup>

Personal genomics companies like 23andMe collect genetic data through saliva-based, direct-to-consumer genetic testing and have already raised concerns about the prospect of Google-style data hoarding. A state or non-state actor could potentially apply the massive computational power to genomic databases, such as 23andMe and Ancestry.com, to design agents specific to individuals, a family, or a group.<sup>70</sup> The larger the group, the less precise the targeting. However, the most vulnerable populations would be those with minimum genetic diversity due to remaining mainly in their ancestral geographic regions with little outbreeding or

those that are genetically distinct even if dispersed. Among such populations may be Uighurs and Ashkenazi Jews.

One would not need individual genomes. Random DNA samples could be collected from sewer systems or subway cars, and they would provide an excellent genetic profile of a population. Coupling algorithms could further increase geographic and ethnic specificity for human DNA signatures (e.g., YES for sequence one, YES for sequence two, NO for sequence three, etc.) to target people with specific sequences but not others. This information could then be combined with DNA from the microbiome (gut) bacteria, which is also very specific in many dimensions. An ingested agent could sample the microbiome first and, if it is a match, enter the body and sample the host DNA.

The same principle could be applied to target crops and farm animals more efficiently than humans since most crops and farm animals are cloned or derived from a small group of prime breeders. Biosynthetic agents manufactured at a nanoscale could be mass-produced and include a high level of specificity. They would also not be alive, so they would not reproduce or reproduce only in specific hosts or conditions. These characteristics would limit both collateral and retroactive casualties.

By combining nanotechnology, computational power, and synthetic biology with AI and robotics, one can imagine a future involving various types of robots, drones, or satellites that could manufacture and deliver “smart germs” anywhere in real time.

In 2019, the US Department of Defense advised all military personnel against using direct-to-consumer genetic tests because they “could expose personal and genetic information, and potentially create unintended security consequences and increased risk to the joint force and mission.”<sup>71</sup> It did not specify the unintended security consequences or increased risk.

Private DNA databases with identifying information could be hacked by (or sold to) malicious actors. Perhaps the Department of Defense worried that China was among those actors. Since 2017, the Chinese government has placed at least one million Uighurs and members of other minority groups in “prisonlike” detention centers “as part of a campaign to stop terrorism.”<sup>72</sup> Hundreds of thousands of them were compelled to provide blood samples. Using their DNA (and with the help of American and European firms), the Chinese government is developing phenotyping technology that would predict someone’s skin color, eye color, ancestry, and other features. Its current goal is to identify a person’s physical appearance from a genetic sample alone.<sup>73</sup>

Experts worry that the phenotyping technology may be used not just for surveillance but also to “decide that someone does belong or does not belong” to a particular race or ethnicity.<sup>74</sup> It could also potentially be used to produce weapons that target individuals or groups based on characteristics such as skin color or ancestry.

Genetic editing could also enable delayed targeting, such as a particular group’s or individual’s future generations.<sup>75</sup> One possible mechanism for doing so may be the so-called gene drive. Gene drives allow propagating new genetic traits into or disabling an unwanted trait within the entire population not immediately but over a few generations. They can override standard molecular mechanisms of inheritance, thus ensuring that virtually all offspring inherit a newly engineered trait. The technique has been used mainly on sexually reproducing species with short life spans and numerous offspring, such as mosquitos and fruit flies. It would not work on bacteria or viruses because they reproduce asexually, but theoretically could be used on humans.<sup>76</sup> The Imperiale Framework describes the use of human gene drives as “impractical” because it relies on generations of sexual reproduction to spread a harmful trait, thus “warrant[ing] a minimal level of concern.”<sup>77</sup>

Delayed targeting could take another form in the future. In 2003, the CIA requested that the National Academy of Sciences hold a closed seminar to consider the security implications of the recent and anticipated advances in genetic engineering. Among the scenarios the panel identified was a “stealth” virus that could be programmed to infect human cells and then remain dormant without provoking disease.<sup>78</sup> Stealth viruses exist in nature, with the notorious herpes virus a case in point. Engineered to be contagious and silently spread through the population years in advance, they would then “be activated by an internal or external signal and produce illness in infected individuals.”<sup>79</sup> Or as one medical expert reckoned, a threat of activation could be used as blackmail.<sup>80</sup> The 2018 National Academy of Sciences report describes the stealth introduction of an engineered threat into the human microbiome as an area of “medium-high concern.” Nevertheless, it also points out that, given our “nascent understanding” of the human microbiome, any targeted manipulation there would be difficult to detect or attribute.<sup>81</sup>

## **International Politics of Genetic Warfare**

Just one week after the September 11 attacks, letters laced with anthrax began arriving at media and congressional offices. Coupled with the earlier revelations about the magnitude of the Soviet and Iraqi biowarfare pro-

grams, biological weapons came to be viewed as “one of the key security issues of the twenty-first century.”<sup>82</sup> Two decades later, the specter of bio-warfare reemerged. With the COVID-19 pandemic came the fear that “the invisible enemy can hide within our ranks, multiplying in secret, planting time bombs in our bodies, and all before we know what’s hit us.”<sup>83</sup>

The fear of secret genetic weapons capability and use is not limited to malicious non-state actors. In what has been characterized as a sign of “a new Cold War,” a Chinese foreign ministry spokesman suggested in March 2020 that the US Army may have brought COVID-19 to Wuhan.<sup>84</sup> The US secretary of state responded in kind by alleging that the outbreak originated in a Chinese laboratory.<sup>85</sup> All the while, conspiracy theories about the origins of the disease spread on online platforms. Among them were the claims that the virus was part of China’s “covert biological weapons program” and that a Canadian-Chinese spy team sent the virus to Wuhan.<sup>86</sup> Such undiplomatic exchanges and conspiratorial claims are particularly hazardous in the era of global competition among great powers.<sup>87</sup>

Biological weapons have always been more accessible than nuclear ones. However, with genetic engineering increasingly solving the problems of weaponization, delivery, and precision, Ebola expert Karl Johnson predicts that “any crackpot with a few thousand dollars’ worth of equipment and a college biology education under his belt could manufacture bugs that would make Ebola look like a walk around the park.”<sup>88</sup>

Predictions about genetic warfare would benefit from identifying the closest parallels and then adjusting and synthesizing the ensuing models. Genetic weapons have the destructive potential of nuclear weapons, but their ease of development is akin to cyber weapons. Both genetic and cyber warfare require inexpensive equipment and only a college-level understanding of these fields. Unlike nuclear weapons that demand enormous engineering expertise, a small team can develop and hone cyber and genetic weapons using common equipment.<sup>89</sup>

Dual-use capability is another similarity. Unlike nuclear and chemical weapons, genetically engineered bioweapons do not require equipment or materials exclusively tailored to their purpose. This concern was among the first raised in the US National Security Strategy in 2017.<sup>90</sup> As one military analyst stated, “A nuclear weapons facility has obvious signals to the outside world. We can look at it and immediately say, ‘Ugh, that is a nuclear reactor. However, the technology for conducting biological weapons research is essentially the same as [for] what keeps a population healthy.’”<sup>91</sup> Many biological engineering techniques with dual-use potential are holy grails of medicine. Research journals publish techniques and results inter-

nationally, publicly, and without consideration for their security implications.<sup>92</sup> Dissemination of this information limits the effectiveness of the Biological Weapons Convention (BWC) and domestic control regimes.<sup>93</sup>

Biological weapons programs are far more challenging to detect than nuclear programs. They look like other biological research programs. The body charged with enforcing compliance with the BWC, the Implementation Support Unit, is significantly underfunded compared to the enforcement arms of the Chemical Weapons Convention and Non-Proliferation of Nuclear Weapons agreements. Much like for cyber weapons, custom bioweapon development is effectively unregulated.<sup>94</sup>

Genetic and cyber weapons are also similar in their strategic utility in terms of versatility, durability, and deniability. The scope and specificity of genetic weapons make them more analogous to cyber than any of the traditional weapons of mass destruction. Genetically engineered bioagents can achieve levels of specificity that were previously impossible using traditional pathogens. Targets can include ethnic groups and even specific individuals. They need not even be human: tailored pathogens can affect rubber, plastics, and other defense and infrastructure-related materials.<sup>95</sup> Similarly, cyberweapons can attack power grids and other nonhuman targets. Versatility, or the capacity to take on different forms of varying lethality against varied targets, makes genetic weapons potentially even more hazardous than nuclear weapons.

Finally, unlike nuclear, but similar to cyber, genetic weapons can be used covertly. Thus, those who employ them have plausible deniability. Much like North Korea proxies' use of ransomware or Russia's disinformation campaigns, a genetic weapon would be difficult to attribute. Even chemical weapons do not have this advantage. Attempts to deny their use, such as in Ghouta, Syria, typically fail miserably upon investigation.<sup>96</sup>

The ease of development and strategic benefits of genetic weapons make them, as one forecaster put it, "the most dangerous threat humanity has ever faced."<sup>97</sup> What would states and non-state actors do once they acquired them? Would they keep their genetic war capability secret? Would they use genetic weapons openly or covertly? These questions are considered next.

### ***Genetic War Capability: Reveal or Conceal?***

Underlying the question of whether to reveal or conceal genetic military capability is a trade-off. To conceal it is to gain a potent secret edge over rivals. To reveal it is to deter or frighten others from attacking.<sup>98</sup>

Deterrence works “because the expected reaction of the attacked will result in one’s own severe punishment.”<sup>99</sup> It is “the power to dissuade.”<sup>100</sup>

Two factors determine whether actors reveal their clandestine capability, according to Brendan Rittenhouse Green and Austin Long.<sup>101</sup> The first is the uniqueness of the capability—the less unique, the less attractive is concealing relative to revealing. The second is the prospect that the adversary will implement countermeasures. Successful countermeasures can sharply degrade a weapon’s military value.<sup>102</sup> The lower the odds of countermeasures, the more likely the actors are to reveal their clandestine capability.

The decision to reveal one’s clandestine capability ultimately depends on one’s need for deterrence. Traditional biological weapons could not deter because their outcome was always uncertain. However, without the problems of weaponizability, delivery, and precision plaguing them, genetic weapons could deter even countries with nuclear weapons. The destructive outcome of genetic weapons may be assured, immediate, and massive. A genetically engineered bioagent with a short incubation period could be released as instantly as a nuclear agent on a population of millions.<sup>103</sup> And, unlike nuclear weapons, which rely on city and civilian attacks, an attack by a genetic weapon is more likely to be militarily decisive—that is, to influence leaders’ decisions about war and surrender. Its effects could inflict harm not only on civilians but also on the leaders themselves.<sup>104</sup> All of these factors make genetic weapons potentially more potent than nuclear weapons as a mechanism of deterrence.

Accordingly, state and non-state actors that need to demonstrate credible deterrence are most likely to reveal their genetic war capability. These actors lack the only other rivaling source of deterrence—nuclear weapons. Because they may be threatened or greedy, they are “willing to incur costs or risks for non-security expansion.”<sup>105</sup> Nuclear states are the actors most disposed to conceal genetic war capability. They can reap the strategic benefits of hidden genetic power without worrying about survival-threatening aggression or retaliation.

Do the effects of genetic weapons need to be demonstrated for them to have a deterrence outcome similar to nuclear weapons? It may be that recent outbreaks, such as Ebola or COVID-19, provide the element of proof needed to convince a population and its political representatives of the credibility of the threat. The recent experience with outbreaks may instill, at least in the current generations, strong aversion and even fear. The collective memory of the atomic bombings of Hiroshima and Nagasaki, and even the Cold War-era duck-and-cover drills, has faded. However, the

memory of the COVID-19 pandemic is fresh and potent, especially for the generation that came of age during the pandemic.<sup>106</sup>

What makes genetic weapons unique is their combination of accessibility and destructive potential. Nuclear deterrence requires some evidence that an actor is capable of creating and delivering a nuclear weapon. However, with genetic weapons—including those the Imperiale Framework has deemed most urgent and concerning—no evidence of capability is necessary. Of itself, the accessibility of relevant technologies and know-how can portend a threat. A mere statement of one's willingness to use genetic weapons, combined with some signals of credibility of intention, may be enough to deter others from an attack. This possibility may be a dream for structural realists like Kenneth Waltz, if not for the accessibility of genetic weapons to states and non-state actors alike.<sup>107</sup>

### ***Offensive Use: Open or Covert?***

So too is there a trade-off between the open and covert use of genetic weapons. Covert use confers strategic and tactical benefits, such as surprise, deniability, and versatility. The benefits of unrestricted use are primarily psychological.

The overt use of genetic weapons can be thought of as a form of “costly signaling” or “actions so costly that bluffers and liars are unwilling to take them.”<sup>108</sup> The strategic logics Barbara Walter and Andrew Kydd use to explain costly signaling by terrorist groups—specifically attrition, intimidation, and outbidding—are particularly productive here.<sup>109</sup> These logics rely mainly on psychological mechanisms. Actors engage in attrition to persuade their challenger that they are strong enough to impose costs if the latter continues the disliked course. Actors use intimidation to obtain compliance from others by signaling that they are strong enough to punish disobedience. Outbidding is used to demonstrate a superior resolve.<sup>110</sup> When it comes to using genetic weapons, it is also important to add ideological motivations to the list, especially genocidal and apocalyptic.

In sum, state and non-state actors are likely to use genetic weapons overtly for attrition, intimidation, and outbidding. They would also opt for unrestricted use to claim credit for genocide or ending the world. For everything else, there is covert genetic warfare.

Walter and Kydd specify the conditions under which the signaling mechanisms are likely to bear fruit. Attrition works best when adversaries are not deeply invested in the issue under dispute, are constrained in their ability to retaliate, and are highly sensitive to the costs of violence. Intimidation is effective on weak adversaries. Outbidding signals greater

commitment to the cause when the others are unwilling or unable to match the behavior.<sup>111</sup> The common theme is a relatively weak or politically constrained adversary. Given its invisible nature, open genetic warfare would affect a population physically and psychologically.<sup>112</sup> The ensuing hypothesis is that actors are more likely to openly use genetic weapons against an adversary that is militarily inferior and/or sensitive to the political fallout from the engagement. A militarily weak democratic state would make a prime target.

For some, genetic violence is not just a means but also an end. Genocidal regimes may consider genetic weapons a godsend. Such a prospect was not lost on CRISPR pioneer Jennifer Doudna, who describes a nightmare she had in which a colleague asked her to teach someone how her technology worked. She followed the colleague into a room to meet this person and “was shocked to see Adolf Hitler, in the flesh.”<sup>113</sup>

Some actors with millenarian, apocalyptic beliefs might also welcome an open genetic war. These may include Protestant fundamentalist groups that anticipate an imminent end of history and embrace “radical violence” to hasten “the new heaven and the new Earth, the coming of the Kingdom of God.”<sup>114</sup> Some jihadis, such as Islamic State of Iraq and Syria (ISIS) founder Abu Musab al-Zarqawi, also embrace the notion of end-times and extreme violence. Al-Zarqawi’s brutality was so “unprecedented” that it shocked even al-Qaeda founder Osama bin Laden.<sup>115</sup> Many of the so-called new religious movements, or groups emerging outside the traditional religious categories, are similarly driven by the idea of a total transformation, though few of them embrace violence. Among those that do, Aum Shinrikyo’s chemical and biological attacks in Tokyo suggest that millenarian cults could use genetic weapons secretly for tactical benefits. Violent racist, far-right groups may openly turn to genetic weapons to foment a “race war.” Their fetishization of guns may, however, keep them away from biotechnology.

## Conclusion

The development of biotechnology is rapid and decentralized. Hundreds of Manhattan projects may soon operate from inconspicuous laboratories around the world. How can we contain their security risks, which present an existential threat to humanity? The following options emerge: government regulation, government transparency, government-scientist collaboration, scientific transparency and self-governance, and norms. None is likely to work alone, but together they offer the best chance of preventing genetic war.



"I have not thought of that at all," Albert Einstein remarked when he first learned that the latest nuclear research discoveries, stemming from his famed equation  $E = mc^2$ , enabled the creation of an atomic bomb.<sup>116</sup> He then signed a letter warning President Franklin D. Roosevelt that Nazi Germany could develop nuclear weapons and suggested that the United States initiate its nuclear program. However, it was not Nazi Germany but the United States that dropped atomic bombs on hundreds of thousands of civilians.

In 1953, James Watson and Francis Crick revealed that the genome, which is the entirety of genetic information in any organism, is essentially digital. With the right tools, it can be decoded and edited. An early proponent of mapping the human genome, Watson recognized the need to address the policy implications of the endeavor. The Ethical, Legal and Social Implications (ELSI) program was thus set up as part of the Human Genome Project. The latter began in 1990 and, by 2003, successfully sequenced the 3 billion base pairs that compose human DNA. The goal of the corresponding ELSI program was, as Watson explained, "to address, anticipate, and develop suggestions for dealing with such [ethical, legal, and social] problems in order to forestall adverse effects."<sup>117</sup> The project's cosponsors, the National Institutes of Health and the US Department of Energy, spent over \$100 million on ELSI research.<sup>118</sup> The ensuing work focused on potential discrimination by employers and health insurers, ethical standards for work with human research subjects and tissues, and controversial issues (e.g., cloning, stem cell research, and eugenics).<sup>119</sup> However, paralleling Einstein's initial approach to his research, the security risks of the new technologies were missing from the equation.<sup>120</sup>

What valuable lessons can we draw from the other weapons of mass destruction for limiting, or even preventing, the proliferation and use of genetic weapons? Considering what kept biological weapons from the battlefield in the twentieth century, medical anthropologist Jeanne Guillemin draws lessons from the nonuse of chemical weapons in World War II battlefields. Why did the Allied and Axis military commanders leave an entire class of armaments, tested in battle during World War I, on the shelf? Guillemin identifies four key factors: legal restraints, public opinion, technical drawbacks, and prospects of retaliation.<sup>121</sup> Could these prevent the development and use of genetic weapons?

The Biological and Toxin Weapons Convention, a Cold War-era treaty signed by the United States, China, Russia, and 176 other countries, bans the development of bioweapons. The previous treaty, the Geneva Protocol of 1925, prohibited chemical and biological weapons (but not their de-

velopment, production, and stockpiling). These treaties have, according to some, generated global norms that “clearly contributed to the fact that few countries have been engaged in research into offensive biowarfare during recent decades.”<sup>122</sup>

Others argue that it was not norms generated by international treaties but the impracticalities of biological weapons that rendered them useless. And overcoming these impracticalities was just a matter of time. On the heels of World War II, bacteriologist Theodor Rosebury predicted that next time around, biological weapons would take center stage. He stated, “If World War III is allowed to come, biologists and men of all related fields, including physicians, will be called upon as never before to serve alongside physicists and other scientists as instruments of human destruction.”<sup>123</sup> This prediction was puzzling because biological weapons were conspicuously absent during the Second World War. However, Rosebury reasoned that norms could prevent biological warfare no more successfully than they prevented the use of the crossbow or musket—both of which were, at some point, deemed weapons of cowards.<sup>124</sup> Technical impediments prevented biological warfare. And those were not “beyond the ken of human genius.”<sup>125</sup>

Brian Mazanec considers the development of constraining norms in the domain of cyberspace. He finds that what causes norms to develop there is their alignment with the national interests of powerful states.<sup>126</sup> While we are witnessing the development of norms in cyber warfare thanks to the concerns of countries such as the United States, the chances of their internalization by everyone are meager.<sup>127</sup> The cyber warfare norms most likely to succeed are those that are limited in scope, such as focusing on applying the existing laws of armed conflict to cyber warfare or prohibiting the first use of cyber weapons.<sup>128</sup>

When it comes to the genome domain, one potential avenue for regulation and norms building lies in a focus on a critical ingredient: genetic data. Repurposing some general responses to data privacy concerns may help address the individual’s rights to protect genetic information. A multipronged approach could borrow from national efforts such as the United States’ Health Insurance Portability and Accountability Act (HIPAA) medical privacy laws or multijurisdictional protections such as the European Union’s growing efforts to enshrine a “right to be forgotten.” Also, policy makers could take complementary steps to grant individuals property rights to their genetic material or to utilize intellectual property protection schemes.

Because a research moratorium would be unrealistic, as the science and the technologies are global, the following are the options available for confronting the specter of genetic warfare. One is government transparency. As Guillemin concludes from her study of biological warfare, the threat of such weapons “increases in direct proportion to government secrecy, closed military cultures, and a subsequent lack of accountability to the public.”<sup>129</sup> Another option is scientific transparency and self-governance. At a CIA-sponsored conference of life science experts that addressed the “darker bioweapons future,” a panel suggested that the bioscience community would act “as a living sensor web at international conferences, in university labs, and through informal networks to identify and alert it to new technical advances with weaponization potential.”<sup>130</sup>


Some advocate for more government-scientist collaboration. Most panelists at the CIA conference argued for a “qualitatively different relationship” between the government and life sciences communities. For example, the former could assist the latter in efforts to develop standards and norms to differentiate between “legitimate” and “illegitimate” research.<sup>131</sup> The US National Research Council Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology has, however, advised the US government not to attempt regulating scientific publishing. It argued that scientists and journal editors could screen their papers for security risks. With biological information and tools widely distributed, regulating only US researchers would have little effect.<sup>132</sup>

Optimism about transparency and self-governance characterizes many in the biotechnology community.<sup>133</sup> As one report summed up, “The scientific community historically has demonstrated its ability to lead the way in the responsible development of new technologies.”<sup>134</sup> In 1975, scientists from around the world gathered in northern California at the famed Asilomar Conference Center to discuss the challenges presented by recombinant DNA technology. The technology permitted them to cut “long, unwieldy molecules of nucleotides into digestible sentences of genetic letters and paste them into other cells.”<sup>135</sup> The scientists considered laboratory and environmental safety and concluded that the field required little regulation. There was no real discussion of deliberate abuse because “at the time, there didn’t seem to be any need.”<sup>136</sup>

This need now exists. The scientific community is currently debating what to do about the emerging technologies of the so-called Fourth Industrial Revolution,” including biotechnology and gene editing. The community supports advancing biosecurity tools and practices like gene synthesis screening and keeping scientists informed about and involved in the

development of policies.<sup>137</sup> It also advocates that it is vital for the United States to collaborate with “equally capable and like-minded allies and partners,” such as South Korea and India.<sup>138</sup> Some advise the United States to provide global leadership on safety standards while expanding security cooperation in the areas of global health, gene synthesis, and medical and pharmaceutical research.<sup>139</sup>

There is also essential work emphasizing the need for government regulation and a national strategy. The 2018 National Academies of Sciences report stresses the need for the government to develop new approaches to meet the new challenges while not abandoning the traditional tools for biological and chemical defense. For the former, it identifies the importance of nimble and adaptable strategies, given the rapid rates of technological change and uncertainty about which approaches an adversary might pursue.<sup>140</sup>

Drawing on the Imperiale Framework, Marcus Cunningham and John Geis propose a framework that prioritizes threats, regulates synthetic biology processes (not products) to guard against accidents and abuses, controls US technology exports, builds international cooperation, and conducts horizon scanning on machine learning.<sup>141</sup> They contend that the United States needs “a separate, comprehensive, whole-of-government national strategy.” Further, the strategy must be globally exportable, as it “cannot be successful if America imposes unilateral restrictions on its activities that the rest of the world ignores or exploits.”<sup>142</sup> Because it cannot wholly coerce or induce other states (and non-state actors) to adopt its model, the United States will also need to devote attention and resources to building global norms for new technologies in the coming decades. Such an effort would require a vast reservoir of soft power. 

### Acknowledgments

The author wishes to thank Brian Roberge and Jared Schwartz for research assistance, Bernard Possidente for guidance, and the Judith Johns Carrico Faculty Grant for supporting fieldwork.

### Yelena Biberman

Dr. Biberman is an associate professor of political science at Skidmore College, a fellow at West Point’s Modern War Institute, and a nonresident senior fellow at the Atlantic Council’s South Asia Center. She is the author of *Gambling with Violence: State Outsourcing of War in Pakistan and India* (Oxford University Press, 2019).

## Notes

1. Francis Fukuyama, *Our Posthuman Future: Consequences of the Biotechnology Revolution* (New York: Picador, 2002).
2. The term refers to the future Homo sapiens with God-like powers in Yuva Harari, *Homo Deus: A Brief History of Tomorrow* (New York: Random House, 2016).
3. Vladimir Putin, "Being Strong: National Security Guarantees for Russia," *Rossiiskaya Gazeta*, 28 February 2012, <https://www.voltairenet.org/>.
4. Putin.
5. Joby Warrick, "Putin Expands Secret Military Labs for 'Genetic' Bombs as Powerful as Nukes," *Miami Herald*, 19 March 2018, <https://www.miamiherald.com/>.
6. Marcus A. Cunningham and John P. Geis II, "A National Strategy for Synthetic Biology," *Strategic Studies Quarterly* 14, no. 3 (Fall 2020): 49–80, <https://www.airuniversity.af.edu/>.
7. James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community Senate Armed Services Committee*, 9 February 2016, 9, <https://www.dni.gov/>.
8. Clapper, 9.
9. National Academies of Sciences, Engineering, and Medicine (NASEM), *Bio-defense in the Age of Synthetic Biology* (Washington, DC: The National Academies Press, 2018), 3, <https://doi.org/10.17226/24890>.
10. NASEM, 3–5.
11. Ben Westcott and Steven Jiang, "Chinese Diplomat Promotes Conspiracy Theory That U.S. Military Brought Coronavirus to Wuhan," CNN, 13 March 2020, <https://www.cnn.com/>; and Julian Borger, "Mike Pompeo: 'Enormous Evidence' Coronavirus Came from Chinese Lab," *Guardian*, 3 May 2020, <https://www.theguardian.com/>.
12. Gary Ackerman, "Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism," in *Routledge Handbook of Terrorism and Counterterrorism*, ed. Andrew Silke (New York: Routledge, 2018).
13. Apocalyptic regimes are led by individuals who hold and/or strategically employ doomsday beliefs. For example, see William McCants, *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State* (New York: Picador, 2015).
14. Jeanne Guillemin, *Biological Weapons: From the Invention of State-Sponsored Programs to Contemporary Bioterrorism* (New York: Columbia, 2005), 205.
15. The United States disavowed biological weapons in 1969. US president Richard Nixon characterized them as having "massive, unpredictable, and potentially uncontrollable consequences," such as pandemics and "impair[ing] the health of future generations." This was the first time a significant power unilaterally abandoned an entire weapon category. Nixon believed that biological weapons had limited tactical utility on the battlefield and were an unreliable strategic deterrent. He also calculated that public denunciation of biological weapons would make it easier for the US to retain its chemical weapons capability, which was of much greater value to the Pentagon. It would "dampen criticism of the ongoing U.S. combat use of tear gas and herbicides in Vietnam," which the Nixon administration intended to continue. Jonathan B. Tucker and Erin R. Mahan, *President Nixon's Decision to Renounce the U.S. Offensive Biological Weapons Program* (Washington, DC: National Defense University Press, October 2009), 10; and Brian M.

Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Lincoln: University of Nebraska Press, 2015), 55.

16. Gigi Gronvall, "The Security Implications of Synthetic Biology," *Survival* 60, no. 4 (August–September): 170.

17. Andrew Moscrop, "Mass Hysteria Is Seen as Main Threat from Bioweapons," *British Medical Journal* 323, no. 3 (November 2001): 1023, <https://www.ncbi.nlm.nih.gov/>.

18. The list of obstacles is adapted from Theodor Rosebury, Elvin A. Kabat, and Martin H. Boldt, "Bacterial Warfare, A Critical Analysis of the Available Agents, Their Possible Military Applications, and the Means for Protection Against Them," *Journal of Immunology* 56, no. 1 (May 1947): 7–96, <https://europepmc.org/>.

19. British Medical Association, *Biotechnology, Weapons and Humanity* (Australia: Harwood Academic Publishers, 1999), 3.

20. Sonia Ben Ouagrham-Gormley, *Barriers to Bioweapons: The Challenges of Expertise and Organization for Weapons Development* (Ithaca, NY: Cornell University Press, 2014), 5.

21. Ben Ouagrham-Gormley, 5–6.

22. Gigi Kwik Gronvall et al., *The Industrialization of Biology and Its Impact on National Security* (Pittsburgh: Center for Biosecurity of UPMC [University of Pittsburgh Medical Center], 8 June 2012), 1, <https://www.centerforhealthsecurity.org/>; and Kathleen M. Vogel, "Intelligent Assessment: Putting Emerging Biotechnology Threats in Context," *Bulletin of the Atomic Scientists* 69, no. 1 (2013): 45, <https://doi.org/10.1177/%2F0096340212470813>.

23. NASEM, *Biodefense in the Age of Synthetic Biology*, 7–8.

24. Cunningham and Geis, "National Strategy for Synthetic Biology," 50.

25. Eric D. Green, Edward M. Rubin, and Maynard V. Olson, "The Future of DNA Sequencing," *Nature* 550 (October 2017): 179–81, <https://doi.org/10.1038/550179a>.

26. Green, Rubin, and Olson, 179–81.

27. Green, Rubin, and Olson, 179–81.

28. Stacey Pereira, Richard A. Gibbs, and Amy L. McGuire, "Open Access Data Sharing in Genomic Research," *Genes* 5, no. 3 (2014): 739–4, <https://doi.org/10.3390/genes5030739>.

29. An example of this is the FAIR (Findability, Accessibility, Interoperability, and Reusability) Principles for genomic data sets. Mark D. Wilkinson et al., "The FAIR Guiding Principles for Scientific Data Management and Stewardship," *Scientific Data* 3 (March 2016), <https://doi.org/10.1038/sdata.2016.18>.

30. Yaniv Erlich and Dina Zielinski, "DNA Fountain Enables a Robust and Efficient Storage Architecture," *Science* 355, no. 6328 (March 2017): 950, <https://doi.org/10.1126/science.aaj2038>.

31. For more on the strategic implications of AI, see James S. Johnson, "Artificial Intelligence: A Threat to Strategic Stability," *Strategic Studies Quarterly* 14, no. 1 (Spring 2020): 16–39, <https://www.airuniversity.af.edu/>.

32. Raquel Dias and Ali Torkamani, "Artificial Intelligence in Clinical and Genomic Diagnostics," *Genome Medicine* 11, no. 70 (2019): 4, <https://genomemedicine.biomedcentral.com/>.

33. Dias and Torkamani, 4.

34. CRISPR researcher (Cold Spring Harbor Laboratory, NY), interview by the author, October 2017.

35. Alan Yu, "How a Gene Editing Tool Went from Labs to a Middle-School Classroom," NPR, 27 May 2017, <https://www.npr.org/>.
36. Rachel M. West and Gigi Kwik Gronvall, "CRISPR Cautions: Biosecurity Implications of Gene Editing," *Perspectives in Biology and Medicine* 63, no. 1 (Winter 2020): 74, doi:10.1353/pbm.2020.0006.
37. Clapper, *Statement for the Record*, 6.
38. Puping Liang et al., "CRISPR/Cas9-Mediated Gene Editing in Human Triplo-nuclear Zygotes," *Protein Cell* 6, no. 5 (2015): 363–72, <https://pubmed.ncbi.nlm.nih.gov/>.
39. Hong Ma et al. "Correction of a Pathogenic Gene Mutation in Human Em-bryos," *Nature* 548 (24 August 2017): 413–19, <https://doi.org/10.1038/nature23305>.
40. Giorgia Guglielmi, "First CRISPR Test for the Coronavirus Approved in the United States," *Nature*, 8 May 2020, <https://www.nature.com/>.
41. I thank Bernard Possidente for suggesting this useful analogy.
42. Cunningham and Geis, "National Strategy for Synthetic Biology," 52–53.
43. Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297, no. 5583 (August 2002): 1016–18, <https://science.sciencemag.org/>.
44. George Church and Ed Regis, *Regenesis: How Synthetic Biology Will Reinvent Nature and Ourselves* (New York: Basic Books, 2014), 2.
45. Church and Regis, 4.
46. Eric Young and Hal Alper, "Synthetic Biology: Tools to Design, Build, and Optimize Cellular Processes," *Journal of Biomedicine and Biotechnology*, 2010, 1, <https://doi.org/10.1155/2010/130781>. For example, see Deborah A. Weighill et al., "Multi-Phenotype Association Decomposition: Unraveling Complex Gene-Phenotype Relationships," *Frontiers in Genetics* 10 (2019), <https://doi.org/10.3389/fgene.2019.00417>. For a review of possible options, see Nadia Solovieff et al., "Pleiotropy in Complex Traits: Challenges and Strategies," *Nature Reviews Genetics* 14, no. 7 (July 2013): 483–95, <https://doi.org/10.1038/nrg3461>.
47. Peter Kornbluh, ed., "Oscars: 'Bridge of Spies,' The Sequel," Briefing Book 542 (Washington, DC: National Security Archives, 26 February 2016), <https://nsarchive.gwu.edu/>.
48. William Rosenau, "Aum Shinrikyo's Biological Weapons Program: Why Did It Fail?," *Studies in Conflict & Terrorism* 24, no. 4 (2001): 296–97, <https://doi.org/10.1080/10576100120887>.
49. Rosenau, 296–97.
50. Edmond Hooker, "Biological Warfare," *emedicinehealth*, 10 January 2019, <https://www.emedicinehealth.com/>.
51. Ben Ouaghrham-Gormley, *Barriers to Bioweapons*.
52. Catherine Jefferson, Filippa Lentzos, and Claire Marris, "Synthetic Biology and Biosecurity: Challenging the 'Myths,'" *Frontiers in Public Health* 2, article 115 (August 2014): 10, <https://doi.org/10.3389/fpubh.2014.00115>.
53. Yaojun Tong et al., "Highly Efficient DSB-Free Base Editing for Streptomyces with CRISPR-BEST," *Proceedings of the National Academy of Sciences of the United States of America* 116, no. 41 (8 October 2019): 20366–75, <https://doi.org/10.1073/pnas.1913493116>.
54. Sean C. Sleight and Herbert M. Sauro, "Design and Construction of a Prototype CMY (Cyan-Magenta-Yellow) Genetic Circuit as a Mutational Readout Device to

Measure Evolutionary Stability Dynamics and Determine Design Principles for Robust Synthetic Systems,” *Artificial Life* 13 (2012): 486, <https://direct.mit.edu/>.

55. Yen-Hsiang Wang, Kathy Y. Wei, and Christina D. Smolke, “Synthetic Biology: Advancing the Design of Diverse Genetic Systems,” *Annual Review of Chemical and Biomolecular Engineering* 4 (2013): 20, <https://doi.org/10.1146/annurev-chembioeng-061312-103351>.

56. A single nanometer is about one half the width of a DNA molecule.

57. NATO, *NATO 2020: Assured Security; Dynamic Engagement – Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO* (Brussels: NATO Public Diplomacy Division, 17 May 2010), 15, <https://www.nato.int/>.

58. Margaret E. Kosal, “The Security Implications of Nanotechnology,” *Bulletin of the Atomic Scientists* 66, no. 4 (July–August 2010): 63, <https://doi.org/10.2968/066004006>.

59. “Experts Warn of New Weapons through Nanotechnology,” *Nuclear Threat Initiative*, 24 May 2005, <https://www.nti.org/>.

60. Evan J. Wallach, “A Tiny Problem with Huge Implications – Nanotech Agents as Enablers or Substitutes for Banned Chemical Weapons: Is a New Treaty Needed?,” *Fordham International Law Journal* 33, no. 3 (2009): 862, <https://ir.lawnet.fordham.edu/>.

61. Jeff Daniels, “Mini-Nukes and Mosquito-Like Robot Weapons Being Primed for Future Warfare,” *CNBC*, 17 March 2017, <https://www.cnn.com/>.

62. Nikolay Kornienko et al., “Interfacing Nature’s Catalytic Machinery with Synthetic Materials for Semi-Artificial Photosynthesis,” *Nature Nanotechnology* 13 (October 2018): 890–99, <https://doi.org/10.1038/s41565-018-0251-7>.

63. Carl A. Larson, “Ethnic Weapons,” *Military Review* 50, no. 11 (November 1970): 4, <https://www.armyupress.army.mil/>.

64. British Medical Association, *Biotechnology, Weapons and Humanity* (Australia: Harwood Academic Publishers, 1999), 63.

65. Pardis C. Sabeti, “Natural Selection: Uncovering Mechanisms of Evolutionary Adaptation to Infectious Disease,” *Nature Education* 1, no. 1 (2008): 13, <https://www.nature.com/>.

66. Sabeti, 13.

67. British Medical Association, *Biotechnology, Weapons and Humanity*, xviii.

68. Martchenko et al., “Human Genetic Variation Altering Anthrax Toxin Sensitivity,” *Proceedings of the National Academy of Sciences* 109, no. 8 (2011): 2972–77, <https://doi.org/10.1073/pnas.1121006109>.

69. British Medical Association, *Biotechnology, Weapons and Humanity*, 64.

70. Christopher Lane, “Personalized Genomics, Data-Hoarding, and Drug Companies,” *Psychology Today*, 14 January 2015.

71. Joseph D. Kernan and James N. Stewart, Office of the Secretary of Defense, Memorandum, Subject: Direct-to-Consumer Genetic Testing Advisory for Military Members, 20 December 2019.

72. Sui-Lee Wee and Paul Mozur, “China Uses DNA to Map Faces, with Help from the West,” *New York Times*, 3 December 2019, <https://www.psychologytoday.com/>.

73. Wee and Mozur.

74. Interview of Yves Moreau by Scott Simon, “Uighurs and Genetic Surveillance in China,” NPR, 7 December 2019, <https://www.npr.org/>.

75. Andrew Goliszek, *In the Name of Science: A History of Secret Programs, Medical Research, and Human Experimentation* (New York: St. Martin’s Press, 2003), 261.



76. "Gene Drives," SciLine, American Association for the Advancement of Science, 18 April 2018, <https://www.sciline.org/>.
77. NASEM, *Biodefense in the Age of Synthetic Biology*, 4.
78. Nuclear Threat Initiative, "U.S. Scientists Warn CIA of New 'Designer' Biological Agents," 17 November 2003, <https://www.nti.org/>.
79. Francisco Galamas, "Biological Weapons, Nuclear Weapons and Deterrence: The Biotechnology Revolution," *Comparative Strategy* 27, no. 4 (2008): 320–321, <https://doi.org/10.1080/01495930802358364>.
80. Michael J. Ainscough, "Next Generation Bioweapons: Genetic Engineering and Biological Warfare," in *The Gathering Biological Warfare Storm*, eds. Jim A. Davis and Barry R. Schneider (Westport, CT: Praeger, 2004), 180, <https://www.nti.org/>.
81. NASEM, *Biodefense in the Age of Synthetic Biology*, 74.
82. Gregory Koblentz, "Pathogens as Weapons: The International Security Implications of Biological Warfare," *International Security* 28, no. 3 (Winter 2003/04): 84, <https://www.belfercenter.org/>.
83. Max Brooks, "The Next Pandemic Might Not Be Natural," *Foreign Policy*, 20 April 2020, <https://foreignpolicy.com/>.
84. John Haltiwanger, "The US and China Are on the Brink of a New Cold War That Could Devastate the Global Economy," *Business Insider Australia*, 13 May 2020, <https://www.businessinsider.com/>; and Westcott and Jiang, "Chinese Diplomat Promotes Conspiracy Theory."
85. Borger, "Mike Pompeo."
86. Shayan Sardarizadeh and Olga Robinson, "Coronavirus: U.S. and China Trade Conspiracy Theories," BBC, 26 April 2020, <https://www.bbc.com/>.
87. Cunningham and Geis, "National Strategy for Synthetic Biology," 50.
88. Quoted in Brooks, "Next Pandemic Might Not Be Natural."
89. Frank Jordans, "Clinton Warns of Bioweapon Threat from Gene Tech," NBC News, 7 December 2011.
90. Donald J. Trump, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 9, <https://trumpwhitehouse.archives.gov/>.
91. Baumgaertner and Broad, "North Korea's Less-Known Military Threat."
92. Michael J. Selgelid, "Governance of Dual-Use Research: An Ethical Dilemma," *Bulletin of the World Health Organization* 87 (2009): 720–23, <https://www.ncbi.nlm.nih.gov/>.
93. Edgar J. DaSilva, "Biological Warfare, Bioterrorism, Biodefence and the Biological and Toxin Weapons Convention," *Electronic Journal of Biotechnology* 2, no. 3 (December 2019), <http://www.ejbiotechnology.info/>.
94. R. Daniel Bressler and Chris Bakerlee, "'Designer Bugs': How the Next Pandemic Might Come from a Lab," Vox, 6 December 2018, <https://www.vox.com/>.
95. Jan van Aken and Edward Hammond, "Genetic Engineering and Biological Weapons," *EMBO Reports* 4, no. S1 (2003): 57–60, <https://doi.org/10.1038/sj.embor.embor860>.
96. Human Rights Watch, "Attacks on Ghouta: Analysis of Alleged Use of Chemical Weapons in Syria," 10 September 2013, <https://www.hrw.org/>.
97. Brooks, "Next Pandemic Might Not Be Natural."
98. Brendan Rittenhouse Green and Austin Long, "Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition," *International Security* 44, no. 3 (Winter 2019/20): 50, <https://direct.mit.edu/>.

99. Kenneth Waltz, "The Spread of Nuclear Weapons: More May Better," *Adelphi Papers* 171 (London: International Institute for Strategic Studies, 1981), <https://www.mtholyoke.edu/>.
100. Glenn H. Snyder, "Deterrence and Defense," in *The Use of Force: International Politics and Foreign Policy*, eds. Robert J. Art and Kenneth N. Waltz (New York: University Press of America, 1983), 129.
101. Green and Long, "Conceal or Reveal?," 50.
102. Green and Long, 51.
103. Galamas, "Biological Weapons," 317.
104. Ward Wilson, "The Myth of Nuclear Deterrence," *Nonproliferation Review* 15, no. 3 (November 2008): 423, <https://www.nonproliferation.org/>.
105. Charles L. Glaser, "Political Consequences of Military Strategy: Expanding and Refining the Spiral and Deterrence Models," *World Politics* 44, no. 4 (July 1992): 501, <https://www.jstor.org/>.
106. As Stephen Rosen observes, while "historical episodes will mark most clearly the men and women who lived through them," young individuals are marked the most by events. This is because "old people have many memories of the past, but new short-term memories are not formed as easily as when young. Young people will not be generally afraid, but when they are afraid, they will react very strongly, and so they will be capable of forming new memories easily." Stephen Peter Rosen, *War and Human Nature* (Princeton, NJ: Princeton University Press, 2005), 52.
107. Kenneth Waltz, "Why Iran Should Get the Bomb," *Foreign Affairs* 91, no. 4 (July/August 2012): 2–5, <https://www.foreignaffairs.com/>.
108. Andrew H. Kydd and Barbara F. Walter, "The Strategies of Terrorism," *International Security* 31, no. 1 (Summer 2006): 58, <https://www.belfercenter.org/>.
109. Kydd and Walter, 51.
110. Kydd and Walter, 51.
111. Kydd and Walter, 60, 67, 77.
112. Galamas, "Biological Weapons," 317.
113. Jennifer A. Doudna and Samuel H. Sternberg, *A Crack in Creation: Gene Editing and the Unthinkable Power to Control Evolution* (Boston: Houghton Mifflin Harcourt, 2017), 199.
114. Thomas Lecaque, "The Apocalyptic Myth That Helps Explain Evangelical Support for Trump," *Washington Post*, 26 November 2019, <https://www.washingtonpost.com/>.
115. Leon Aron, "Kingdom Come: Millenarianism's Deadly Allure, from Lenin to ISIS," *New York Review of Books*, 13 February 2018 <https://www.nybooks.com/>.
116. William Lanouette, *Genius in the Shadows: A Biography of Leo Szilard, the Man Behind the Bomb* (New York: Skyhorse Publishing, 2013), 205.
117. Lauren McCain, "Informing Technology Policy Decisions: The US Human Genome Project's Ethical, Legal, and Social Implications Programs as a Critical Case," *Technology in Society* 24, nos. 1–2 (2002): 112, <https://www.sciencedirect.com/>.
118. McCain, "Informing Technology Policy Decisions."
119. National Human Genome Research Institute, "Ethical, Legal and Social Issues in Genomic Medicine," accessed July 2021, <https://www.genome.gov/>.
120. For example, see testimonies at *The Science and Ethics of Genetically Engineered Human DNA, Hearing before the Subcommittee on Research and Technology, Committee on Science, Space, and Technology, House of Representatives*, 114th Cong., 1st sess., 16 June

2015 (Washington, DC: Government Printing Office, 2016), <https://www.govinfo.gov/>. While all of the participants acknowledged that gene editing raises important “ethical” considerations and called for regulations, none directly tackled its national and international security implications.

121. Guillemin, *Biological Weapons*, viii.

122. Aken and Hammond, “Genetic Engineering and Biological Weapons,” 59.

123. Theodor Rosebury, *Peace or Pestilence: Biological Warfare and How to Avoid It* (New York: Whittlesey House, 1949), 183.

124. Rosebury, 178.

125. Rosebury, 116.

126. Mazanec, *Evolution of Cyber War*, 6.

127. Mazanec, 2.

128. Mazanec, 6–7.

129. Guillemin, *Biological Weapons*, 204.

130. Central Intelligence Agency (CIA), “The Darker Bioweapons Future,” 3 November 2003, 2, <https://fas.org/>.

131. CIA, 2.

132. National Research Council of the National Academies, Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *Biotechnology Research in an Age of Terrorism: Confronting the Dual-Use Dilemma* (Washington, DC: The National Academies Press, 2003), <https://www.nap.edu/>.

133. Author’s interviews at Bio-IT World Conference, Boston, MA, 15–17 May 2018.

134. National Research Council of the National Academies, *Biotechnology Research in an Age of Terrorism*, vii.

135. Michael Specter, “A Life of Its Own: Where Will Synthetic Biology Lead Us?,” *New Yorker*, 28 September 2009, <https://www.newyorker.com/>.

136. Specter.

137. Amanda Kobokovich et al., “Strengthening Security for Gene Synthesis: Recommendations for Governance,” *Health Security* 17, no. 6 (2019): 427, <https://doi.org/10.1089/hs.2019.0110>; and Gigi Kwik Gronvall, “Safety, Security, and Serving the Public Interest in Synthetic Biology,” *Journal of Industrial Microbiology and Biotechnology* 45, no. 7 (July 2018): 463, <https://doi.org/10.1007/s10295-018-2026-4>.

138. Vaughan Turekian et al., *Building a Smart Partnership for the Fourth Industrial Revolution* (Washington, DC: Atlantic Council, April 2018), 1, <https://www.atlanticcouncil.org/>; and Gigi Kwik Gronvall et al., *US-India Strategic Dialogue on Biosecurity: Report on the Sixth Dialogue Session* (Baltimore: Johns Hopkins Center for Health Security, June 2019), <https://www.centerforhealthsecurity.org/>.

139. Gigi Kwik Gronvall, “Chapter 3: Ensuring Biosafety and Security,” in Turekian et al., *Building a Smart Partnership for the Fourth Industrial Revolution*, 30.

140. NASEM, *Biodefense in the Age of Synthetic Biology*, 126.

141. Cunningham and Geis, “National Strategy for Synthetic Biology,” 60–71.

142. Cunningham and Geis, 50, 71.

# An Overlooked Aid to Arms Control: US Nuclear Modernization

MATTHEW R. COSTLOW

## Abstract

As the United States seeks to expand its nuclear arms control efforts in scope, incorporating all nuclear weapon types, and in numbers of partners beyond Russia (i.e., China), US officials must examine what policies might enable the best arms control outcome. An important but understated factor in helping the United States reach acceptable arms control agreements is its nuclear modernization program. US nuclear modernization efforts have been a major inducement in the past for the Soviet Union to agree to come to the negotiating table. Additionally, US nuclear modernization programs have provided its diplomats additional options for discovering areas of agreement with the Soviets. Finally, US nuclear modernization programs can further incentivize states to adhere to their commitments in an arms control agreement because they face a credible threat of counteraction should they choose to cheat. Alternative arms control approaches that emphasize unilateral US nuclear reductions to induce nuclear arms control agreements are unlikely to be successful.

\*\*\*\*\*

## Introduction

*Our experience has shown us only too clearly that weakness in arms strength means weakness in diplomacy.*

—Neville Chamberlain, 1938

Military forces and diplomacy are both tools that advance US national interests and work best when used together. Military forces add credibility to US diplomats at the negotiating table. Diplomacy promotes deterrent messages by reaching the intended audiences and reducing the chances for miscalculation or misperception. Thus, when states seek to enter arms control agreements, as the United States has made clear it seeks to do, they must consider the military forces and the diplomatic positions needed to retain and increase their security.

The Biden administration has extended the New Strategic Arms Reduction Treaty (New START) for an additional five years. However, it has also signaled that it hopes to discuss further strategic nuclear arms reductions or caps with Russia while perhaps persuading China to join in discussions. It is an open question as to how willing Russian and Chinese leaders will be to consider US nuclear arms control proposals, but Moscow and Beijing will almost certainly factor US nuclear modernization plans into their response. Thus, the Biden administration must consider the effects of the ongoing US nuclear modernization program on its arms control prospects and priorities. To bring some clarity to this important but underappreciated aspect of defense strategy, this article explains the benefits a modernized US nuclear force brings to US nuclear arms control prospects. Conversely, it also examines how a failure to modernize US nuclear weapons, or to take unilateral efforts to significantly reduce them, may harm prospects for arms control that support US national security objectives.

### **Political Context of Nuclear Arms Control and Modernization**

The great Prussian military strategist Carl von Clausewitz taught in his classic book *On War* that war is the continuation of politics by other means. By extension, so too is nuclear arms control the continuation of politics by diplomatic means. Just as war is not waged for its own sake, arms control cannot be negotiated for the sake of an agreement—it must be driven by political leaders with political goals. “Political” here is not meant in a partisan way but as the origination of goals that can exist only in the realm of governing a state versus a focus on operational or tactical military objectives. Exactly what form a nuclear arms control agreement must take that advances US, allied, and partner security is left open for definition by the president and the negotiating team—whether they seek an agreement on nuclear weapons that caps them, reduces them, allows their expansion under certain constraints, or some other combination. In any case, the point remains: political goals determine ends, and nuclear arms control negotiations are one of the means. This article is not concerned with the ends per se (be they reductions, caps, transparency, etc.). Rather, it is focused on how the means of US nuclear modernization and US nuclear arms control negotiations interact—specifically, how the former can strengthen the latter.

One must note that the United States is not modernizing its nuclear weapons for the sake of having new weapons. Nor is it modernizing its nuclear arsenal for the primary reason of improving the prospects of nu-

clear arms control. Instead US nuclear weapons serve political goals such as providing deterrence against attack and supporting the security of allies and partners. Exactly what forms this modernization take is up to the president and Congress. The parallel US efforts to modernize its nuclear arsenal and pursue nuclear arms control intersect around the question of how one effort should affect the other. Should the United States, as John F. Kennedy stated, “depend on the strength of armaments—to enable us to bargain for disarmament?”<sup>1</sup> Or should the United States reduce its planned nuclear modernization to better the chances of enabling an arms control agreement?

### **US Nuclear Modernization as an Aid to Arms Control Success**

While a successful nuclear arms control agreement can only be identified via politically defined metrics (e.g., decreased destructive power, fewer missiles, increased transparency, etc.), it is still possible to describe how a modernized US nuclear arsenal may make success more likely—even without knowing the particular US end goals that would define “success.” The key concept in this regard is leverage. A clear assumption of US government officials, going back to the Cold War, is that states like Russia or China will not make major nuclear reductions unilaterally and instead need an incentive to do so.<sup>2</sup> US nuclear modernization, according to current US officials and policies, is the main source of leverage to incentivize Russian and Chinese officials.

There are three reasons why US nuclear modernization can increase the chances for nuclear arms control success and, by extension, US security. First, US nuclear modernization can influence states like Russia and China to participate in negotiations for fear of a more capable US nuclear arsenal. Second, once the United States has one or more negotiating partners, a modernized US nuclear arsenal provides more counters and offsets to adversary systems in either capability, number, or age—making a beneficial agreement more likely. Third, once an agreement is reached, a modernized or modernizing US nuclear arsenal can create additional incentives for other states to refrain from significant cheating because of the risk of a relatively swift US counter enabled by “warm” weapons production lines. Each of these reasons is examined below.

### ***An Incentive for Others to Participate in Negotiations***

Perhaps the most widely discussed perceived benefit of US nuclear modernization related to nuclear arms control is its purported ability to pressure another state to participate in negotiations. That is, another state may fear that US nuclear modernization would lead to a more capable US nuclear arsenal and, should arms control agreements expire, a larger arsenal as well. This belief likely lies behind the 2018 *Nuclear Posture Review's* statement that “ensuring our nuclear deterrent remains strong will provide the best opportunity for convincing other nuclear powers to engage in meaningful arms control initiatives.”<sup>3</sup> Indeed, a myriad of former senior Department of Defense and Department of State officials, including several ambassadors and diplomats, have espoused this view in the atomic age.

For example, US secretary of state George Shultz, looking back on the arms control environment of the 1980s, stated, “But if the West did not deploy Pershing II and cruise missiles, there would be no incentive for the Soviets to negotiate seriously for nuclear weapons reductions.”<sup>4</sup> Longtime arms control negotiator Ambassador Edward Rowny made a similar observation in 1984 after the Soviet Union’s arms control delegation walked away from the Intermediate-Range Nuclear Forces (INF) and START negotiations. He asserted, “The best way to encourage the Soviets to return to the table is to continue current programs designed to ensure our common defense, while simultaneously reiterating our readiness to resume negotiations toward balanced and verifiable agreements. One-sided cuts in our defense programs or failure to uphold alliance commitments would only reward the Soviets for their intransigence and make a return to the negotiating table less likely.”<sup>5</sup> Four years earlier, in 1980, Richard Burt, who later became an ambassador, likewise stated, “The Soviets are concerned about the US strategic modernization program. Going forward with the US modernization program gives them a strong incentive to negotiate seriously in START.”<sup>6</sup>

These assertions by US officials appear to have strong support in the historical record, especially from testimony by former Soviet arms control officials. In a comprehensive review of Soviet arms control decision-making, Aleksandr G. Savelyev, and Nikolay N. Detinov found that “the American defense spending increase, SDI [Strategic Defense Initiative], and other defense programs greatly troubled the Soviet leadership, which now [1985] concluded that appropriate Soviet-American agreements were the only way out.”<sup>7</sup> Retired general Viktor Starodubov, the chief Strategic Arms Limitation Talks II (SALT II) adviser to the Soviet General Staff and official member of the SALT II Soviet delegation, stated post-Cold War,

"I think it was logical for both countries that at some point the leaders . . . [concluded] that it was impossible to continue increasing armaments any longer." He noted, "We in the Soviet Union understood it too, but we also understood that for us trying to catch up to the United States would be too costly, too difficult, in terms of the economy and so forth. That is why we . . . [determined] the need for negotiating limits on, and later reducing, strategic weapons."<sup>8</sup> The change in Soviet leadership to Mikhail Gorbachev, with his focus on economic and military reforms, largely contributed to Soviet participation in nuclear arms control discussions with the United States. However, Soviet officials also recognized that US nuclear modernization programs could continue unabated. The Soviet Union would then be forced to either reduce its nuclear arms unilaterally due to funding or continue producing weapons at an economically unsustainable rate with unknown, potentially disastrous consequences.

Thus, there appears to be historical justification for the belief that if states like Russia perceive that the United States was willing and able to modernize its nuclear arsenal, they are more likely to seriously consider joining nuclear arms control negotiations.

### ***Comparable Arsenals Increase Chances of Agreement***

Once the United States and others have agreed to negotiate, a modernized or modernizing US nuclear arsenal will likely benefit the US negotiating position by providing more options for US negotiators to parry the other side's proposals. In short, if the United States is extensively constrained—for instance, in the size, capability, or age of its arsenal—there will be fewer scenarios where negotiators can make like-to-like weapon system comparisons and find a balance agreeable to all sides. As in the case of the INF Treaty, the United States could counter Soviet intermediate-range ballistic missiles with its in-kind systems. These comparable systems allowed like-for-like exchanges while also serving deterrence and assurance roles.

US officials have often stated the same idea. As Gen Paul Selva, then vice chairman of the Joint Chiefs of Staff, testified to the US Congress, "The places we [the United States] have had success in negotiating types and classes of weapons out of adversary nuclear arsenals in our strategic arms reductions talks [have] been when we possess a similar capability that poses a tactical, operational, and strategic problem for our adversaries."<sup>9</sup> A historical example of US systems posing a "problem" for an opponent was the US Safeguard antiballistic missile (ABM) system. In this instance, US ABM technology was well advanced beyond that of the Soviets, bring-



ing them to the negotiating table and providing an incentive to agree once negotiations had begun. Ambassador Burt remarked, “Moscow did agree to forgo the heavy deployment of ballistic missile defenses. But the United States, on the verge of deploying the Safeguard system—a much more proficient ABM than the Soviets possessed at the time—possessed considerable leverage in negotiations that led to the 1972 treaty.”<sup>10</sup>

From the Russian perspective, perceived gaps in capability between systems appear to affect the willingness to negotiate seriously about further reductions. Sergei Ivanov, then–presidential chief of staff for Vladimir Putin, stated in 2013, “When I hear our American partners say: ‘Let’s reduce something else,’ I would like to say to them: ‘Excuse me, but what we have is relatively new.’ They [the U.S.] have not conducted any upgrades for a long time. They still use Trident [missiles].”<sup>11</sup> President Putin even claimed at the end of 2019 that “the share of modern weapons in the [Russian] nuclear triad has reached 82 percent.”<sup>12</sup> Since most of the newest US nuclear systems under the current modernization program will not be deployed until the late 2020s and early 2030s, states like Russia may have less incentive, at least in the near term, to find like-for-like comparisons with the US arsenal. This is the case unless, of course, Russian officials view the US commitment (both fiscal and political) to its modernization program to be nearly unquestionable.

It may be reasonable, therefore, for US officials to consider these Russian perceptions about the value of characteristics in their respective nuclear forces—like age, capability, and number—when planning for nuclear modernization and the possibility of nuclear arms control negotiations in the future. As Assistant Secretary of Defense Robert Scher stated at the time, the DOD plans for a US nuclear arsenal that, in part, “retains leverage for future arms control agreements.”<sup>13</sup> Such planning may pay off when negotiating a nuclear arms control agreement by permitting US diplomats several otherwise unavailable negotiating options. Certainly, the more options the United States has, the more likely it may reach an agreement acceptable to a state like Russia and to the security interests of the United States. Should an arms control agreement, however, not be possible or prudent, modernized US nuclear weapons will retain their value for their traditional roles nevertheless. In essence, a limited US nuclear arsenal diminishes the leverage of the US, constrains the number of options to achieve its political goals, and increases the risk of it being forced to make unnecessary concessions.

To be clear, the United States should pursue nuclear modernization on its own merits for the traditional roles of enhancing deterrence, strength-

ening assurance, achieving US objectives should deterrence fail, and hedging against an uncertain future. The useful byproduct of this modernization can be better possibilities for arms control that are in the US national interest. Yet a modernized US nuclear arsenal will not, on its own, guarantee an equal or advantageous balance of forces as a result of an arms control agreement. Nevertheless, it could increase the chance of such an outcome if other factors such as political will and domestic support remain equal.

### ***A Modernizing US Nuclear Arsenal Could Help Discourage Arms Control Violations***

Finally, a modernized or modernizing US nuclear arsenal could boost the chances for arms control success by deterring others' arms control violations. The prospect of a relatively rapid US response in kind (e.g., production of more or new missiles), or even a disproportionate response that far outweighs any expected benefit of the violation, can help deter violations in the first place. It appears that when the Soviet Union and Russia have violated arms control treaties in the past, they have sought a military advantage from the violation. To deter such violations, therefore, the United States should present the possibility that not only will the violation be detected but that the violator will become less secure because of the US military response.

This response could take the form of increased production or production rate of nuclear weapons of the same type as the violating weapon. Or the prospective response might be the increased production or production rate of nuclear weapon types that the violator perceives as the most threatening. These options become substantially more realistic—and perhaps credible to the other side—as the United States maintains warm production lines amid its nuclear modernization effort. US political leaders may not decide to use these options when responding to a violation, but having them available as a convenient byproduct of US nuclear modernization may improve the chances of deterring a violation in the first place, especially when combined with other potential diplomatic and military efforts.

While historical examples of this dynamic are thin, US officials have consistently pointed out the possibility of the deterring effect of weapons production lines already operating. In his article “After Detection—What?,” Fred Iklé stated, “In entering into an arms-control agreement, we must know not only that we are technically capable of detecting a violation but also that we or the rest of the world will be politically, legally and militarily in a position to react effectively if a violation is discovered.”<sup>14</sup> Further, “A potential violator of an arms-control agreement will not be

deterred simply by the risk that his action may be discovered. What will deter him will be the fear that what he gains from the violation will be outweighed by the loss he may suffer from the victim's reaction to it."<sup>15</sup> Over 20 years later, US defense official and strategist Walter Slocombe wrote, "Indeed, the knowledge that the United States could respond to detected violations in ways that would prevent any Soviet gain is at least as important a deterrent to Soviet cheating as the knowledge that the United States would detect the violation."<sup>16</sup>

In the most recent major Russian arms control violation, Russia's possession of the 9M729 ground-launched cruise missile (GLCM) was a transgression under the INF Treaty that the United States could not immediately counter militarily in a like-for-like manner.<sup>17</sup> Since the United States had remained compliant with the INF Treaty, it had no GLCM manufacturing capability at the time of the Russian violation. Consequently, the US lack of a like-for-like response meant that it had no equal deterrent presenting a threat of decreased Russian security.

Certainly, the US ability to increase the production or production rate of nuclear weapons in response to a nuclear arms control violation is no panacea and must work in conjunction with other factors such as political will, diplomatic efforts, and domestic support to be effective. But US nuclear modernization and its warm production lines offer another incentive to others to comply with their nuclear arms control commitments. The prospect of a US capability to detect and respond quickly with increased nuclear weapons production to a major nuclear arms control violation also gives US officials another tool of leverage to bring the violator back into compliance—as would likely be the goal. Critics may contend that another response such as increasing conventional weapons production or deployments would still be credible. It would be unlikely, however, to convince the violator to come back into compliance in the same way that a like-for-like increase in nuclear weapons would.

### **Objection to the Benefits of a Modernized US Nuclear Arsenal for Arms Control**

Despite the benefits described above of a modernized US nuclear arsenal for its arms control objectives, some proponents of a more limited US nuclear arsenal (perhaps only partially modernized) also have their arguments. They contend that the leverage of increasing the numbers and/or capability of US nuclear weapons is unnecessary to achieve arms control objectives. The following examines their claim.

## ***US Nuclear Reductions Could Induce Russian or Chinese Arms Control Cooperation***

Advocates for US unilateral nuclear reductions commonly posit that this avenue could lead to arms control benefits without the expensive bill for US nuclear modernization or at least only a partial bill. For instance, Kingston Reif and Alicia Sanders-Zakre propose that “a [US] decision to reduce to 1,000 deployed strategic warheads would put the United States in a stronger position to pressure Russia to rethink some of its expensive nuclear recapitalization projects and reduce its deployed strategic nuclear warheads. Perhaps more intriguingly, a US willingness to reduce its arsenal could lead China to take a less passive approach to nuclear disarmament and more openly discuss the size, composition, and operations of its nuclear forces.”<sup>18</sup> Or as a Deep Cuts Commission report recently stated, “Even if Russia is reluctant to join the United States in building down, a US reduction would put Russia on the defensive and force Moscow to explain to a critical international community why it needs to maintain a larger deployed nuclear arsenal than the United States.”<sup>19</sup> Although anything is possible, the history of nuclear arms control with the Soviet Union and Russia and the complete lack of nuclear arms control with China undermine this claim.

If it is true that Russia and China will respond positively to reductions in either the size or capability of the US nuclear arsenal, then one would expect to see such action-reaction dynamics in the past. However, there is little such evidence. A few examples demonstrate this. Post-Cold War, the United States minimized its nonstrategic nuclear arsenal, and while Russia reduced its nonstrategic nuclear arsenal, it did not go nearly as far as the United States. Instead, it is now well into a modernization program and projected to substantially grow its nonstrategic nuclear arsenal.<sup>20</sup> There is also no indication that Russia’s modernization program was influenced in any positive way by the US decision to unilaterally reduce its forces by retiring the nuclear-armed Tomahawk Land Attack Missile (TLAM-N) in 2010. While the United States has steadily reduced the number of its nuclear weapons, China has thus far refused to engage in a meaningful nuclear arms control dialogue. If US nuclear reductions could spur additional arms control benefits, one would expect to see much greater arms control cooperation today.

Analysts must ask the question then, Why has it become standard practice in the arms control community to recommend that the United States engage in unilateral reductions for the sake of a better arms control environment? This question is especially puzzling when there is no good ex-

ample of success in adopting that strategy. On the other hand, the approach of leveraging a capable, credible US nuclear arsenal has proven successful. As former secretary of defense Harold Brown observed, “Appropriate restraint in our programs and actions is still warranted. But there is no evidence from history that unilateral reductions in our posture will produce Soviet reciprocity. An important function of our various arms control negotiations is precisely to achieve equitable and verifiable mutual reductions without undue risk. To substitute unilateral reductions for these negotiations does not seem to be either prudent or realistic.”<sup>21</sup> Calls for unilateral US nuclear reductions thus appear self-defeating because, if implemented, they would reduce chances for future arms control agreements by limiting or eliminating necessary US leverage.

If the United States were to, for example, eliminate its intercontinental ballistic missile (ICBM) force, past experience indicates that it would then have no leverage over Russia and China to do the same. They would likely pocket the concession and hold out for more since withholding from an agreement netted them that much. Even worse, the US arsenal would then have no credible counters or offsets comparable to the Russian or Chinese nuclear arsenal in type, making further opportunities for nuclear arms control agreements more difficult.

What is the ultimate reason then why leverage in the form of a modernized US nuclear arsenal is to be preferred over unilateral US nuclear reductions in maximizing the benefits of arms control? The answer comes down to differences in national goals. While many US arms control proponents are seeking ways to solve the problem of nuclear war, the leaderships of Russia and China are pursuing ways to increase their countries’ security at the expense of the United States. Ambassador Ed Rowny, who had decades of experience in negotiations with the Soviets, assessed that “the Soviets simply do not negotiate in a spirit of problem-solving. Those of us who have negotiated with the Soviets do not expect them to. We have come to understand that, whereas we would like to work out solutions, the Soviets would rather compete.”<sup>22</sup> Equally experienced, Ambassador Paul Nitze explained why the Soviet Union saw little need for urgency on significant nuclear arms reductions in the 1970s during the Strategic Arms Limitation Talks:

We [the United States] could not get the Soviets to agree to tight limitations on offensive arms comparable to those applied to ABM systems or reductions in such arms. Indeed, limiting defenses did not appear to have any effect on the Soviet offensive buildup. Part of the problem was that the Soviets were doing well concerning offensive systems. We had ceased

building new ICBMs, ballistic missile submarines, and heavy bombers some years earlier; we were improving them through qualitative changes. The Soviet Union was actively deploying large numbers and new types of ICBMs and SLBMs. Momentum thus tended to favor the Soviets; they saw no reason to sign a piece of paper that would cause them to forgo that advantage.<sup>23</sup>

Leverage matters when negotiating with other states on nuclear arms control measures. Former under secretary of defense for policy James Miller lent credence to the US need for leverage, noting, “When the Obama administration asked the Russians, ‘Ok, we want to talk about tactical nuclear weapons. We are open to talking about them as an entity by themselves or to roll them together with strategic for conversation,’ the answer that we got was *nyet*. And it was, ‘. . . You Americans don’t have anything going on in this arena. Why should we negotiate?’”<sup>24</sup> Future nuclear arms control prospects hinge not only on the negotiating leverage provided by a modernized US nuclear arsenal but also on the recognition that leverage itself is most likely to be the superior negotiation tactic over unilateral concessions.

## Conclusion

Arms control is one of many tools designed to achieve and protect US national interests, as is the US nuclear arsenal. A modernized US nuclear arsenal is only a partial solution to the inherently political problem of achieving satisfactory arms control agreements with other states—should that be the goal. By itself, US nuclear modernization will not guarantee that a plausible arms control agreement will materialize. However, it is the most likely technical catalyst to produce the conditions favorable to arms control in the US national interest.

The United States should prioritize its nuclear modernization efforts for the traditional roles of deterring adversaries, assuring allies and partners, achieving US objectives should deterrence fail, and hedging against an uncertain future. Policy makers should realize, however, that particular benefits for the arms control process may result from a modernized US nuclear arsenal. First, it may increase the chance that others will join the negotiations for fear of a more capable US nuclear arsenal. Second, it may increase the chance of favorable counters and offsets between countries’ nuclear arsenals, making an agreement on comparable systems more plausible. Third, it may increase the chance of deterring serious arms control violations by credibly threatening a proportionate or disproportionate nuclear buildup as a response. History indicates that the alternative

strategy of unilateral US nuclear reductions would not provide the same benefits and make significant and beneficial arms control less likely for the United States—not to mention the damaging effects on accomplishing the traditional missions of nuclear weapons.

The US nuclear arsenal's primary mission—and the main goal of its modernization—should always be contributing to the defense of the United States, its allies, and partners. If political leaders seek a nuclear arms control agreement with other states, US nuclear modernization efforts—besides contributing to US security—can increase the chance of successful nuclear arms control. As Ambassador Burt affirmed, “Arms control will only prosper if the Soviet Union has the incentive to negotiate; what is required to bring this about is a sound military foundation on our part. . . . Arms control has the potential to buttress our security and deterrence; it cannot take the place of our collective efforts to do the same.”<sup>25</sup> Ultimately, only US political leaders can decide whether and what kind of nuclear arms control will advance US national security. But when they do, a modernized US nuclear arsenal will likely increase the chance they can achieve those goals—while strengthening deterrence against the worst outcomes should those efforts fail. **SSQ**

#### **Matthew R. Costlow**

Matthew Costlow is a PhD candidate at George Mason University and a senior analyst at the National Institute for Public Policy. He was formerly a special assistant in the Office of Nuclear and Missile Defense Policy, US Department of Defense.

#### **Notes**

1. John F. Kennedy, “Remarks of Senator John F. Kennedy in the United States Senate, National Defense, Monday, February 29, 1960,” JFK Library, <https://www.jfklibrary.org/>.
2. In addition to the US arms control negotiators quoted in the article, see, for example, Department of Defense, *National Security Strategy of Realistic Deterrence: Secretary of Defense Melvin R. Laird's Annual Defense Department Report FY 1973* (Washington, D.C.: Department of Defense, 1972), 77, <https://history.defense.gov/>; James R. Schlesinger, *Annual Defense Department Report FY 1976 and 1977* (Washington, D.C.: Department of Defense, 1975), II-10–II-11, <https://history.defense.gov/>; and Donald H. Rumsfeld, *Annual Defense Department Report, 1977* (Washington, D.C.: Department of Defense, 1976), 60, <https://history.defense.gov/>.
3. Department of Defense, *Nuclear Posture Review 2018* (Washington, D.C.: Department of Defense, 2018), III, <https://media.defense.gov/>.
4. George P. Shultz, *Turmoil and Triumph: My Years as Secretary of State* (New York: Charles Scribner's Sons, 1993), 351.
5. Edward L. Rowny, “Nuclear Arms Control and the NATO Alliance,” US Department of State, Current Policy No. 591, 21 June 1984, 1, <https://babel.hathitrust.org/>.

6. Richard E. Burt, "Evolution of the U.S. START Approach," US Department of State, Current Policy No. 436, September 1982, 4, <https://babel.hathitrust.org/>.
7. Aleksandr' G. Savelyev and Nikolay N. Detinov, *The Big Five: Arms Control Decision-Making in the Soviet Union* (Westport, CT: Praeger, 1995), 92.
8. Viktor Starodubov quoted in "SALT II and the Growth of Mistrust: Conference #2 of the Carter-Brezhnev Project," 6–9 May 1994, 35. On file at National Security Archive, George Washington University, <https://nsarchive2.gwu.edu/>.
9. Gen Paul Selva quoted in House, *Military Assessment of Nuclear Deterrence Requirements: Hearing before the Committee on Armed Services*, 115th Cong., 1st sess. (Washington, D.C.: Government Publishing Office, 8 March 2017), <https://www.govinfo.gov/>.
10. Richard Burt, "Reassessing the Strategic Balance," *International Security* 5, no. 1 (Summer 1980): 49.
11. Russia Beyond the Headlines and Interfax, "Russia Not Interested in U.S.-Proposed Arms Reduction – Russian presidential Chief-of-Staff," 5 March 2013, <https://www.rbth.com/>.
12. Vladimir Putin, "Defence Ministry Board Meeting," President of Russia website, 24 December 2019, <http://en.kremlin.ru/>.
13. Statement of Robert Scher, Assistant Secretary of Defense for Strategy, Plans, and Capabilities, before the House Armed Services Subcommittee on Strategic Forces, 2 March 2016, 4, <https://docs.house.gov/>.
14. Fred Charles Iklé, "After Detection – What?," *Foreign Affairs* 39, no. 2 (January 1961): 208, <https://doi.org/10.2307/20029480>.
15. Iklé, 208.
16. Walter B. Slocombe, "Arms Control: Prospects," in *Nuclear Arms: Ethics, Strategy, Politics*, ed. R. James Woolsey (San Francisco: Institute for Contemporary Studies, 1984), 143.
17. Daniel Coats, "Director of National Intelligence Daniel Coats on Russia's Intermediate-Range Nuclear Forces (INF) Treaty Violation," Office of the Director of National Intelligence, 30 November 2018, <https://www.dni.gov/>.
18. Kingston Reif and Alicia Sanders-Zakre, *U.S. Nuclear Excess: Understanding the Costs, Risks, and Alternatives* (Washington, D.C.: Arms Control Association, April 2019), 18, <https://www.armscontrol.org/>.
19. Kingston Reif and Victor Mizin, *A Two-Pronged Approach to Revitalizing U.S.-Russia Arms Control*, Deep Cuts Working Paper no. 10 (Hamburg, GE: Deep Cuts Commission, July 2017), 9, <https://deepcuts.org/>.
20. Robert P. Ashley Jr., "Russian and Chinese Nuclear Modernization Trends," DIA, 29 May 2019, <https://www.dia.mil/>; and Department of Defense, *Nuclear Posture Review 2018*, 53.
21. Harold Brown, *Department of Defense Annual Report, Fiscal Year 1979* (Washington, D.C.: Department of Defense, 1978), 35, <https://history.defense.gov/>.
22. Edward L. Rowny, "U.S. and Soviet Approaches to Arms Control," US Department of State, Current Policy No. 868, 19 September 1986, 2, <https://catalog.hathitrust.org/>. Some may disagree with this statement, indicating that US officials have on occasion viewed arms control as a competition with the Soviet Union. But the overall point remains that, in general, the Soviet Union sought to compete in arms control while the majority of writing in the United States was focused on finding mutually acceptable solutions.



23. Paul H. Nitze, "The Objectives of Arms Control," US Department of State, Current Policy No. 677, 28 March 1985, 14–15, <https://www.cia.gov/>.
24. Jim Miller quoted in "The Logic of American Nuclear Strategy," The Atlantic Council, streamed live on 26 February 2018, minute 52:44–53:19, <https://www.youtube.com/>.
25. Richard E. Burt, "A Critical Juncture for the Atlantic Alliance," US Department of State, Current Policy No. 486, 25 April 1983, 3.

# Strategic Imperative: A Competitive Framework for US-Sino Relations

CAPT MICHAEL P. FERGUSON, USA

## Abstract

Recognizing interstate competition between China and the United States as a strategic priority for the US defense enterprise is one issue that appears to transcend presidential administrations. But despite its merits, this notion of “great power competition”—or “strategic competition” as some prefer to term it—has led many in the foreign policy, defense, and academic communities to question the value of competition as a strategic tool for shaping policies against rogue and revisionist powers like the Chinese Communist Party (CCP). More cooperative approaches, some say, could yield favorable results. While competition and cooperation are not mutually exclusive, analysis of the current strategic environment reflects the former as more of a geopolitical imperative than a policy decision. This study presents evidence that forsaking the conceptual framework of competition could signal a return to toothless engagement policies of the twentieth century, overlook the human rights abuses of competitors, abandon critical allies, and concede global influence and access to regional powers emboldened by decades of US collaboration. Although there is room to debate the nuances of its supporting policies, denying the competitive environment’s existence is ill advised. The United States should build on the existing competitive framework in its future strategic documents if it seeks to prevent the CCP from achieving its clearly expressed, but rarely understood, strategic objectives at the cost of US values and national security interests.

\*\*\*\*\*

*This is what Philip has bought with all his lavish expenditure: that he is at war with you, but you are not at war with him!*

—Demosthenes of Athens, 341 BCE

**A**fter the 2017 publication of Graham Allison’s wildly popular book *Destined for War*, the term “great power competition” has elicited reference to the Peloponnesian Wars and the risk of competition escalating into a conflict between major powers in the twenty-first century.

But the relationship between Athens and Macedonia might be a more suitable historical parallel. Demosthenes issued the above impassioned statement to a rather passive Athenian ecclesia during his Third Philippic speech, the final warning in a series of admonishments designed to promote awareness vis-à-vis the intentions of Alexander the Great's father, King Philip II of Macedon. Powerful as his words were, Athens would lose its independence to Macedonia three years later.<sup>1</sup> Quite plainly, Philip out-competed his Athenian opponents with a series of political maneuverings spread over more than a decade that culminated in the decisive Battle of Chaeronea (338 BCE). This precarious balance between strategic competition and cooperation warrants further reflection in light of US-Sino relations and the now controversial term "great power competition."<sup>2</sup> This article uses the term "strategic competition" as does, for example, the White House's 2021 *Interim National Security Strategic Guidance* document.

Since its official reintroduction to the US national security lexicon in 2017, the strategic framework of interstate competition has faced resistance in terms of both style and substance from numerous foreign policy scholars and defense analysts.<sup>3</sup> This resistance usually consists of two arguments. The first is that "competition" is too aggressive and simplistic a term to drive strategic formulation. The second is that prioritizing competition precludes international cooperation by increasing interstate tensions.<sup>4</sup> Recommended alternative solutions typically amount to advocating for linguistic adjustments to status quo political cooperation in line with the "engagement" policies of Presidents George H. W. Bush and Bill Clinton. These policies will become increasingly problematic as Beijing's leaders face charges of genocide and technological authoritarianism from the Western world.<sup>5</sup> The United States and Canada have issued statements regarding the Chinese Communist Party's (CCP) treatment of its minority Uighur population and the exportation of invasive surveillance platforms to authoritarian states.<sup>6</sup> Curiously, these legitimate and deeply concerning accusations are presented almost parenthetically in much of the sterilized advocacy for a more cooperative approach to US-Sino engagement.<sup>7</sup>

To be taken seriously, any proposal for peaceful cooperation as a guiding foreign policy principle must also recognize the free world's obligation to openly condemn reports of genocide and systematic oppression through diplomatic channels as well as military readiness across the conflict spectrum. The resistance to competition as a strategic guidepost is evidence that many in the US national security enterprise have yet to recognize a problem with how the United States understands and applies competition with China. Similar to the conditions described by Demosthenes above,

the United States will remain in competition with other states whether it chooses to use the word in its strategic documents or not. This reality should not preclude cooperation but serve as a realist playbook that acknowledges and accounts for the inherent limitations of cooperation as a twenty-first-century foreign policy tool. Because Secretary of Defense Lloyd Austin has identified China as the US's pacing threat and therefore primary competitor, this analysis is framed accordingly.<sup>8</sup>

### **To Compete or Not to Compete?**

Georgetown University professor Daniel Nexon wrote recently in *Foreign Affairs* that the vague idea of competition as a strategic means is not specific enough to support the desired ends of US national security policy.<sup>9</sup> His commentary reflects a growing outcry from foreign policy observers—and even some practitioners—that the conceptual framework of competing with other regional or global powers is an ill-conceived means of shaping policy.<sup>10</sup> The arguments vary. Some suggest that the security threat from the CCP is overblown while others highlight the catastrophic nature of a potential conflict between nuclear powers. However, they seem to reach the same conclusion: the United States should tread more carefully in its approach to China.<sup>11</sup>

Each of these proposals, however, appears to either misinterpret competition as simply a matter of arms races and intimidation tactics or make vague recommendations that mirror a return to the foreign policy stance of the US toward China for the last 40 years. Such policies may not have led to war, but that does not mean they deterred it. Certainly, they did little to increase the probability of success should deterrence fail, considering the Chinese military is more powerful, influential, and confrontational today than it was in Mao's era. More concerning is that the trepidation expressed by Western analysts in response to the 2017 competition mandate is an indicator that the CCP's strategy of increased military capacity and presence as a deterrent to Western encroachment is working.

A reluctance to compete for global influence born out of a fear of conflict with the prescribed opponent is the *raison d'être* of adversarial deterrence efforts. The hesitancy to recognize the CCP as a potentially bad actor that may require more than "engagement" to restrain is understandable given the extent of Beijing's integration into the world's economic and security infrastructure. It is also a contributing factor to much of the apprehension directed toward competition. Economic decoupling, as the process has come to be known, is a frightening prospect for nations dependent upon Chinese labor, technology, and transnational commerce to

prop up their economies.<sup>12</sup> The value of cooperation between great powers is not lost on the political establishment in the United States either.

President Joe Biden's administration recognized as much in its *Interim National Security Strategic Guidance* by stating that "strategic competition does not, and should not, preclude working with China when it is in . . . [the US] national interest to do so."<sup>13</sup> Coincidentally, Chairman Xi Jinping has made similar proclamations. Author and Tufts University professor Sulmaan Wasif Khan, a dispassionate observer of China's activities, suggests that Beijing "will cooperate with the United States where cooperation suits its interests."<sup>14</sup> But if both leaders are willing to cooperate merely on these terms and each nation sees fit to expand its influence, ultimately, their interests will encounter disunity. In other words, the United States must account for the space in which interests do not intersect—and it is in that widening space that competition occurs.

As defense officials and policy makers struggle to balance cooperation and competition, most of the suggested vectors of cooperation between the United States and CCP—such as carbon emissions reduction, technological exchange, and disaster response and relief—remain less than promising. The White House's interim strategic guidance mentions climate change as a national security concern 27 times. According to 2020 data compiled by the International Energy Agency and published by the Union of Concerned Scientists, China is the single greatest carbon emitter on the planet (28 percent)—more than the United States (15 percent), India (7 percent), and Russia (5 percent) combined.<sup>15</sup> Despite Xi Jinping's recent claim that his regime eradicated poverty, which might explain an increase in emissions due to industrial productivity, Martin Raiser of the World Bank estimates that China still has roughly 200 million people below the poverty line or 13 percent of its population.<sup>16</sup>

Regarding technological exchange and disaster response, the interim strategic guidance mentions the need to keep US technological research far from prying eyes in the CCP. Even China expert Michael Schuman admitted recently that "fueling Xi's rise by sharing our best technology is not a good idea." He proceeded to recommend sanctions as a response to Beijing's alleged human rights violations.<sup>17</sup> The pandemic that swept the world in early 2020 provided unique insight into the CCP's practices of international information exchange and communication. In January 2021, the World Health Organization-sponsored Independent Panel for Pandemic Preparedness and Response criticized China's slow reaction to the outbreak, while other reports cited Beijing's domestic stranglehold on information as a key factor in the spread of the virus.<sup>18</sup>

Although some may see these shortcomings as opportunities for further cooperation, one should bear in mind that they occurred at the apex of 40 years of cooperative US policies toward China—even in the wake of the 1989 Tiananmen Square protests. According to former national security advisor Lt Gen H. R. McMaster, this retrenchment from the competitive space emboldened Beijing's leaders. As a result, China pursued aggressive policies toward its neighbor Taiwan, including constructing islands with military significance in the South China Sea.<sup>19</sup> The United States must retain the option of cooperation, but it should not engage the CCP with the notion that cooperation is beneficial to US interests as long as it is approached earnestly. Nor should it prop up its strategic documents and therefore public expectations on a political reality that does not exist.

In what should be required reading for defense professionals examining this problem, National Intelligence University professor Dan Tobin's March 2020 testimony before the US-China Economic and Security Review Commission explains much that is missing from the public discussion on Xi Jinping's ambitions—chiefly Xi's own words.<sup>20</sup> Though Tobin also takes issue with the term "great power competition" (this article adopts the term "strategic competition"), his feasibility assessment of a purely cooperative strategy with Beijing is less than sanguine. Xi Jinping's declared "new era of Socialism with Chinese characteristics," delivered at the CCP's Nineteenth National Congress in October 2017, was a watershed moment of candid Chinese policy. The United States and indeed the entire free world must reconcile their aversion to competing with Xi's goal of making China "a global leader in terms of composite national power and international influence" before midcentury—and they must come to terms with what this world would look like.<sup>21</sup> Comments from China's top diplomat, Yang Jiechi, during a March 2021 meeting with US officials in Anchorage, Alaska, made clear that the political ways and ends of the two nations have never been more divergent.<sup>22</sup> Stated bluntly—and paraphrasing Demosthenes—the CCP competes with the United States even if the United States is not in competition with the CCP.

### **The Uses and Abuses of Cold War Analogies**

Comparisons to the Cold War are inevitable, and there has been no shortage of juxtaposition between then and now in the professional literature.<sup>23</sup> That does not mean, however, that each comparison is viable. Xi Jinping is not Mikhail Gorbachev, China is not Soviet Russia, and it is not the 1980s. As Sir Michael Howard and Margaret MacMillan suggest, using history as a guide for current policy is somewhat of a double-edged

sword. It can arm its wielder with information suited to fit predetermined ends.<sup>24</sup> In the case of US-Sino relations, MacMillan's 2008 observation is important: "Today's world is far removed from the stasis of the Cold War. It looks more like that of the decade before 1914 and the outbreak of World War I or the world of the 1920s." MacMillan clarifies that "in those days, as the British Empire started to weaken and other powers, from Germany to Japan to the United States, challenged it for hegemony, the international system became unstable."<sup>25</sup>

Perhaps it is the presumptuous Cold War scaffolding upon which many comparisons rest that stifles original strategic thought directed toward US-Sino relations in the first place. Using 30-year-old allegories to understand the present strategic environment, even as Xi Jinping couches his struggle in medieval references, exemplifies the conceptual fissures that separate US strategic thought from Beijing's reality. This observation is laid bare by Xi Jinping's fixation on "great national rejuvenation" following a period of humiliation at the hands of Western powers that he likens to the hundred years of Mongolian oppression China suffered in the thirteenth century.<sup>26</sup> Reducing the complexities of US-Sino relations to a Cold-War-or-not construct could do more harm than good in strategic formulation. This is not to say that Cold War analogies are outdated or irrelevant, only that they are not always the best lens through which one might capture a deeper understanding of current US-Sino relations.

Gorbachev was the first and last university-educated Soviet leader since Lenin. He charmed most with whom he parlayed, openly recognized fundamental problems with Russia's governing Marxist-Leninist ideology, and pledged a willingness to rid his country of nuclear weapons. He even welcomed Secretary of State George Shultz to teach classes on free market economics in Moscow (elements of which Gorbachev later echoed in his 1987 book *Perestroika*).<sup>27</sup> These developments occurred amid the backdrop of President Ronald Reagan's Strategic Defense Initiative or "Star Wars" program that many chided as too confrontational. Although the prospect of Xi Jinping entertaining similar liberal tendencies is unlikely today, some nevertheless suggest that cooperation with Beijing is a favorable strategic approach because it bore fruit on occasion with Soviet leaders. Yet according to officials with access to recent US-Sino communications, Xi Jinping considers Gorbachev's example a political model to avoid. McMaster, for instance, argues that Beijing's leaders see Gorbachev's concession to Western values as causal factors in the Soviet Union's demise. This view has led them to burrow ever deeper into their "China model" as an alternative to the rules-based international order of the last 75 years.<sup>28</sup>

Others have transplanted the strategic tissue of the Cold War into present challenges, describing the US-Sino competitive framework as a matter of arms races and military strength metrics. In reality, the current competition has less to do with numbers of tanks and more with the proliferation of information and the public's perception of truth. A common notion is that a war will be won only through aggressive, whole-of-government competition in the information space.<sup>29</sup> Xi Jinping's fascination with and desire to control Chinese history is emblematic of this environment, resulting in his reluctance to criticize Mao Zedong. Xi likely wants to avoid the same backlash Gorbachev encountered after expressing his lack of faith in Marxist-Leninism as a viable long-term political model.

In MacMillan's estimation, Gorbachev's exposure of the Soviet Union's dark associations with Nazi Germany led to its downfall. This verdict further reinforces McMaster's assessment of the central role of information in the China model: lose control of the past, and the CCP could lose control of its future.<sup>30</sup> These observations reflect two strategic imperatives. The first is to be wary of the eagerness with which one cooperates. Over the long arc of history, this proclivity may result in entanglement with unsavory bedfellows that damage a nation's standing. The second is to recognize the power of information in shaping strategic outcomes. If information was influential before the advent of the Internet and social media, then it is transformational now. History is undoubtedly an important tool for promoting understanding, but leaders may need to cast their net beyond the Cold War to find the most instructive lessons it has to offer. When choosing to cooperate, the United States must be sure who is dictating the terms of cooperation. Otherwise, that relationship becomes the very zero-sum game that so many decry in competition.

### **Cooperation as a Strategic Formula for US-Sino Relations**

For all the attention it has received in recent years, cooperation as a strategic approach to managing rival powers is little more than a rebranded model of twentieth-century "engagement" policies, and the same shortfalls remain intact. The Bush and Clinton administrations were forced to deviate from their engagement construct when Beijing overstepped. In 1999, for instance, President Clinton forbade the sale of communications equipment to a Singapore-based company because of its links to the People's Liberation Army (PLA).<sup>31</sup> Such circumstances led to soul-searching in the US defense community regarding the utility of engagement as a means of shaping China's behavior. By the end of the twentieth century, many experts agreed that engagement had been an insufficient framework for ne-



gotiating US policy toward China when it violated international norms.<sup>32</sup> Concurrently, members of the engagement camp maintained that confronting China on its human rights abuses would be damaging to its fated liberalization.<sup>33</sup> It appears as though this approach has served as the CCP's means to an end, allowing it to accumulate power and influence via Western engagement even as it pursued illiberal social, economic, diplomatic, and security policies. Before the United States could formulate a comprehensive response to these developments, the 2001 terrorist attacks on New York City and the Pentagon reoriented US national resources toward the Middle East for the next 16 years.

In the twenty-first century alone—and while the United States combatted global terrorism—the PLA more than tripled the strength of its navy (surpassing the number of ships in the US fleet by a margin of 60 or more). The PLA also expanded its archipelago of ersatz islands in the South China Sea and developed a robust suite of counterspace defense capabilities. Numerous projections suggest that China will become the world's largest economy by 2035 and by 2050 will have an economy roughly twice that of the United States.<sup>34</sup> Such developments imply military potential far removed from the “technically backward and operationally immature” force plagued by funding shortages described in professional journals near the end of the twentieth century.<sup>35</sup> Perhaps most worrisome is a critical disconnect that seems to be developing between the popular consensus about the CCP's threat and the assessments of career China experts. Dan Tobin and Gregory B. Poling, director of the Asia Maritime Transparency Initiative, have each commented on this pattern contributing to growing misunderstandings surrounding Beijing's capabilities and intentions.<sup>36</sup> A byproduct of this confusion is the artificially magnified strategic value of cooperation.

The above developments serve as bargaining chips that will ultimately carve out a new paradigm of global cooperation over time—much of which will likely be pursued in contention with US and allied national interests. This reality brings to light a fundamental point: competition is not a bipolar exercise. It is as much about empowering and protecting allies as it is securing US interests. In terms of options, China as a regional hegemony reduces those available to the United States and its partners to cooperation alone. This situation, which is a plausible corollary of Beijing's grand strategy, is also coincidentally the argument put forth by many critics of competition: cooperate or risk war.<sup>37</sup> If these are the only two options, then there is no option, no matter how egregious the CCP's transgressions. And if the options available to the United States become so

restricted, where does that leave its vulnerable partners? This paradox was the same binary construct submitted to President Ronald Reagan by State Department officials before he delivered his ill-advised but now world-renowned 1987 speech calling on Gorbachev to “tear down this wall!”<sup>38</sup> Cooperation as the driving factor of foreign policy during eras of heightened interstate competition is typically rooted in lofty assumptions.

One of these is that the United States can defend its national security interests—and those of its allies and partners—while cooperating with increasingly brazen revisionist powers with often opposing national interests and, perhaps more significant, incompatible values.<sup>39</sup> In the years following the Second World War, most notably between the 1945 Bush Plan and the Soviet Union’s “unexpected” test of an atomic bomb in 1949, the United States went to great lengths to cooperate with Russia on nuclear counterproliferation efforts.<sup>40</sup> But further exposure of Soviet espionage as the United States and Great Britain began decrypting the intercepts in 1946 led to a perception that the ends of the two nations’ cooperative means were in a contest—making competition inevitable.<sup>41</sup> Similar dynamics are evident in China’s proliferation of artificial-intelligence-powered surveillance technology, continued theft of US intellectual property, and espionage directed against the United States.<sup>42</sup> A 2020 report found that out of 152 public instances of Chinese-linked espionage since 2000, 74 percent occurred between 2010 and 2020 (Xi Jinping assumed power in 2011).<sup>43</sup> As of April 2021, over 500 scientists in the United States were under investigation for potentially illicit interactions with Chinese companies or officials.<sup>44</sup> Certainly, the United States must compete to lessen the damage of these efforts. It cannot do so without a strategic mandate because the historical default involves US government agencies cooperating despite such aggressive activities.

The second assumption is that there will be ample opportunities for productive cooperation and at least two parties willing to sacrifice some of their interests to do so.<sup>45</sup> The DOD, however, will struggle to cooperate with the CCP on matters such as defense technology and information sharing while Beijing proliferates oppressive surveillance tools and spreads black propaganda about US intentions and activities globally.<sup>46</sup> Similar to the conditions laid out in the short-lived uranium enrichment agreement between the United States and the Islamic Republic of Iran, the CCP should meet particular conditions if it expects cooperation. One of these would be the immediate halt to its Uighur detention program.<sup>47</sup> As of this writing, no such conditions exist, and the majority of arguments against a competitive strategy for US-Sino relations frame cooperation with the

CCP in unconditional terms. In fact, they put the onus to cooperate on the United States. If cast upon any other state, suspicion of widespread human rights abuses would preclude the United States from engaging in security cooperation endeavors with the said nation. Surely the same standards should apply to a regional power with the largest navy in the world.

Despite the tendency to frame competition as a military endeavor, neither diplomacy nor defense has a monopoly on the concept. Most peacetime DOD activities fall under the umbrella of a specific task known as security cooperation. It often involves close coordination with State Department officials and other agencies—meaning competition has little chance of success when it is interpreted as a matter of military confrontation.<sup>48</sup> Calls to compete more seriously in the diplomatic realm have characterized the urgings of everyone from George Kennan to M. Taylor Fravel of the Massachusetts Institute of Technology in his 2021 testimony on US-Sino relations.<sup>49</sup> Strategic competition should not prevent diplomatic engagement, only shape the contours of its agenda. And if by nature the DOD must be prepared to compete and fight an adversary, then it should have some notion of who it might contend with. The conceptual framework of competition supports both diplomatic and defense efforts, while the well-meaning theory of cooperation or engagement does not. Further, while cooperation can and should be an implied and underlying current of competition, the inverse is not true. If instructed to cooperate with its competitors generally, then the capacity for the United States to compete aggressively with specific adversarial capabilities will stagnate. And so, according to the 2018 National Defense Strategy, it has.<sup>50</sup>

### **The Inevitability of a Competitive Framework**

A senior China studies fellow at the Council on Foreign Relations, Elizabeth C. Economy, testified recently before the Senate Foreign Relations Committee that the “U.S.-China relationship remains overwhelmingly competitive.” She added that supporting this framework is “essential to U.S. competitiveness with China, not to mention the future well-being of the international system.”<sup>51</sup> Her testimony made clear, however, that this reality should not close the door to cooperation with China’s leaders when opportunities arise—likely a nod to her 2019 testimony on “smart competition.”<sup>52</sup> It is the scarcity of such opportunities amid a growing list of troubling CCP activities with which the United States must compete that poses the most significant risk to US-Sino cooperation.

Despite the relatively nascent boon to China-watching spurred by language in recent strategic documents, China’s rise as a global power has

been a slow and steady one. A 1999 RAND Corporation report presented the realist perspective that a China with an economy equal to the United States, and therefore “roughly comparable military potential,” would become a “rival for world power.”<sup>53</sup> Additionally, “according to this theoretical outlook, a China that approached or equaled the United States in power would seek to vindicate its territorial claims, attain regional hegemony, increase its status in global terms, and alter the rules of the international system to its advantage.”<sup>54</sup>

The Pentagon’s 2020 report to Congress on the People’s Republic of China (PRC) made some bleak assessments within the context of Xi Jinping’s self-described goal of becoming a “world-class” military power by 2049.<sup>55</sup> The report states that Beijing will likely seek a military equal or superior to that of the United States. It also submits that the PLA is “already ahead” of the United States in several key areas, including shipbuilding, land-based ballistic and cruise missile development, and integrated air defense systems. Further, the PRC uses the PLA as a tool of statecraft to advance global interests and reshape the international order.

Uncomfortable as it may seem, the DOD is just beginning to take seriously a competitive environment to which its adversaries are already well adapted. The United States drafted its Irregular Warfare Annex to the 2018 National Defense Strategy largely out of a recognized need to improve its whole-of-government capabilities in the gray zone where Beijing has dedicated the preponderance of its security resources since at least 1999.<sup>56</sup> Surely the United States cannot honor the guidance in this document without an enduring strategic mandate to counter these influence mechanisms. China’s systems warfare and unrestricted warfare, much like Russia’s new generation warfare, aim to apply all instruments of national power to an opponent’s strategic pressure points—which consist of ever fewer traditional military weaknesses.<sup>57</sup> China and Russia are each focused on competing primarily with the United States across the conflict spectrum and specifically below the threshold of total war. The spirit and letter of these approaches to political warfare do not reflect an urgent desire to cooperate for mutual benefit. Instead, they demonstrate a capacity to achieve warlike objectives in the competitive space. Like King Philip, competitors of the United States are already competing aggressively. Like Athens, the United States is still engaged in an impassioned internal debate over whether it should rise to the challenge.

According to the International Monetary Fund, China’s economy will experience 8.1 percent growth in 2021 (3 percent more than the US). With a 6.8 percent increase to its defense budget the same year, these trends put

China on a path to achieve its goal of becoming a comprehensive military power by 2035.<sup>58</sup> It is important to remember that China's government does not have a clear separation of powers. Therefore, China can mobilize all instruments of national power, if required, for military purposes through its military-civil fusion (MCF) model.<sup>59</sup> As a result, using China's comparatively small defense budget as a metric to gauge national strength amounts to mirror-imaging that fails to account for fundamental differences between the two nations. If the United States goes to war, the Pentagon goes to war. If China goes to war, China goes to war—"private" companies and all. The same appears true in competition as Xi Jinping promotes international cultural solidarity while pursuing interests in locales that should be of little concern if the CCP was constrained to merely negotiating its domestic troubles, as some of the literature indicates.<sup>60</sup>

In Africa, for instance, China has been laying security and telecommunications groundwork for decades; making direct cash payments to African leaders; and funding federal buildings, infrastructure projects, and police stations. Simultaneously, it has sought greater oversight of interstate commerce and port security activities through a process some call "palace diplomacy."<sup>61</sup> One study found that since 1966 Chinese companies have built hundreds of government buildings in Africa, including presidential residences, the opulence of which are conspicuous amid an otherwise underdeveloped backdrop.<sup>62</sup> China's investments on the continent have earned the approval of current and former African government officials, such as W. Gyude Moore, who now works at the Center for Global Development and remains an outspoken critic of US foreign policy in Africa.<sup>63</sup> From 5G platforms in Kenya to billion-dollar energy investments in Nigeria, each policy is portrayed in Chinese state media through the comparative lens of US activity. Such juxtapositions are to the extent that after public outcry over China's handling of the coronavirus, China's top diplomat, Wang Yi, claimed his country was fighting two viruses in Africa—the coronavirus and the US "political virus."<sup>64</sup> In 2021, as Chinese officials seem keen to export their party-controlled military model to developing nations in the region, it is hard to overstate the value of competing to promote liberal values and secure governing configurations there.<sup>65</sup>

Meanwhile, China's naval base in Djibouti—its first foreign military headquarters—appears to be expanding.<sup>66</sup> Some predict that China will lead the world in increased overseas security spending by 2023, and the PLA's goal to become a "global strategic force" supports these projections.<sup>67</sup> Since 2005, China has invested more than \$2 trillion overseas, roughly \$83 billion of which went to Sub-Saharan Africa. China's exports in the

region amount to more than those of the United States, United Kingdom, Russia, and India combined.<sup>68</sup> With little attention from the international community, Chinese military fortifications on the Red Sea can now provide maritime access via the Suez Canal to NATO's Mediterranean underbelly. Importantly, certain African leaders have also cushioned the CCP from international outrage. Beijing enjoys broad support from its African partners in the United Nations on critical votes concerning everything from maritime disputes in the South China Sea to human rights abuses.<sup>69</sup> By no means do these developments make China an enemy—especially not the Chinese people. Nevertheless, these are not the actions of a regional power simply trying to survive, and US strategic thought should reflect that somewhat disquieting reality.

### **Recommendations and Implications**

As Dan Tobin explained to the author, it would be a straw man to say that arguments exist for purely competitive or exclusively cooperative strategies toward the CCP.<sup>70</sup> Most China experts are rather measured in their approach, and even doves agree that a tougher stance is warranted. But as explained in this article, many also see value in purging the great power or strategic competition narrative altogether. Doing so would erase gains already achieved in how security professionals view the present operational environment. It would also nullify studies completed within that conceptual space and force the national security enterprise to revise countless publications and doctrinal references for what amounts to little more than a stylistic amendment. This change would further contribute to the already dizzying array of jargon bombarding security professionals and produce minimal substantive benefit to US national security. The United States should reinforce the competition imperative in its next tranche of strategic documents, with a particular focus on the CCP's intended proliferation of socialism with Chinese characteristics. US strategic guidance should describe the concept as a political model antithetical to the liberal values shared by the world's free nations. Such clarification would provide two key opportunities for the US defense enterprise.

First, it would license a much-needed injection of awareness and education initiatives into the DOD vis-à-vis Chinese history lessons, translated public statements of CCP officials, and instruction on the ideological architecture of socialism with Chinese characteristics. Contrary to assertions that the current rivalry between the United States and China is nonideological, Beijing officials have for years championed their ideological system as the preferred way ahead for developing nations. At a recent

Anchorage meeting, Mr. Yang demanded that the United States “stop advancing its democracy in the rest of the world” because many Americans “have little confidence in the democracy of the United States.”<sup>71</sup>

Xi Jinping himself proclaims that his personalized brand of socialism will eventually be at the helm of global influence and military power. In his 1 July 2021 speech commemorating the Chinese Communist Party centennial, Xi described Marxist-Leninism as fundamental to the “soul of our party.” He pledged to wield Marxist and Maoist thought as tools to “observe, understand, and steer the trends of our times.”<sup>72</sup> Thus, it stands to reason that the greater US national security enterprise—from military cadets to elected officials—should be intimately familiar with the ideology’s topography. Such educational reforms during the Cold War armed defense officials, diplomats, and elected leaders not merely with the knowledge to understand an opponent and therefore counter him more effectively. They also engendered the empathy to prevent careless or ignorant mistakes that lead to unnecessary conflicts or costly policy decisions.

Second, ratifying the competition imperative in the next national security strategy would allow the Pentagon to further refine its already expansive modernization efforts with a priority mandate. These efforts would not simply pertain to conducting large-scale combat operations or cornering the market on artificial intelligence and space capabilities. The CCP is adept in political warfare and strategic irregular warfare to a degree that makes Western powers accustomed to force-on-force military engagements uncomfortable.<sup>73</sup> If the United States and its allies want to broaden their competitive toolsets in this realm below the threshold of war, they must recognize not only that the realm exists but also that they are entering a game their opponent is already well versed in. China’s government is especially skilled in exploiting all instruments of national power in competition for information dominance and global influence.<sup>74</sup> Affirming the mandate to compete would serve both of these critical interests.

## **Conclusion**

Samuel Huntington articulates the value of cooperation as well as any before him or since: “The futures of both peace and Civilization depend upon understanding and cooperation among the political, spiritual, and intellectual leaders of the world’s major civilizations.”<sup>75</sup> He is right. But had Huntington uttered these words to Demosthenes in 341 BCE, they may have lost some of their instructive quality. Context matters. By its nature, cooperation requires two or more willing parties. The view that there are pearls of useful collaboration waiting to be plucked from the

geopolitical sea if the United States would only toss aside its competitive syntax is based more on wishful thinking than any historical reality. A framework of cooperation with revisionist powers suggests that all or most US interests and values are mutual or negotiable with regimes that have wildly different views of the world. This is simply not true.

Historian Margaret MacMillan wrote that “if the study of history does nothing more than teach us humility, skepticism, and awareness of ourselves, then it has done something useful.”<sup>76</sup> Thousands of years of history considered, the belief that the United States can maintain the same prosperous international order it has enjoyed for 75 years without competing assertively with a challenger is a display of strategic hubris that might have surprised even the late Alistair Horne.<sup>77</sup> Although competition and cooperation are not mutually exclusive, one must indeed take priority over the other. Competing for influence, strategic access, and ultimately options should take priority while cooperating when and where feasible with revisionist powers remains a supporting function. If the concept of competition is simple, then in an age of such strategic complexity that simplicity should be welcomed.<sup>78</sup> There is certainly room to build on the 2017 and 2018 documents—and the Biden administration seems to be doing just that. However, the solid foundation they established should not be ripped asunder over a semantic grudge match. Even reformed CCP doves are beginning to entertain a more realist stance toward Beijing in light of its recent activities.<sup>79</sup>

Strategic competition should be viewed less as a gateway to escalation and more as a realist alternative to the decades-old status quo of often-abandoned laissez-faire policies designed to counter the expansionist illiberal conduct of China’s leaders. It merely affords the US national security enterprise a frame of reference for the environment in which it operates, without telling it how to negotiate its complexities. That challenge is and should be left to the individual departments and services. Strategic competition is not a policy; it is a statement of geopolitical reality. The United States should acknowledge that reality and continue using it to refine its defense policies even as cooperation remains preferable when two or more willing parties enjoy shared interests. **SSQ**

#### **CAPT Michael P. Ferguson, USA**

Captain Ferguson is an author and analyst with nearly 20 years of infantry and intelligence experience in dozens of countries across four continents. His research focuses on applied history, strategic theory, and irregular warfare. He is a senior military advisor assigned to Fort Bragg, North Carolina, and coauthor of a forthcoming book from Routledge on the legacy of Alexander the Great.



## Notes

1. Ian Worthington, *Demosthenes of Athens and the Fall of Classical Greece* (Oxford: Oxford University Press, 2013), 335–37.

2. Zack Cooper, “Bad Idea: ‘Great Power Competition’ Terminology,” *Defense 360*, Center for Strategic and International Studies, 1 December 2020, <https://defense360.csis.org/>.

3. The 2017 National Security Strategy reframed the strategic environment as one driven by heightened interstate competition. See The White House, *2017 National Security Strategy of the United States of America* (Washington, DC: Department of Defense, 2017), <https://trumpwhitehouse.archives.gov/>; and Evan A. Feigenbaum, “Why the US and China Forgot How to Cooperate,” Carnegie Endowment for International Peace, 28 April 2020, <https://carnegieendowment.org/>.

4. Austin Doehler, “Great Power Competition Is Too Narrow a Frame,” *Defense One*, 6 December 2020, <https://www.defenseone.com/>; Daniel H. Nexon, “Against Great Power Competition: The U.S. Should Not Confuse Means for Ends,” *Foreign Affairs*, 15 February 2021, <https://www.foreignaffairs.com/>; Sharon Squassoni, “Why Biden Should Abandon the Great Power Competition Narrative,” *Bulletin of the Atomic Scientists*, 12 January 2021, <https://thebulletin.org/>; and Emma Ashford, “Great-Power Competition Is a Recipe for Disaster,” *Foreign Policy*, 1 April 2021, <https://foreignpolicy.com/>.

5. Zalmay Khalilzad et al., *The United States and a Rising China: Strategic and Military Implications* (Washington, DC: RAND Corporation, 1999), 63–69, <https://www.rand.org/>.

6. Edward Wong and Chris Buckley, “U.S. Says China’s Repression of Uighurs is ‘Genocide,’” *New York Times*, 19 January 2021, <https://www.nytimes.com/>; Steve Scherer, “Canada’s Parliament Passes Motion Saying China’s Treatment of Uighurs Is Genocide,” *Reuters*, 22 February 2021, <https://www.reuters.com/>; and Sheena Chestnut Greitens, “Dealing with Demand for China’s Global Surveillance Exports,” Brookings Institution, April 2020, <https://www.brookings.edu/>.

7. Ewelina U. Ochab, “British Lawyers Find Credible Evidence of Genocide against the Uyghurs in Xinjiang,” *Forbes*, 8 February 2021, <https://www.forbes.com/>; and Matthew Hill, David Campanale, and Joel Gunter, “Their Goal Is to Destroy Everyone: Uighur Camp Detainees Allege Systematic Rape,” *BBC News*, 2 February 2021, <https://www.bbc.com/>.

8. Mallory Shelbourne, “SECDEF Nominee Austin Affirms Threat from China, Will ‘Update’ National Defense Strategy,” *US Naval Institute News*, 19 January 2021, <https://news.usni.org/>.

9. Nexon, “Against Great Power Competition.”

10. Robert Sutter, also of Georgetown University, testified before the Senate Foreign Relations Committee in 2010 on the merits of a “less confrontational” strategy to counter the CCP’s illiberal activities. See *Principles for US Engagement with Asia: Hearing before the Senate Foreign Relations Committee*, 111th Cong., 2d sess. (21 January 2010) (statement of Robert Sutter, faculty, Georgetown University), <https://www.foreign.senate.gov/>. By 2021, likely due in no small part to Xi Jinping’s presence, Sutter’s stance on US policy toward the CCP had hardened significantly. See *US-China Relations at the Chinese Communist Party Centennial: Hearing before the U.S.-China Economic and Security Review*

Commission, 117th Cong., 1st sess. (28 January 2021) (statement of Robert Sutter, professor, George Washington University), <https://www.uscc.gov/>.

11. Ryan Hass, "China Is Not Ten Feet Tall: How Alarmism Undermines American Strategy," *Foreign Affairs*, 3 March 2021, <https://www.foreignaffairs.com/>; Kathy Gilsinan, "How the U.S. Could Lose a War with China," *The Atlantic*, 25 July 2021, <https://www.theatlantic.com/>; and Jeff Schogol, "The United States Risks Getting into Another Cold War with China," *Task and Purpose*, 13 March 2021, <https://taskandpurpose.com/>.

12. Valbona Zeneli and Joseph Vann, "The Real Strategic End Game in Decoupling from China," *The Diplomat*, 18 September 2020, <https://thediplomat.com/>.

13. The White House, *Interim National Security Strategic Guidance* (Washington, DC: Department of Defense, 2021), <https://www.whitehouse.gov/>.

14. Sulmaan Wasif Khan, *Haunted by Chaos: China's Grand Strategy from Mao Zedong to Xi Jinping* (Cambridge, MA: Harvard University Press, 2018), 219.

15. "Each Country's Share of CO2 Emissions," Union of Concerned Scientists, 12 August 2020, <https://www.ucsusa.org/>.

16. John Ruwitch, "What China's 'Total Victory' Over Extreme Poverty Looks Like in Actuality," NPR, 5 March 2021, <https://www.npr.org/>.

17. Michael Schuman, "Xi Jinping Turned Me into a China Hawk," *Politico*, 5 March 2021, <https://www.politico.eu/>. The Biden administration announced on 17 March 2021 that it will impose sanctions on China and several other states for their supposed interference in the 2020 US presidential elections. See Chun Han Wong, "Biden Imposes His First Sanctions on Chinese Officials Ahead of Bilateral Meeting," *Wall Street Journal*, 17 March 2021, <https://www.wsj.com/>.

18. Alexa Lardieri, "China, WHO Fumbled Coronavirus Pandemic Response, Independent Panel Finds," *U.S. News & World Report*, 19 January 2021, <https://www.usnews.com/>; and "China COVID-19: How State Media and Censorship Took on Coronavirus," BBC News, 29 December 2020, <https://www.bbc.com/>.

19. H. R. McMaster, *Battlegrounds: The Fight to Defend the Free World* (New York: HarperCollins, 2020), 125–29.

20. "A China Model?" *Beijing's Promotion of Alternative Global Norms and Standards: Hearing before the U.S.-China Economic and Security Review Commission*, 116th Cong., 2d sess. (13 March 2020) (statement of Dan Tobin, Faculty Member, China Studies, National Intelligence University), <https://www.uscc.gov/>.

21. "A China Model?," 1.

22. Mr. Yang Jiechi ran the gamut from accusing Secretary of State Antony Blinken and national security advisor Jake Sullivan of hypocrisy to suggesting that Western values are not universal values, even criticizing democratic systems of government as inherently flawed. See Justin McCurry, "The US and China Publicly Rebuke Each Other in First Major Talks of Biden Era," *The Guardian*, 18 March 2021, <https://www.theguardian.com/>.

23. Andrey Lungu, "The U.S. Needs an Endgame before It Plunges into the Next Cold War," *Foreign Policy*, 24 September 2020, <https://foreignpolicy.com/>.

24. Michael Howard, "The Use and Abuse of Military History," *Parameters* 11, no. 1 (1981), <https://press.armywarcollege.edu/>; and Margaret MacMillan, *Dangerous Games: The Use and Abuse of Military History* (New York: Modern Library, 2008).

25. MacMillan, *Dangerous Games*, 11.

26. Michael Schuman, *Superpower Interrupted: The Chinese History of the World* (New York: Public Affairs, 2020), 128–31, 310–12.

27. John Lewis Gaddis, *The Cold War: A New History* (New York: Penguin Press, 2005), 233.

28. McMaster, *Battlegrounds*, 103.

29. For a view of modern competition with twentieth-century characteristics, see Robert Spalding, “Yes, We Can Win the Cold War with China—Here’s How,” *The Hill*, 13 June 2020, <https://thehill.com/>. For the role of information in the current environment, see Doowan Lee and Philip Reynolds, “The Strategic Offensive against the CCP,” *The Cipher Brief*, 8 February 2021, <https://www.thecipherbrief.com/>; and Michael P. Ferguson, “The Evolution of Disinformation: How Public Opinion Became Proxy,” *The Strategy Bridge*, 14 January 2020, <https://thestrategybridge.org/>.

30. MacMillan, *Dangerous Games*, 138; and McMaster, *Battlegrounds*, 101.

31. Khalilzad et al., *Rising China*, 67.

32. H. R. McMaster made this observation more recently in *Battlegrounds*, 128. Also see Khalilzad et al., *Rising China*, 67–68.

33. Khalilzad et al., 65–66.

34. For PLAN strength and space capabilities, see Department of Defense, *Military and Security Development Involving the People’s Republic of China 2020* (Washington, DC: Department of Defense, 2020), <https://media.defense.gov/>; Brad Lendon, “China Has Built the World’s Largest Navy. Now, What’s Beijing Going to Do with It?” *CNN*, 5 March 2021, <https://www.cnn.com/>. A 2010 report from the Carnegie Endowment for International Peace has aged remarkably well. Its prediction that China’s economy will outgrow that of the United States by 2035—and be roughly twice its size by mid-century—remains consistent with more current reports. See Uri Dadush and Bennett Stancil, “The World Order in 2050,” *Carnegie Endowment for International Peace*, April 2010, <https://carnegieendowment.org/>.

35. This quote, taken from the 1990 edition of *Jane’s Fighting Ships*, appears in *Red Star over the Pacific*, along with a litany of other predictions casting a “regionally oriented Chinese Navy” as “implausible until 2020.” See Toshi Yoshihara and James R. Holmes, *Red Star over the Pacific: China’s Rise and the Challenge to U.S. Maritime Strategy* (Annapolis, MD: Naval Institute Press, 2010), 214–16.

36. Gregory B. Poling, “The Conventional Wisdom on China’s Island Bases Is Dangerously Wrong,” *War on the Rocks*, 10 January 2020, <https://warontherocks.com/>. For Dan Tobin’s comments, see Tobin, *Testimony before USCC*, 2020.

37. Zhou Bo, “The Risk of China-US Military Conflict Is Worryingly High,” *Financial Times*, 25 August 2020, <https://www.ft.com/>.

38. President Reagan gave the speech on 12 June 1987. See Gaddis, *Cold War*, 235.

39. Robert B. Zoellick, “The U.S. Doesn’t Need a New Cold War,” *Wall Street Journal*, 18 May 2020, <https://www.wsj.com/>. In terms of values, it is important to highlight that senior CCP officials have repeatedly stated that the United States and the West do not have a monopoly on universal values. See also Hal Brands and Zack Cooper, “U.S.-Chinese Rivalry Is a Battle over Values,” *Foreign Affairs*, 16 March 2021, <https://www.foreignaffairs.com/>.

40. US Department of Energy, Office of History and Heritage Resources, “Nuclear Proliferation (1949–Present),” accessed July 2021, <https://www.osti.gov/>.

41. John Earl Haynes and Harvey Klehr, *Venona: Decoding Soviet Espionage in America* (New Haven, CT: Yale University Press, 1999), 8–23, 287–330.

42. Ross Andersen, "The Panopticon Is Already Here," *The Atlantic*, September 2020, <https://www.theatlantic.com/>; and "China Exports AI Surveillance Tech to over 60 Countries: Report," *Nikkei Asia*, 19 December 2019, <https://asia.nikkei.com/>.

43. Of note, these numbers do not include the more than 1,200 cases of alleged intellectual property theft filed by US companies against Chinese-linked organizations during the same period. See "Survey of Chinese Espionage in the United States Since 2000," Center for Strategic and International Studies, accessed July 2021, <https://www.csis.org/>.

44. Matthew Impelli, "Over 500 U.S. Scientists under Investigation for Being Compromised by China," *Newsweek*, 23 April 2021, <https://www.newsweek.com/>.

45. Julian Brave Noisecat and Thom Woodroffe, "The United States and China Need to Cooperate—for the Planet's Sake," *Foreign Policy*, 4 February 2021, <https://foreignpolicy.com/>.

46. Eric Chan and Peter Loftus, "Chinese Communist Party Information Warfare: US-China Competition during the COVID-19 Pandemic," *Journal of Indo-Pacific Affairs*, 1 May 2020, <https://www.airuniversity.af.edu/>.

47. Natasha Turak, "Iran's Uranium Metal Production Is 'Most Serious Nuclear Step' to Date, but Deal Can Still Be Saved," CNBC, 16 February 2021, <https://www.cnbc.com/>.

48. Joint Publication 3-20, *Security Cooperation*, 23 May 2017, <https://www.jcs.mil/>.

49. For Kennan's famous telegram that informally began the Cold War, see Wilson Center Digital Archive, "George Kennan's 'Long Telegram,'" 22 February 1946, <https://digitalarchive.wilsoncenter.org/>. For Fravel's comments, see *US-China Relations at the Chinese Communist Party's Centennial: Hearing* (statement of M. Taylor Fravel, director, Security Studies Program, Massachusetts Institute of Technology), 20, <https://www.uscc.gov/>.

50. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America* (Washington, DC: DOD, 2018), <https://dod.defense.gov/>.

51. *Advancing Effective U.S. Policy for Strategic Competition with China in the Twenty-First Century: Hearing before the U.S. Senate Foreign Relations Committee* (17 March 2021) (statement of Elizabeth Economy, senior fellow, China Studies, Council on Foreign Relations), <https://www.foreign.senate.gov/>.

52. *Smart Competition: Adapting U.S. Strategy Towards China at 40 Years; Hearing before the U.S. House Committee on Foreign Affairs*, 116th Cong., 1st sess. (8 May 2019) (statement of Elizabeth Economy, director, Asia Studies, Council on Foreign Relations), <https://www.congress.gov/>.

53. Khalilzad et al., *Rising China*, 17.

54. Khalilzad et al., 17.

55. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020*, Annual Report to Congress (Washington, DC: Department of Defense, 2020), <https://media.defense.gov/>.

56. Department of Defense, *Summary of the Irregular Warfare Annex to the U.S. National Defense Strategy* (Washington, DC: Department of Defense, 2020), <https://media.defense.gov/>; Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy* (Carlisle, PA: US Army War College Press, 2016), <https://apps.dtic.mil/>; and Charles T. Cleveland with Daniel Egel, *The American Way of Irregular War: An Analytical Memoir* (Santa Monica, CA: RAND Corporation, 2020), <https://www.rand.org/>.

57. Phillip A. Karber, "Russia's New Generation Warfare," National Geospatial-Intelligence Agency, 4 June 2015, <https://www.nga.mil/>; David A. Deptula, "Mosaic

Warfare,” *Air Force Magazine*, 1 November 2019, <https://www.airforcemag.com/>; and David Barno and Nora Bensahel, “A New Generation of Unrestricted Warfare,” *War on the Rocks*, 19 April 2016, <https://warontherocks.com/>.

58. International Monetary Fund, “World Economic Outlook,” January 2021, <https://www.imf.org/>; and Bonnie S. Glaser et al., “Understanding China’s 2021 Defense Budget,” Center for Strategic and International Studies, 5 March 2021, <https://www.csis.org/analysis/>.

59. For a brief overview of MCF, see US Department of State, “Military-Civil Fusion and the People’s Republic of China,” <https://www.state.gov/>. For a more detailed analysis, see Elsa B. Kania and Lorand Laskai, “Myths and Realities of China’s Civil-Military Fusion Strategy,” Center for a New American Security, 28 January 2021, <https://www.cnas.org/>.

60. For instance, see Stein Ringen, *The Perfect Dictatorship: China in the 21st Century* (Hong Kong: Hong Kong University Press, 2016).

61. Joshua Meservey, “China’s Palace Diplomacy in Africa,” Heritage Foundation, 29 January 2020, <https://www.heritage.org/>; and Will Reno and Jesse Humpal, “As the US Slumps Away, China Subsumes African Security Arrangements,” *Defense One*, 21 October 2020, <https://www.defenseone.com/>.

62. Meservey, “Palace Diplomacy.”

63. W. Gyude Moore, “A New Cold War Is Coming. Africa Should Not Pick Sides,” *Mail & Guardian*, 21 August 2020, <https://mg.co.za/>.

64. “Coronavirus: China Accuses U.S. of Spreading ‘Conspiracies,’” *BBC News*, 24 May 2020, <https://www.bbc.com/>.

65. Paul Nantulya, “China Promotes Its Party-Army Model in Africa,” *Africa Center for Strategic Studies*, 28 July 2020, <https://africacenter.org/>.

66. Peter Suci, “China’s Naval Base in Africa Is Getting Bigger. Is a Network of Bases Next?” *The National Interest*, 11 May 2020, <https://nationalinterest.org/>.

67. Paul Nantulya, “Chinese Security Contractors in Africa,” *Carnegie Center for Global Policy*, 8 October 2020, <https://carnegietsinghua.org/>.

68. For data on Sub-Saharan Africa investment, see “China Global Investment Tracker,” *American Enterprise Institute*, 2021, <https://www.aei.org/>.

69. Wang Chen and Chen Xiaochen, “Who Supports China in the South China Sea and Why,” *The Diplomat*, 27 July 2016, <https://thediplomat.com/>; and Catherine Putz, “Which Countries Are For or Against China’s Xinjiang Policies?” *The Diplomat*, 15 July 2019, <https://thediplomat.com/>.

70. Dan Tobin (faculty member, China Studies, US National Intelligence University), interview by the author, 19 March 2021.

71. See, for instance, Jeffrey A. Bader, “Avoiding a New Cold War between the US and China,” *Brookings Institute*, 17 August 2020, <https://www.brookings.edu/>. For Mr. Yang’s comments, see Matthew Lee and Mark Thiessen, “US, China Spar in First Face-to-Face Meeting under Biden,” *Associated Press*, 18 March 2021, <https://apnews.com/>.

72. “Full Text of Xi Jinping’s Speech on the CCP’s 100th Anniversary,” *Nikkei Asia*, 1 July 2021, <https://asia.nikkei.com/>.

73. The Irregular Warfare (IW) Annex to the 2018 National Defense Strategy began moving in the right direction, but realizing its vision will require a comprehensive embrace of IW across the US defense enterprise. See Linda Robinson et al., *The Growing Need to Focus on Modern Political Warfare* (Washington, DC: RAND Corporation, 2019), <https://www.rand.org/pubs/other/2019/07/>.

[www.rand.org/](http://www.rand.org/); and Jacques deLisle, “Political Warfare, Sharp Power, the U.S., and East Asia,” Foreign Policy Research Institute, 6 April 2020, <https://www.fpri.org/article/>.

74. Ainikki Riikonen, “Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China,” *Strategic Studies Quarterly* 13, no. 4 (Winter 2019): 122–45, <https://www.airuniversity.af.edu/>. See also Conrad Crane, “The United States Needs an Information Warfare Command: A Historical Examination,” War on the Rocks, 14 June 2019, <https://warontherocks.com/>.

75. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (London: Free Press, 2002), 321.

76. MacMillan, *Dangerous Games*, 169.

77. While Horne’s thesis connects hubris to “overreach” in war, his final chapter, “Echoes of Verdun,” explores the perils of powerful nations that come to believe certain contests are “unlosable,” such as the postwar French Army in Indochina. Alistair Horne, *Hubris: The Tragedy of War in the Twentieth Century* (New York: HarperCollins, 2015), 314.

78. Josh Kerbel, “The US Talks a Lot about Strategic Complexity. Too Bad It’s Mostly Just Talk,” Defense One, 9 March 2021, <https://www.defenseone.com/>.

79. Schuman, “China Hawk.”

# The Remote Sensing Revolution Threat

LTC BRAD TOWNSEND, USA

## Abstract

Remote sensing—using satellites to image objects on the ground—is rapidly evolving from primarily a strategic intelligence threat to national security to an operational threat to military forces. Remote sensing will further complicate the already well-understood intelligence and targeting threat created by drones and other battlefield sensors. Imminent remote sensing technologies will allow near real-time observation of military forces anywhere, at any time, and under any conditions. Ubiquitous observation will provide an overwhelming military advantage to the nation best able to leverage it while denying that capability to others. The current diplomatic, regulatory, and military means for managing this threat are inadequate for the level of challenge that these sensors will present to modern warfare. This article assesses the weaknesses in existing US approaches to managing the remote sensing threat. It then proposes a combination of novel diplomatic approaches and increased regulatory control measures that will complement future active military means of addressing the emerging threat of ubiquitous remote sensing.

\*\*\*\*\*

Early on the morning of 8 January 2020, as many as 10 Iranian missiles struck al-Assad Air Base in Iraq, a major hub of US military activity in the region.<sup>1</sup> That same day, news outlets worldwide commented on the apparent effectiveness of the Iranian missiles and the implications of the damage caused by the strikes. Much of this commentary and analysis used high-quality satellite imagery—provided by the US-based and licensed company Planet—taken in the hours after the attack. The photos allowed the world to see the extent of the damage and judge the relative accuracy of the strikes.<sup>2</sup> This episode was a watershed moment in the history of space. A US-based commercial remote sensing company had just released detailed, same-day satellite images of the effects of war between the US and a foreign power.

Iran also gained vital information that it might otherwise not have had on the effectiveness of its strikes and targeting. Using this imagery, Iran

could conduct poststrike analysis to refine its targeting for future strikes, presenting an even greater risk to US and Iraqi forces. Without Planet's satellite data, Iran would have had access only to fragmented and unconfirmed reports from eye-witnesses on the ground. Alternative means of gathering overhead imagery, such as the use of aircraft or drones, likely would have failed as neither Iraq nor the US would have allowed Iran to overfly al-Assad Air Base uncontested. Ultimately, Iran chose not to conduct follow-up strikes and further escalate the conflict, mitigating any potential damage that Planet's imagery could have caused. However, the swift public release of high-quality satellite imagery of an attack on US forces signaled the beginning of a new era in warfare—one that brings significant challenges, risks, and opportunities to future war fighting.

The opportunities inherent in having access to real-time imagery are easy to grasp. However, addressing the threat of high-quality, high-revisit rate, space-based remote sensing data in modern warfare is more complicated. It will require a tailored approach with military, regulatory, and diplomatic aspects. This article addresses existing and possible regulatory and diplomatic approaches while leaving the details of purely technical military options for dealing with the threat for future analysis. First, it discusses the development of remote sensing, trends in the rapidly evolving remote sensing market, and the effects of these trends on future war fighting. It then highlights current regulatory controls that can help mitigate the risk from domestic and allied commercial satellite imagery while balancing industry needs and national security. Finally, the article outlines the challenges of controlling third-party remote sensing through diplomatic means and proposes an approach to managing the third-party threat when diplomacy is inadequate.

## **Remote Sensing Development, Trends, and the Future of War Fighting**

### ***Remote Sensing Development***

Before the advent of satellites, obtaining detailed intelligence on enemy locations and disposition during a conflict required risky overflights or the use of ground-based reconnaissance. Outside of conflict, getting overhead imagery of other nations for intelligence purposes was even more difficult without satellites, as nations jealously guard their sovereign airspace. For decades the satellites that acquired this valuable overhead intelligence were expensive, few, and controlled by only a handful of nations. In the last decade, advances in commercial technology have led to a proliferation of



remote sensing technology, with at least 25 nations now possessing some remote sensing satellites of various quality.<sup>3</sup> For countries without national platforms, high-quality imagery is readily available from commercial sources. The democratization of remote sensing information represents a new and real threat to military forces that only adds to the future battlefield's increasing complexity. There are some overarching trends in remote sensing satellite development, and they represent a substantial threat to future military operations.

With the advent of remote sensing in the 1960s, satellites could largely replace aircraft overflights for intelligence gathering purposes, but not without limitations. While a satellite can pass freely overhead in its orbit, it cannot reasonably change its orbit to pass over a specific target sooner. Thus, space-based intelligence is dictated by time limitations (temporal resolution) that are exacerbated by cost and target resolution limitations (spatial resolution).<sup>4</sup> Once digital return was possible and imagery satellites were no longer single use, a balance needed to be struck between resolution and on-orbit lifetime. Imagery satellites are, or at least were, ruinously expensive, so they needed to be high enough in their orbits to avoid a level of atmospheric drag that would limit their on-orbit lifetime. Higher altitudes drove the need for larger and more exquisite optics to ensure that spatial resolution remained relevant, further increasing costs. These high costs made space-based intelligence a privilege limited to the handful of nations that could afford to build, launch, and operate remote-sensing satellites. Because space-based imagery remained expensive, the number of commercial platforms remained relatively small, limiting their operational impact.

This began to change in 2001 when relatively high-resolution imagery became readily available for purchase by third parties with the launch of QuickBird-2 and the advent of highly capable and fully commercial remote sensing satellites. The first to break the .5-meter resolution barrier was the US-based DigitalGlobe's WorldView-1, launched in 2007. WorldView-1's capabilities were exceeded by WorldView-3's in 2014. This satellite could capture images at a .3-meter panchromatic resolution, but it cost nearly \$600 million and had a best-case revisit rate to anywhere in the world of just over one day.<sup>5</sup> The most recent commercial satellite to follow this exquisite model was WorldView-4, which launched in 2016 and failed on orbit in early 2019—only two years into an expected 10-year lifespan.<sup>6</sup> These satellites returned high-resolution imagery but were limited by various technical factors to imaging 680,000 km<sup>2</sup> per day, an area roughly equivalent to the size of Texas.<sup>7</sup> With high spatial resolution but low tem-

poral resolution, these satellites were valuable intelligence tools but remained a relatively small operational risk to military forces in the field.

Increasing temporal resolution requires launching more satellites, but the technical limitations discussed above made doing so cost prohibitive as long as launch costs remained high. Only since 2015 have launch costs begun to fall in real terms as true commercial companies, most notably SpaceX, entered a market previously dominated by near national monopolies. These national monopolies relied primarily on domestic government contracts for funding and had no real competition, so they had little incentive to attempt revolutionary innovation. Beginning with NASA's Commercial Orbital Transportation Services (COTS) contract that essentially provided seed funding for SpaceX, real commercial competition entered the launch market for the first time, leading to dramatic technological leaps that have opened new market opportunities.

### ***Remote Sensing Trends***

A paradigm shift occurred with the drop in launch costs that coincided with a rapid shift toward satellite miniaturization. Miniaturization altered the economics of satellite construction, leading to a revolution in satellite imagery. Smaller satellites are cheaper. Dozens can be launched simultaneously into a single orbital plane, where careful manipulation of the space environment places them in useful configurations and decreases temporal resolution. The tradeoff is that remote sensing satellites launched in this way are individually much less capable of hosting large optical payloads, reducing their spatial resolution. Small remote sensing satellites compensate by being launched into much lower orbital altitudes—250 km versus 600 km or more for DigitalGlobe's more traditional WorldView satellites. However, the increased atmospheric drag on satellites in these orbits substantially reduces their lifetime. Thus, maintaining a constellation requires these small satellites to be frequently replenished. The shortened replacement cycle drives a demand for more satellites and launches, reduces unit cost, and allows for iterative improvements of both. These benefits further reinforce the economic incentives associated with this approach. A race is on to achieve the best spatial and temporal resolution possible. In late 2017, the US-based company Planet attained the goal of imaging the entire earth's surface at a 3–5 meter resolution in a single day.<sup>8</sup> Most would have considered this paradigm-shifting achievement impossible just a few years earlier. It was one of these relatively cheap satellites that provided the initial imagery of al-Assad Air Base. Planet is not alone in introducing disruptive approaches to remote sensing. Dozens of new imagery provid-

ers have begun to enter the market, offering a variety of capabilities from synthetic aperture radar (SAR) to hyperspectral imaging capabilities. As of 2021, many of these systems are already on orbit in small numbers as the first tranche of future constellations of similar satellites. The end state of this race between commercial companies and nations leveraging commercial technology is ubiquitous high-resolution coverage of the entire globe at all times. This resolution convergence will undoubtedly occur before 2030. However, hints of the war-winning nature of ubiquitous observation in modern warfare have already been demonstrated in the recent conflict between Armenia and Azerbaijan, albeit by airborne rather than space-based sensors.

### ***Effects of Remote Sensing Trends on Future War Fighting***

In late 2020, Armenia and Azerbaijan fought a small but intense conflict over the contested region of Nagorno-Karabakh demonstrating that that long-range precision strikes and indirect fire aided by overhead intelligence can be a war-winning combination. At the outset of the conflict, Armenia was considered a conventionally superior military to Azerbaijan with better training and leadership.<sup>9</sup> Even so, it was quickly outclassed by Azerbaijan's tactical use of drones to provide targeting data to Azerbaijan's artillery and other long-range precision weapons. Initially, Armenia operated a Russian-built air defense system that Azerbaijan needed to eliminate to fully use its Turkish- and Israeli-provided drone capability.<sup>10</sup> Azerbaijan was forced to use 11 unmanned Soviet-era AN-2 aircraft as bait to get the Armenian air defenses to fire so that it could identify and eliminate them.<sup>11</sup> Once Azerbaijan neutralized the air defenses, it could use drones to track and then destroy Armenian forces on the ground. By some counts, Azerbaijan destroyed nearly 1,000 tanks, armored fighting vehicles, and other vehicles during the short campaign using this precision fire, forcing Armenia to sue for peace.<sup>12</sup> Azerbaijan's success in using drones to provide targeting data to its indirect fire weapons offered a glimpse of future warfare.

Despite its success in the Nagorno-Karabakh conflict, drone warfare is not without limitations that satellite-based intelligence could overcome or augment. First, Azerbaijan defeated Armenia with airborne platforms that had limited fields of view and were subject to weather limitations on operations—constraints that would not impact satellites. Second, Russia quickly fielded a new counter-drone electronic warfare system, Krashukha-4, which successfully downed Turkish drones over ranges of up to 300 km.<sup>13</sup> This quick and effective counter to unmanned airborne platforms demonstrated their vulnerability to electronic warfare. Clearly,

electronic warfare will be applied to satellites should they become a threat as well, but unlike air-breathing drones, they are not immediately vulnerable to physics. The targeting picture against satellites will also be far more complex with various foreign and commercial platforms passing overhead simultaneously, which may or may not be aiding an adversary. Finally, within the conflict zone, the warring parties were able to declare a no-fly zone. This ability—not possible in orbit—greatly aided their capacity to identify and track potential hostile targets.<sup>14</sup>

The exact particulars of any one conflict are never repeated, as circumstances, terrain, and technology are constantly evolving. However, one can draw several predictions from Nagorno-Karabakh on how more capable opponents will fight in the future. First, the larger lesson from this conflict is that the vast majority of combat losses in nation-state conflict continue to come from indirect fire and other long-range weapon systems.<sup>15</sup> Second, the ability to accurately track and target your opponent is critical to the effectiveness of these systems, so the side that has the better intelligence will be able to eliminate its opponent faster. Finally, preventing your opponent from saturating the battlespace with sensors—whether drones or other unmanned systems—will be a critical priority for the defender. In sum, the side that can best fuse intelligence with long-range precision fires will dominate the battlefield.

The role of real-time intelligence from remote sensing satellites in a future conflict will be akin to that of drones in gathering targeting intelligence for Azerbaijan. The proliferation of commercial and national remote sensing capabilities to image broad areas in detail and relay that information back to fire direction centers will be a new critical node in the kill chain. Commercial providers are already working on real-time tasking and response from satellites.<sup>16</sup> Purpose-built national efforts like the Space Development Agency's tracking and transport layer will surely be even more capable than commercial systems and critical to tactical success on the future battlefield.<sup>17</sup> The ever-decreasing spatial and temporal resolution of remote sensing satellites will bring space-based intelligence forward from its use as a historically strategic-level tool to a tactical tool. Mitigating this shift will require a mixture of active, passive, regulatory, and diplomatic tools.

## **Approaches and Options**

The effect of a resolution convergence on military operations will become impossible to ignore over the next decade. As space-based remote sensing platforms transition from primarily an intelligence risk to a real-

time operational risk to military forces, effective methods of managing these systems will be necessary. Active military means of targeting remote sensing satellites will be a key future element of managing this threat. Already, Russia and China are developing ground-based laser systems designed to counter remote sensing systems in lower orbits.<sup>18</sup> These systems will likely be an effective counter to an opponent's remote sensing platforms. Nevertheless, the threat picture in orbit is much more politically complex than in an airborne environment. The nature of orbital mechanics means that remote sensing platforms from dozens of nations and commercial entities will transit any conflict zone daily. For relatively diplomatically isolated nations, such as Russia or China, engaging every satellite not belonging to a direct ally using active military means will be a real possibility. However, a less diplomatically isolated nation like the US—which historically prides itself on its alliances and generally adheres to international law—will find it much more difficult to engage in indiscriminate use of active military means. As a result, a much more nuanced approach to managing the satellite threat that mixes novel diplomatic and regulatory measures with active military means is needed. Discussed next are existing and potential new approaches to managing the threat outside of active military means.

Active measures are needed against adversary remote sensing systems, but they should be a last resort against domestic commercial systems or those owned by third parties. These systems still represent an operational threat since the imagery they capture can become publicly available or accessible for purchase and give an adversary valuable intelligence. In situations where the adversary nation has no significant domestic remote sensing capability, the active measures discussed above are largely unnecessary. Instead, a combination of regulatory and diplomatic options becomes the primary method of limiting the distribution of valuable overhead intelligence.<sup>19</sup> Currently, the US has the largest commercial remote sensing market and is likely to continue to lead the market due to an increasingly friendly regulatory structure, a robust industrial base, and lucrative government contracts. The remaining global commercial market will likely remain concentrated in close US allied and partner countries. Thus, the US is presented with particular difficulties in managing these remote sensing threats because using active military measures against domestic or allied commercial systems is not a politically palatable option. However, it is possible to use the US regulatory structure and other methods to control domestic commercial remote sensing. Also, diplomatic measures accompanied by reciprocal agreements and international notifications could be

an effective control measure for allied and third-party systems. A combination of these regulatory and diplomatic controls could be effective complements to military means of controlling remote sensing intelligence, limiting the inadvertent operational and intelligence risk that these systems represent.

### ***US Commercial Remote Sensing Systems***

**Regulatory controls.** US regulation of commercial remote sensing systems began in 1984 with the passage of the Land Remote Sensing Commercialization Act.<sup>20</sup> This act was primarily intended to privatize the Landsat program, but it also included provisions to allow the secretary of commerce to issue licenses for commercial remote sensing satellites. The Department of Commerce quickly delegated this authority to the National Oceanic and Atmospheric Administration (NOAA), where it has remained.<sup>21</sup> While the 1984 act was far from perfect, it established a framework for licensing commercial remote sensing systems and included many of the philosophical underpinnings of the current law. The 1984 act was superseded in 1992 by the Land Remote Sensing Policy Act, which removed some of the more egregious licensing conditions, including the ability of the secretary of commerce to “terminate, modify, condition, transfer, or suspend licenses” without any legal recourse for the licensee.<sup>22</sup> Included without substantive change in an updated 2010 National and Commercial Space Programs legislation, the 1992 act remains the foundational legal basis of US remote sensing licensing.

The basic tenants of the 1992 remote sensing act are relatively benign but do include several national security caveats. As part of the law, a US licensed commercial operator must employ “the system in such a manner as to preserve the national security of the United States and to observe the international obligations of the United States.”<sup>23</sup> Further, a licensee is required to inform the secretary whenever entering into any agreement “with a foreign nation, entity, or consortium involving foreign nations or entities.”<sup>24</sup> Other basic requirements include providing the orbital characteristics of the system, satisfactorily disposing of the satellite, and informing the secretary of any deviations to its orbit. At the surface level, it seems reasonable to request that a commercial provider comply with these requirements due to the US’s international obligations concerning debris tracking and national security. Where ambiguity quickly presents itself is with what is meant by the requirement to operate in a manner that preserves national security. Commercial providers and various government

agencies are very likely to have different interpretations of what constitutes protecting national security.

The Planet imagery example mentioned earlier illustrates this conflict of interest and opinion. Using these images, Iran could judge the effectiveness of its targeting systems and the impact of its strikes on specific targets on al-Assad—a clear national security risk. Alternatively, the rapid release of detailed imagery into the public sphere allowed the American people and the international community to independently determine that the number of missile strikes and the amount of damage was limited. This information served to calm media speculation and support the narrative that the missile strike was merely a face-saving exercise for Iran—a clear national security gain.<sup>25</sup> Planet's release of imagery could then have different national security interpretations depending on perspective and subsequent actions. In this case, Iran did not conduct follow-up strikes. Thus, in hindsight, Planet's release of imagery did not harm national security. This case demonstrates the ambiguity behind the seemingly straightforward requirement to preserve the national security of the US levied on commercial imagery providers.

If the US government had chosen to exercise regulatory control over Planet and restrict the release of its imagery, the regulatory options are limited. Presidential Decision Directive 23 (PDD-23), signed by President Bill Clinton in 1994, introduced the concept of modified operations colloquially known as “shutter control.” PDD-23 stipulated that commercial imagery providers might be required “during periods when national security . . . may be compromised, as defined by the Secretary of Defense or the Secretary of State, respectively, to limit data collection and/or distribution by the system to the extent necessitated by the given situation.”<sup>26</sup> Shutter control is a powerful regulatory tool that the US government could enact to prevent US licensed commercial providers from imaging everything from an individual air base to an entire theater of military operations. However, despite its usefulness as a regulatory tool, shutter control has never been invoked.

**Challenges of implementing regulatory controls.** The challenges of enforcing shutter control have likely prevented its implementation. First, doing so would almost certainly trigger a legal challenge. A legal challenge would probably not come from the licensed satellite owner. Instead, it would likely emerge from news agencies or other entities seeking access to the denied imagery—unless there was broad consensus that the justification for invoking shutter control demonstrably supported national security. As in the Planet example, proving the requirement for shutter control

is difficult under even the most seemingly clear-cut circumstances. Second, the use of shutter control could have long-term repercussions on the health of the US commercial remote sensing industry. It would demonstrate the vulnerability of US-licensed providers to government interference, potentially making the US a less attractive licensing environment.

Logistical challenges also present obstacles to invoking and verifying the effective execution of shutter control. With the growing number of remote sensing license holders in the US, active verification of compliance is not reasonably possible. The government would effectively be reliant on voluntary compliance from license holders. Given that the civil penalty cap the secretary of commerce can impose on an imagery provider for violating the terms of its license is only \$10,000, a licensee might simply decide that the cost of compliance is more than the price of the punishment.<sup>27</sup> A provider could also maliciously conclude that the value of the shutter-controlled imagery is worth much more than the fine and sell it despite the government order. This scenario is possible, though doubtful, despite the relatively low civil penalty. The US government is the largest single purchaser of commercial satellite imagery with the EnhancedView contract with the US National Reconnaissance Office (NRO) alone worth \$300 million per year for Maxar technologies.<sup>28</sup> In an industry with an estimated global revenue of just \$2.2 billion, US-based imagery providers are unlikely to risk the possibility of lucrative future contracts with the US government by intentionally ignoring shutter control requests.<sup>29</sup>

A final obstacle to invoking shutter control is a recently released regulatory structure that does not explicitly require that all US-licensed remote sensing providers be subject to shutter control. This new regulation, the first revision since 2006, relies on a tiering structure determined primarily by foreign availability benchmarks.<sup>30</sup> Under this regulation, if a remote sensing capability is marketed for purchase from any foreign supplier, it is considered available. The US provider is then placed in the lowest of three possible regulatory categories, tier one. Within tier one, remote sensing providers are still required to operate their systems “to preserve the national security of the United States,” but they are not subject to shutter control.<sup>31</sup> If a remote sensing capability is common only to other US-licensed providers or is unique, it is placed in tier two or tier three, respectively. As foreign availability grows, a larger percentage of highly capable remote sensing systems will no longer be subject to shutter control directives. The secretary of defense can still overrule the availability determination based on national security concerns, but exercising this authority will likely be difficult and rare given the political implications.<sup>32</sup> Despite these



regulatory restrictions on shutter control, it remains in law as a capability that the US can invoke, though the new regulatory structure will make its broad implementation extremely difficult. Even so, shutter control is a powerful regulatory tool for controlling domestically licensed remote sensing systems, but an alternative approach is necessary for foreign commercial systems.

### ***Foreign Commercial Remote Sensing Systems***

Foreign commercial remote sensing systems are categorized as allied, third party, or partly adversary owned—with each requiring a slightly different approach.

**Allied commercial systems.** Allied systems can be addressed through diplomatic channels. However, the degree of control that allied countries have over their remote sensing industry varies, and any request would have to be matched by restrictions on US commercial companies. Canada is an example of a nation with remote sensing regulations that closely mirror those of the US, including a provision that the minister of defense can “interrupt or restrict” the operations of a licensee on national security grounds.<sup>33</sup> This language is essentially mirrored in US law, which grants the secretary of defense the ability to direct modified operations (shutter control) of US licensees. With its regulatory structure, Canada, as a close ally of the US, would be receptive to and capable of limiting the operations of its satellites upon request using its similar regulatory mechanisms. However, it would certainly expect reciprocal restrictions on US systems. While Canada uses the same basic approach to security as the US, with modified operations directives used at the discretion of the Defense Department, not all Western nations take the same regulatory approach.

Germany takes a different approach to remote sensing regulation than either the US or Canada. German law for remote sensing platforms is sensitive to the possible use of German commercial imagery for military purposes and its impact on domestic security and foreign policy. The country's regulations require licensed operators to conduct a sensitivity check of all data transactions against a government database, taking into account data quality, target area, and the individual making the request.<sup>34</sup> Transaction controls avoid the complexities of attempting to regulate the technical aspects of remote sensing systems as the US has done and instead focuses on controlling the product. This control by the German government would allow for a quick response if it judged a request by a foreign government to limit the release of imagery to be valid. Since German remote sensing law is intended to support the national commitment to peace and is sensitive to

endangering foreign security interests, Germany would likely be among the most receptive nations to diplomatic requests to limit imagery distribution. Alongside France, Germany is one of just two European Union (EU) members with an overarching national policy governing remote sensing.

Managing the remote sensing security threat through diplomatic means with the broader European Union presents a more challenging problem than with Germany or France. Outside of the US, the member states of the European Union collectively have the largest commercial and privatized remote sensing market, with some smaller members such as Finland possessing highly capable commercial providers. Remote sensing companies based in these less-regulated EU member states present a much more difficult challenge since the EU does not have clear overarching policies governing remote sensing. The lack of an EU-wide regulatory mechanism for controlling the release of satellite imagery to protect domestic or foreign national security is problematic. Even if the nation receiving the diplomatic overture accepts a request as valid, it may find it legally impossible to impose any sort of limiting controls on the providers based within their borders. If allied nations lack an adequate regulatory framework or the legal authority to prevent their commercial providers from releasing imagery, then individual providers must be treated in the same manner as third-party commercial systems.

**Third-party commercial systems.** The second category of foreign commercial remote sensing systems is third-party commercial systems. They present a challenge for any nation attempting to deny observation of military operations. Unlike products from third-party national systems—which are unlikely to be shared outside the owning government due to concerns over revealing capabilities and limitations—commercial providers operating from neutral nations will likely consider hostilities between other nations as an opportunity. Operationally this means that they are just as much a threat as adversary systems, but active measures cannot be used against them without a careful assessment of the risk of angering the host nation. Diplomatic overtures would seem to be the best approach and certainly a necessary step in limiting the release of data from third parties, but alone they are unlikely to be effective or timely. Neutral nations may be slow in responding to diplomatic overtures for innocent or malicious reasons. Once hostilities have begun, the normally slow pace of the diplomatic process will likely create unacceptable risk. Historically, the US has successfully applied this diplomatic approach just once before, and it is unlikely to work again. This was during the Gulf War when the United Nations, at US urging, mandated an embargo on satellite imagery sales to

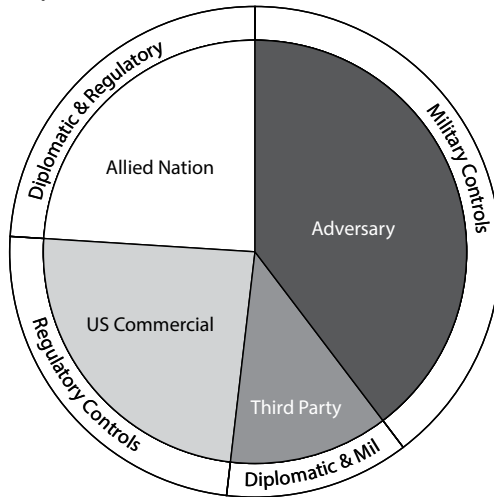
Iraq.<sup>35</sup> The only available non-US imagery was from France's SPOT satellite, and the agreement required SPOT to forgo sales to media companies to avoid the inadvertent release of imagery to Iraq through third parties. SPOT had a relatively low 10-meter resolution at the time but could still have provided valuable overhead intelligence to the Iraqi government, which also had lost access to aerial reconnaissance.<sup>36</sup> This embargo on the sale of imagery to Iraq worked and allowed the US to successfully execute the "left hook" maneuver that outflanked and surprised the Iraqi Army.

Replicating the same diplomatic embargo would be orders of magnitude more difficult today than it was in 1990. At that time, only a single close ally had a commercial capability that presented a threat. The threat today is proliferated across many nations, with imagery commercially available from most major US allies, third parties, and potential US adversary China.<sup>37</sup> It is doubtful that in the future the US could successfully request a United Nations embargo or that it could be enforced with the same degree of success achieved during the Gulf War. An alternative to negotiations is to develop a mechanism that provides notice yet is quick and effective at warning operators that imaging of specified areas is not authorized and would risk damaging or interfering with the imaging satellite. Aviation notices to Airmen (NOTAM) offer a possible framework for how this mechanism could effectively function.

NOTAMs provide aircraft with information in an internationally recognized format warning of hazards or airspace restrictions. They are an outgrowth of the Convention on International Civil Aviation hosted by the US in 1944 that established international guidelines for civil aviation. The convention does not apply to military aircraft, but the resulting regulatory mechanisms and processes are generally adhered to by military aviation during normal operations. Among the guidelines in the convention is an understanding that civil aircraft operating for non-civil purposes in the airspace of a nation may be dealt with by "any appropriate means."<sup>38</sup> It is a stretch to translate this understanding and its meaning into the space domain. Still, a similar agreement applied to space systems could provide the legal framework for nations to interfere with the operations of third-party commercial satellites, which become threats to security when transiting over sovereign territory. For military operations outside of sovereign territory, which is more likely for the US, the NOTAMs mechanism could simply provide clear and unambiguous warning that third-party systems should not image an area. Systems that violate this notice by pointing their optics at Earth in these areas may be damaged by active

directed-energy weapon systems or, in the case of SAR systems, may be actively interfered with if they are detected radiating energy.

**Adversaries with an ownership stake.** Commercial systems that an adversary has a significant ownership stake comprise the third category of commercial systems that might necessitate a diplomatic or regulatory approach. This category is not as clear-cut as it first seems. The international consortiums that operate many commercial systems may be partially owned by companies based in the territory of both sides in a conflict. Multiparty ownership creates an added difficulty for determining the degree of aggressiveness in managing these satellites. Some commercial providers will be based in an adversary's territory and have contracts with their host government, making them equivalent to adversary national assets. For other commercial systems, the threshold for treatment as an adversary system is difficult to discern. Determining a threshold for designation as an adversary-controlled system will ultimately require a judgment call at the national level, which balances the diplomatic risk against the operational risk of taking active measures. Figure 1 summarizes approaches to allied, third-party, adversary, and US commercial satellite remote sensing systems.



**Figure 1. Approaches to remote sensing.** Each remote sensing satellite will need to be managed broadly by category.

### *A New Approach to Mitigating Third-Party Threats*

Diplomatic and regulatory approaches to controlling the release of remote sensing data are a necessary complement to active and passive military measures (table 1). However, no simple solution exists to mitigate the operational risk from non-adversary remote sensing satellites. Diplomatic

means are the best approach with allied commercial systems, while third-party systems may require a more aggressive approach. Further, complexities in determining the risk posed by commercial systems, as well as by assigning ownership, present a formidable challenge. Cutting through the complexity by developing and exercising a NOTAM-type mechanism—in this case, a notice to Spacemen (NOTSM)—to protect sensitive military operations is the most straightforward approach, but it requires enforcement. This enforcement requires dedicated on-site assets capable of tracking and engaging any ISR asset transiting overhead with destructive and nondestructive effects. A comprehensive and intensive multipart strategy that includes both diplomatic and active measures is a challenging but necessary part of limiting the impact that non-adversary remote sensing can have on military operations.

		Level of War		
		<i>Peacetime</i>	<i>Tension</i>	<i>Conflict</i>
Satellite Owner	<i>Adversary national and commercial</i>	Passive measures (denial and targeted deception)	Increased passive measures (denial and targeted deception)  Dazzling plus limited nondestructive interference	Nondestructive: cyberattacks, jamming of links  Destructive: lasers, ASATs and other space weapons
	<i>Third party</i>	Passive measures (denial)	NOTAMs and diplomatic efforts	NOTAMs escalating to dazzling and nondestructive attacks
	<i>Allied national and commercial</i>	Passive measures (denial)  Shared regulatory controls	Diplomatic efforts	Continued diplomatic efforts, NOTAMs escalating to nondestructive in the event of serious security violation
	<i>US Commercial</i>	Regulatory limitations on highly capable systems plus passive measures	Shutter control	Shutter control

**Table 1. Methods of control.** Example measures that can be applied across the spectrum of conflict to control remote sensing. Note that measures build from right to left, though that does not mean that peacetime control measures should cease in conflict.

## Conclusion

The near-ubiquitous space-based observation of Earth is coming and cannot be ignored by military planners. Already an intelligence threat, remote sensing satellites are rapidly developing into an operational threat

to military forces. Passive-only measures of managing the risk from remote sensing satellites will become increasingly ineffective unless accompanied by active measures to limit the observation of friendly forces, such as those capabilities that China and Russia are already developing.<sup>39</sup> Where and when to apply active measures is an increasingly complex problem requiring a careful balance of diplomatic and operational risks since not all remote sensing threats are necessarily adversary controlled. Thus, some require diplomatic or regulatory methods of control.

Only a handful of nations possess a clear regulatory framework for managing domestic remote sensing threats. The US regulatory structure for commercial systems is robust. Still, it has shifted away from relying primarily on system-level technical limitations toward reliance on shutter control and broad language governing national security as its regulatory control mechanism. As a regulatory mechanism, shutter control is, in theory, an efficient tool for protecting national security. However, it is one that the US has never exercised for fear of legal challenges or doing harm to its domestic remote sensing industry. For allied nations, a patchwork of regulatory controls exists, which those nations may be willing to enforce when asked through diplomatic channels.

Managing the threat is most difficult for third-party systems or for those unwilling to accommodate foreign security concerns. In these cases, a NOTAM/NOTSM concept may be necessary to prevent observation. The NOTSM concept allows for appropriate forewarning that imagery of a specified area is not welcome and attempts to image the area will be met with an active response. Such a concept currently has no legal framework to rely on and would need to be declared unilaterally or developed as a norm acceptable over sovereign territory or regions with active combat operations. Either way, active measures against non-adversary satellites would require careful analysis of the associated risk.

Remote sensing satellites in an era of ubiquitous imagery will provide an overwhelming military advantage to the side that is best able to leverage them for its own gain while denying its opponent access. Despite this seemingly obvious conclusion, there seems to be relatively little acknowledgment of the threat that these satellites will pose to operational forces in the future. Remote sensing satellites that historically promoted strategic stability by allowing clear observation inside an adversary's borders are quickly developing into a critical enabling tool for future warfare. Full recognition of the scale of the threat and the opportunity that these systems present may not come until a nation can successfully exploit its advantage in using and controlling space to rapidly defeat a near-peer mili-

tary power. When that day arrives, military space will truly have come of age as a war-fighting domain. **SSQ**

**LTC Brad Townsend, USA**

Colonel Townsend serves as a space policy advisor on the Joint Staff. He is the author of *Security and Stability in the New Space Age: The Orbital Security Dilemma* (Routledge Press, 2020). He holds a PhD and MPhil in military strategy from the US Air Force's Air University School of Advanced Air and Space Studies. A 2002 graduate of the US Military Academy, he also earned an MS in astronautical engineering from the Air Force Institute of Technology and an MS in space operations management from Webster University.

**Notes**

1. Geoff Brumfiel, "Satellite Photos Reveal Extent of Damage from Iranian Strike on Air Base in Iraq," NPR, 8 January 2020, <https://www.npr.org/>.
2. Diana Stancy Correll and Aaron Mehta, "See the Damage at Al-Asad Airbase Following Iranian Missile Strike," *Military Times*, 8 January 2020, <https://www.militarytimes.com/>.
3. Jon B. Christopherson, Shankar N. Ramasari Chandra, and Joel Q. Quanbeck, *2019 Joint Agency Commercial Imagery Evaluation—Land Remote Sensing Satellite Compendium* (Reston, VA: US Geological Survey, 2019), 41–43, <https://pubs.usgs.gov/>.
4. *Temporal resolution* refers to the amount of time required for a satellite or constellation to revisit a specific point on Earth's surface. For example, a satellite that passes over the same place once each day would have a temporal resolution of 24 hours. In contrast, two satellites in a constellation that each pass over the same spot once each day but 12 hours apart would have a temporal resolution of 12 hours. *Spatial resolution* refers to the quality of an image and for electro-optical imagery is synonymous with ground sample distance (GSD) or the midpoint of two adjacent pixels on a sensor when projected onto the ground. Spatial resolution is a broader term, as it also captures synthetic aperture radar technology and post-processing techniques to capture the best "picture quality" of a sensor.
5. Debra Werner, "WorldView-4's Long Road to Launch about to Pay Off for DigitalGlobe," *SpaceNews Magazine*, 15 August 2016, <http://www.spacenewsmag.com/>.
6. "DigitalGlobe Loses WorldView-4 Satellite to Gyro Failure," *SpaceNews*, 7 January 2019, <https://spacenews.com/>.
7. "WorldView-3 Satellite Sensor," Satellite Imaging Corp, accessed 19 January 2020, <https://www.satimagingcorp.com/>.
8. Robbie Schingler, "Planet Launches Satellite Constellation to Image the Whole Planet Daily," 14 February 2017, <https://www.planet.com/>.
9. Gustav Gressel, "Military Lessons from Nagorno-Karabakh: Reason for Europe to Worry," European Council on Foreign Relations, 24 November 2020, <https://ecfr.eu/>.
10. Michael Kofman, "Perspectives | Armenia's Military Position in Nagorno-Karabakh Grows Precarious," Eurasianet, 24 October 2020, <https://eurasianet.org/>.
11. Robyn Dixon, "Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh — and Showed Future of Warfare," *Washington Post*, 11 November 2020, <https://www.washingtonpost.com/>.
12. Dixon.

13. "Russia Shot-Down A Total of Nine Turkish Bayraktar Drones Near Its Armenian Military Base — Russian Media Reports," *Eurasian Times*, 21 October 2020, <https://eurasianimes.com/>.
14. "Armenia Declares No-Fly Zone in Armenia and Nagorno-Karabakh," Reuters, 12 November 2020, <https://www.reuters.com/>.
15. Gressel, "Military Lessons from Nagorno-Karabakh."
16. Debra Werner, "Capella Sends First Task Order through Inmarsat Data Relay," *Space News*, 23 November 2020, <https://spacenews.com/>.
17. Space Development Agency, "Transport," accessed 19 July 2021, <https://www.sda.mil/>.
18. Defense Intelligence Agency, *Challenges to Security in Space*, (Washington, DC: Defense Intelligence Agency, January 2019), 20, 29, <https://www.dia.mil/>.
19. There is risk that nations opposed to US actions will provide a disadvantaged opponent with imagery from national level systems. This risk is mitigated by the fact that nations are hesitant to provide third parties access to raw imagery and reveal national capabilities (and limitations) and by the time that making a decision to release even blurred imagery or intelligence to a third party requires. These practical limitations prevent this source of imagery from being a real-time operational threat but does present challenges from an intelligence perspective.
20. Land Remote-Sensing Commercialization Act of 1984, Pub. L. No. 98-365, 15 USC 4201 (1984).
21. Dorinda Dalmeyer and Kosta Tsipis, "USAS: Civilian Uses of Near-Earth Space," *Heaven and Earth* 16 (1997): 47.
22. Land Remote-Sensing Commercialization Act of 1984, sec. 403a(1).
23. Land Remote-Sensing Act of 1992, Pub. L. No. 102-588, 15 USC 5623 (1992), sec. 5622(b)1.
24. Land Remote-Sensing Act of 1992, sec. 5622(b)6.
25. Shane Harris et al., "‘Launch, Launch, Launch’: Inside the Trump Administration as the Iranian Missiles Began to Fall," *Washington Post*, 8 January 2020, <https://www.washingtonpost.com/>.
26. William J. Clinton, Presidential Decision Directive 23, "US Policy on Foreign Access to Remote Sensing Space Capabilities," 9 March 1994, Clinton Digital Library, <https://clinton.presidentiallibraries.us/>.
27. "Licensing of Private Land Remote-Sensing Space Systems," 15 CFR 960, Vol. 71, No. 79 § (2006), pt. 960.15.
28. Theresa Hitchens, "NGA Re-Ups Maxar Imagery Contract," *Breaking Defense*, 28 August 2019, <https://breakingdefense.com/>.
29. "Commercial Satellite Imaging Market Statistics, Trends | Forecast - 2026," Allied Market Research, accessed 5 May 2020, <https://www.alliedmarketresearch.com/>.
30. Licensing of Private Remote Sensing Space Systems, 15 CFR 960 (2020), Cornell Law School, <https://www.law.cornell.edu/>.
31. 15 CFR 960, sec. 960.8.
32. 15 CFR 960, sec. 960.6a.
33. Remote Sensing Space Systems Act (Canada), SC 2005, c. 45, sec. 14(5), <https://laws-lois.justice.gc.ca/>.
34. "National Data Security Policy for Space-Based Earth Remote Sensing Systems," Background Information for the Act on Satellite Data Security, Bonn, German Federal



Ministry of Economics and Technology, 15 April 2008, 5, <https://www.bmwi.de/>. Effective 1 December 2007.

35. Denette L. Sleeth, "Commercial Imagery Satellite Threat: How Can U.S. Forces Protect Themselves?" (master's thesis, Naval War College, 2004), 12.

36. "SPOT Medium Resolution Satellite Imagery," Apollo Mapping, accessed July 2021, <https://apollomapping.com/>.

37. Shankar N. Ramaseri Chandra, Jon B. Christopherson, and Kimberly A. Casey, 2020 *Joint Agency Commercial Imagery Evaluation—Remote Sensing Satellite Compendium*, US Geological Survey (USGS) Circular 1468, ver. 1.1 (Reston, VA: USGS, October 2020), <https://doi.org/10.3133/cir1468>.

38. *Convention on International Civil Aviation*, doc. 7300/9, 9th ed. (Montreal: International Civil Aviation Organization, 2006), 3, <https://www.icao.int/>.

39. Defense Intelligence Agency, *Challenges to Security in Space*, 20.

# Arctic Space Strategy: The US and Norwegian Common Interest and Strategic Effort

LT COL KJETIL BJØRKUM, ROYAL NORWEGIAN AIR FORCE

## Abstract

The US and Norway are Arctic and space nations and members of the NATO alliance. The increased strategic significance of the Arctic due to the retreating ice presents challenges best solved by elevated space capabilities. Both nations will gain from greater cooperation regarding the Arctic as a region and space as a domain. Areas of collaboration should include space domain awareness; communication capacity; intelligence, surveillance, and reconnaissance; launch capability; and education, research, and technology development. An improved combined Arctic space strategy for both nations with an immediate focus on shared knowledge and understanding through education and liaising will increase cooperation and effectiveness at a low cost.

\*\*\*\*\*

The Arctic region has historically been a remote, unfriendly area where only the most eager hunters, explorers, and scientists have shown any interest. Climate change and the following increased temperatures in the last 10 to 20 years have changed the Arctic's characteristics. The Arctic region is still a harsh environment not suitable for regular human settlement and operations. However, resources previously inaccessible are now readily available due to the melting ice. Formerly unusable sea lines of communication are now open and free of ice for extended periods of the year. Many nations see the opportunities the melting ice brings in the Arctic. China and Russia have declared their interests in the new possibilities regarding resources in the area and have increased their presence commercially and militarily. The Arctic has become an area of strategic competition and increased global strategic significance but lacks the basic infrastructure to be controlled and exploited safely and securely.

The Arctic's harsh environment and weather conditions limit the region's settlements and infrastructure. Space will play a unique role in pro-

viding the necessary means to control and secure operations in the Arctic for commercial, civil, and military activity for all stakeholders. As an Arctic nation, Norway has learned to live, function, and thrive in the region. The nation has played a significant strategic role for NATO due to its northern geography and proximity to the Russian Northern Fleet's operating area. As the most prominent member of the NATO alliance and an Arctic nation, the US has emphasized Norway's crucial geostrategic position. The increased activity and access to the Arctic region further increase Norway's global strategic importance. Norway should continue to have a key role in US Arctic strategy because the two nations have an equal interest in the region. Both nations have specific knowledge and technology to bring to the cooperation, and enhanced space capabilities will increase security to operate in the region for both.

This article first investigates what makes the Arctic an increasingly important area for many stakeholders and, more specifically, China's and Russia's interests. Next, it explores US, Norwegian, and NATO strategies for the Arctic and space while emphasizing coinciding focus areas. Finally, it examines areas for cooperation—some already in play and some for the future—and suggests focus areas for the US and Norwegian Arctic space strategies.

### **Significance of the Arctic**

The Arctic is the cold and remote wasteland north of the 66.3° north latitude, commonly referred to as the Arctic Circle.<sup>1</sup> The United Nations Convention on the Law of the Sea defines the Arctic Five, the nations with an Arctic coastal area and an exclusive economic zone (EEZ) extending into the region.<sup>2</sup> They include Russia, Canada, Denmark (Greenland), Norway, and the US (Alaska).<sup>3</sup> Iceland, Sweden, and Finland are also considered Arctic nations but do not have an Arctic coastal area. These eight nations constitute the members of the Arctic Council and have special interests in the Arctic.<sup>4</sup> The region's considerable economic value in oil and gas resources, fisheries, and minerals make it of interest to many nations beyond the Arctic Council.<sup>5</sup>

These resources have long been unavailable for exploitation due to ice coverage, but their growing accessibility brought on by climate change is making the Arctic even more valuable. Surveys estimate that 13 percent of the world's undiscovered oil reserves and 30 percent of undiscovered gas reserves reside in the Arctic.<sup>6</sup> Until recently, the Arctic's minerals, oil, and natural gas liquids have been inaccessible due to harsh conditions. However, the declining Arctic ice has opened up access to areas where

these resources are located, and more extensive sea areas for fisheries are now reachable.<sup>7</sup> Also, the retreating ice opens up previously closed sea lines of communication.

The Northwest Passage and the Northern Sea Route are open for more extended periods, transporting merchandise from the Pacific to the Atlantic free from piracy activity and faster than the traditional routes through the Suez or Panama Canal.<sup>8</sup> At the same time, the increasing availability of resources presents several problems.<sup>9</sup> Although most disagreements regarding maritime boundaries have been resolved peacefully, a more “complicated disagreement involves the North Pole itself.”<sup>10</sup> Canada, Denmark (Greenland), and Russia claim ownership of the Lomonosov Ridge, an underwater ridgeline that extends well into the central Arctic.<sup>11</sup> The issue is unsettled and a possible source of conflict—but it has been solely a diplomatic one.<sup>12</sup> Naturally, as Arctic nations, Russia and the US are interested in the Arctic region due to its resources and vital strategic points. The increased potential for economic gain and military-strategic advantage has made the Arctic an arena for strategic competition and has led to an increased military, civil, and commercial presence from both nations. In particular, Russia has “gradually reintroduced army, navy and air force elements into the region,” expanding its military footprint in the Arctic.<sup>13</sup>

Russia is the only nation in the Arctic Council that is not a NATO member or partner.<sup>14</sup> Russia has the largest Arctic population, with more than 2 million citizens living north of the Arctic Circle.<sup>15</sup> Russia also generates 22–30 percent of its gross national product (GNP) from the Arctic.<sup>16</sup> Because of the melting ice and changing Arctic environment, Russia is “optimistic about the potential for Siberia and the Russian Far East” to significantly boost the nation’s economy.<sup>17</sup> Energy projects and faster shipping between Asia and Europe because of the Northern Sea Route will increase the need for supporting ports and infrastructure. Building and maintaining this infrastructure will be a potentially positive economic revenue for the nation.<sup>18</sup> The economic potential has intensified Russia’s interest in protecting its Arctic assets through a heightened military presence. Signs of this interest include Russia’s reopening of abandoned military installations and more “incursions by Russian aircraft and submarines into or close to other [nations’] Arctic spaces.”<sup>19</sup> The planting of a Russian metal flag under the ice at the North Pole by a Russian submarine crew in 2007 shows that a greater military presence may have a secondary purpose.<sup>20</sup> President Putin has demonstrated a will to use illegal aggression and violate international law to seize territory in Europe.<sup>21</sup> Russia may

intend to contest the economically and strategically important region and likely make claims for ownership and economic rights in the Arctic that extend beyond the 200-nautical-mile EEZ. Similarly, China has shown increased interest in the Arctic region.

An exciting aspect of the Arctic and strategic competition is China's claim to be a near-Arctic state.<sup>22</sup> China's 2018 Arctic strategy outlines a "Polar Silk Road economic plan."<sup>23</sup> China sees the shorter distance from China to Europe through the Northern Route as a possible "economic boom."<sup>24</sup> It has also invested heavily in energy projects in Russia and does not hide its desire to access Arctic natural resources.<sup>25</sup> China's investments in ports, airports, research stations, and satellite ground stations are reasons to raise concerns about its intentions in the "autonomous territory" of the Arctic.<sup>26</sup> China is also developing a "constellation of twenty-four polar observation satellites."<sup>27</sup> The first satellite, launched in September 2019, has already delivered over 2,500 pictures covering the Arctic and Antarctic.<sup>28</sup> China's increased activity and interest in the Arctic confirms the Arctic as a new ground for strategic competition between Russia, China, and the US.

The Arctic has risen as a new arena for strategic competition and a region of increased interest for other stakeholders with economic motives. The unfortunate consequences of its environmental changes are a potential increase in natural resource exploitation and new transportation lines. This new paradigm affects commercial, civil, and military operations and has increased the strategic value of all Arctic and near-Arctic countries.

The corresponding threats to the area are significant. In fragile regions like the Arctic, an accident from oil drilling or shipping would have dire consequences. Continued environmental change might also impact the wildlife and fisheries in the area, and further research and surveillance are critical. A conflict in the area leading to the use of arms may have the same effects. The vast amount of international waters and disputed rights to resources may lead to conflicts between Arctic nations and other stakeholders claiming their rights to exploit the region. Increased activity has "fueled a demand for communication, navigation, and surveillance infrastructures."<sup>29</sup> In the 2013 *National Strategy for the Arctic Region*, President Barack Obama recognized the Arctic as "an amazing place" where climate changes represent emerging opportunities and "very real challenges."<sup>30</sup> These challenges are multifaceted, and many of them fall under the purview of the Department of Defense.

## Arctic Strategies

### *US Arctic Strategy*

Since the US bought Alaska from Russia in 1867, it has been an Arctic nation and is currently one of the Arctic Five and a member of the Arctic Council.<sup>31</sup> In Alaska, permafrost dominates the northern third of the state, making regular settlements challenging.<sup>32</sup> Less than 68,000 Americans live in the Arctic, and Alaska produces only 0.3 percent of the US GNP.<sup>33</sup> Mineral production in Alaska constitutes about four percent of US mineral production.<sup>34</sup> Nevertheless, the Arctic is vital to US geostrategic interests.<sup>35</sup> As the Arctic as a “geostrategic buffer is eroding” and strategic competition in the area is increasing, the US needs a comprehensive US military strategy for the region.<sup>36</sup>

The DOD’s 2019 Arctic strategy expands on the complex security environment in the region. It recognizes the security threat emerging from increasing access to resources, an uncertain strategic environment, and the fragile but still enduring cooperation in the region.<sup>37</sup> The DOD established three main objectives for the Arctic: defend the homeland, compete when necessary to maintain favorable regional balances of power, and ensure common domains remain free and open.<sup>38</sup> The DOD acknowledges the Arctic as an increasingly vital region due to strategic competition and greater access to the region and its resources. This focus gives the Air and Space Forces a direction for an Arctic strategy.

The Department of the Air Force views the Arctic as “residing at the intersection between the U.S. homeland and two critical theaters, Indo-Pacific and Europe, [thus making] the Arctic . . . an increasingly vital region for U.S. national security interests.”<sup>39</sup> The Air Force’s *Arctic Strategy* also recognizes the “Arctic as a region of strategic opportunity for the Air and Space Forces, Joint Force, allies, and partners.”<sup>40</sup> The strategy builds around four lines of effort: maintaining vigilance through command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR); projecting power through bases in Alaska and Greenland; cooperating with allies and Arctic partners; and finally, preparing through training, research, and development.<sup>41</sup> Allied and partner cooperation is emphasized throughout the strategy. The strategy recognizes space as a solution for the challenges in the demanding Arctic operating environment. The Space Force must overcome the region’s unique orbital and electro-magnetic obstacles that negatively affect all communication and navigational signals.<sup>42</sup>

### ***Norway's Arctic Strategy***

As one of the eight nations in the Arctic Council and one of the five nations with an Arctic coastline, Norway has extensive interests in the Arctic. Approximately 10 percent of its population—a greater proportion than any other Arctic country—or half a million Norwegians live north of the Arctic Circle.<sup>43</sup> Key industries in North Norway such as fisheries, aquaculture, and tourism depend on natural resources.<sup>44</sup> It is estimated that more than half of Norway's undiscovered oil resources are in the Arctic region.<sup>45</sup> The Norwegian political vision for North Norway and the Arctic region is economic, environmental, and social sustainability.<sup>46</sup> Arctic policy goals focus on international cooperation and international legal order to achieve peace, stability, predictability, value creation, and ecosystem-based management.<sup>47</sup> The five priority areas in the Arctic strategy are international cooperation, knowledge development, infrastructure, environmental protection and emergency preparedness, and business development.<sup>48</sup> These priorities are essential for the development in the Arctic region and coincide with US policy and strategy for the region. Due to the Gulf Stream, Norway is ice-free in the summer and has no permafrost. Without the Gulf Stream, the average temperature in Norway would be 10 to 15 degrees Celsius colder.<sup>49</sup> Although the latitude is similar to Alaska's, Norway's climate is friendlier to human activity.

### ***NATO's Arctic Strategy***

NATO also understands the Arctic's strategic importance, particularly in light of environmental changes, but has failed to develop an Arctic strategy that incorporates the Arctic's unique challenges. The rapidity of change “suggests the Arctic is likely to be one of the twenty-first century's most contested areas.”<sup>50</sup> The current strategic concept of NATO is “active engagement, modern defense.”<sup>51</sup> Collective defense, crisis management, and cooperative security are core tasks, and deterrence “remains a core element” of NATO's strategy.<sup>52</sup> In developing an Arctic strategy (excepting the operational plan), “NATO lags significantly behind” Russia and China.<sup>53</sup> An increased Russian military presence and Russia's enhanced weapons available for anti-access and area denial (A2/AD) in the gap from Greenland to Iceland to the United Kingdom (GIUK) and north-bound represent a major strategic problem for some of the alliance's Arctic members.<sup>54</sup> Unfortunately, not all NATO nations, and not even all NATO Arctic nations, have the same viewpoint.<sup>55</sup> An intensified focus on the Arctic from the US and Norway may shift NATO's focus toward the

north. However, currently, there is no NATO Arctic strategy other than deterrence and cooperative security.

## **The Significance of Space as the Solution**

The obvious solution to the unique infrastructure challenges in the Arctic is space.<sup>56</sup> Commercial satellite services can support the need for increased communications, surveillance, and understanding of events in the region while also increasing cooperation between nations and partners. The use of space assets and space-based infrastructure is not without challenges. However, by “optimizing existing and future space-based infrastructure, using low Earth, geosynchronous, and highly elliptical orbits, the United States can work cooperatively with other Arctic nations to build situational awareness, enhance operations, and strengthen a common rule-based order.”<sup>57</sup> Continued research and information sharing in a region formerly neglected due to the harsh environment should be the preferred measure to solve these issues.

## **Space Strategies**

### ***US Space Strategy***

The 2020 *National Space Policy of the United States of America* declares that “the United States will continue to use space for the nation’s security and our allies,” continuing the high focus on allied cooperation, involvement, and protection from the US Arctic strategy.<sup>58</sup> Among the many goals of the policy, “lead, encourage, and expand international cooperation,” and “preserve and expand United States leadership . . . [working] with like-minded international and private partners” also confirm this focus on allied and partner cooperation.<sup>59</sup> The policy explicitly calls for assured access to space; enhanced positioning, navigation, and timing (PNT); and the development of space professionals as foundational activities.<sup>60</sup> Furthermore, the policy defines national security guidelines. In addition to recognizing space as a war-fighting domain, it emphasizes “robust space domain awareness of all activities in space with the ability to characterize and attribute potentially threatening behavior” as an essential tool.<sup>61</sup> The policy focuses on “advanced technologies, capabilities, and concepts that anticipate and rapidly respond to changes in the threat environment and improve timeliness and quality of intelligence and data to support operations.” It also tries to “integrate cybersecurity into space operations and capabilities” and “collaborate with allies and partners actively engaging in space security and intelligence operations . . . for the exchange of relevant



space and space-related information.”<sup>62</sup> Additionally, this policy instructs the secretary of defense (SecDef) to defend the US and its allies, protect freedom of navigation, defend space assets while supporting joint operations, and use space to deter conflict and defeat aggression. Other SecDef responsibilities include providing affordable and timely space access; developing rapid launch options; detecting threatening space behavior; conducting strategic space posture reviews; and developing, acquiring, and operating space intelligence capability to support joint operations.<sup>63</sup> Allied cooperation and defense are vital to accomplishing these tasks. Likewise, the 2020 *Defense Space Strategy* emphasizes allied cooperation.

The *Defense Space Strategy* defines the objectives of “maintain[ing] space superiority; provid[ing] space support to national, joint, and combined operations; and ensur[ing] space stability.”<sup>64</sup> The space strategy defines some lines of effort: “build a comprehensive military advantage in space; integrate military spacepower into national, joint, and combined operations; shape the strategic environment; [and] cooperate with allies, partners, industry, and other U.S. Government departments and agencies.”<sup>65</sup> Some specific objectives are to improve intelligence and command and control capabilities; develop capabilities to counter the hostile use of space; integrate allies into plans; and expand cooperative research, development, and acquisition with allies and partners.<sup>66</sup> As with much of US military strategy, the document focuses on strategic competition with China. But the strategy also recognizes Russia as a threat. As the Arctic nation with the most citizens north of the Arctic Circle, Russia is also a threat to US security in the Arctic region extending into space.<sup>67</sup>

The *Department of the Air Force Arctic Strategy* notes that satellite communications and data links are major C3ISR improvements in the area while recognizing that space assets “reduce the need for a physical footprint in the demanding Arctic operation environment.”<sup>68</sup> Another high-focus topic in the strategy is “all-domain awareness” and the accompanying challenges of “unique orbital mechanics” and “electromagnetic obstacles” in the region.<sup>69</sup> The strategy also emphasizes allied cooperation, the development of new technology to “ensure access to and freedom to operate in space,” and the need to use space capabilities to “mitigate and predict environmental disturbances unique to the Arctic Region.”<sup>70</sup> Norway’s space strategy, like that of the US, emphasizes international cooperation.

## **Norway's Space Strategy**

Although Norway is not a large nation in geographical terms or population, it is an essential and experienced space nation. Situated as it is in the High North, Norway is an Arctic nation. It is a technologically developed nation that emphasizes research and development in many space-related areas.<sup>71</sup> Norway's space strategy, last updated in 2019, presents four goals for Norwegian space operations. These are promoting profitable businesses, growth, and employment; ensuring crucial needs for society and the population; ensuring adequate security for an essential space infrastructure; and securing Norwegian foreign policy, security, and defense policy activities and operations in space.<sup>72</sup> Prioritizing the user's end needs leads to multisector solutions requiring cooperation between government agencies, commercial interests, and international entities.<sup>73</sup> International cooperation is a key focus area for environmental surveillance, security and preparedness, research and education, and military use of space.<sup>74</sup> Bilateral agreements and commercial cooperation will enhance the Norwegian military's capacities.<sup>75</sup>

Norway's ambition to be the "NATO in the North" creates responsibilities to develop space-based services in the Arctic, an area of high strategic significance for Norway.<sup>76</sup> At the same time, Norway has ambitions of being independent in critical security sector services.<sup>77</sup> Due to its global dependence on space infrastructure, Norway's territory in the Arctic (e.g., Svalbard and Bjoernoeya) and Antarctic (e.g., Queen Maud's Land) increases its geostrategic significance.<sup>78</sup> As the Kongsberg Satellites Services' station SvalSat on Svalbard exemplifies, these areas are favorable for ground stations.<sup>79</sup> Norway will work in multilateral and bilateral processes to ensure Norwegian and allied security and freedom to use space.<sup>80</sup> Traditionally, the US and Norway have cooperated on space activities. One recent example is the Rimfax radar developed in Norway and carried by the *Perseverance* rover on Mars.<sup>81</sup>

The Norwegian Armed Forces Space Department was established in 2016 to integrate the space activities of Norway's armed forces in an operational domain.<sup>82</sup> The department will strengthen the strategic development, coordination, and leadership of military space operations.<sup>83</sup> The new long-term plan for the armed forces through 2024 confirms the military focus on space operations. Maritime surveillance, communications, command and control, space domain awareness (SDA), and cooperation with allies and commercial actors are focus areas.<sup>84</sup> There is a broad understanding of space as a war-fighting domain and the need for including space in strategy development.<sup>85</sup> SDA is a capacity relevant for

NATO contribution and a prioritized national focus area and therefore aligns with NATO's strategy.<sup>86</sup>

### ***NATO's Space Strategy***

NATO established space as a new operational domain in 2019 when alliance members adopted NATO's space policy.<sup>87</sup> In October 2020, the NATO Space Centre at Allied Air Command in Ramstein, Germany, was established. The center will coordinate allied space activities, support NATO missions and operations such as communications and satellite imagery, and protect allied space systems.<sup>88</sup> NATO will not put weapons in space but will procure all products from NATO allies.<sup>89</sup> The alliance will not become an autonomous space actor.<sup>90</sup> Some essential military space functions to be provided to NATO include SDA, satellite imagery, PNT, and communications.<sup>91</sup> NATO's demand for space support aligns with US and Norwegian strategic focus areas regarding space assets and support in the Arctic.

### **Topics of Cooperation**

The US and Norway may have different goals and motivations for their Arctic and space strategy efforts. These differences are natural since the US is a great power while Norway is a smaller nation with political and cultural ties to the US and Russia. Norway's neighbor brings strategic competition to Norway's doorstep, strengthening relations between Norway and the US. Although the two countries may have separate reasons for their interest in the Arctic and their strategy rationales may differ, their activities to achieve these goals often align. The coinciding lines of effort and focus areas for the two nations establish common grounds for cooperation.

First and foremost, cooperation is the common ground for the described policies and strategies, and it is the foundation for all other topics discussed in this article. Norway and the US have already established a unique cooperative relationship in some of these areas. Nevertheless, better cooperation and awareness of the potential advantages of joining forces may lead to even greater gains for both nations. Not limited to just the Arctic region, SDA is one of the most critical areas where both countries can cooperate. The following table summarizes lines of effort and strategies for the US, Norway, and NATO.

**Table. Lines of effort and strategies**

Lines of Effort	Strategies		
	United States	Norway	NATO
International, allied, and partner cooperation in both domains	<ul style="list-style-type: none"> <li>• US space policy</li> <li>• Department of the Air Force Arctic strategy</li> <li>• Defense space strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Norway's Arctic strategy</li> <li>• Norway's space strategy</li> <li>• Norwegian armed forces long-term plan</li> </ul>	<ul style="list-style-type: none"> <li>• NATO strategy</li> </ul>
Space domain awareness	<ul style="list-style-type: none"> <li>• US space policy</li> <li>• Defense space strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Norway's space strategy</li> <li>• Norwegian armed forces long-term plan</li> </ul>	<ul style="list-style-type: none"> <li>• NATO space strategy</li> </ul>
C3ISR in the Arctic	<ul style="list-style-type: none"> <li>• Department of the Air Force Arctic strategy</li> <li>• Defense space strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Norway's Arctic strategy</li> <li>• Norwegian armed forces long-term plan</li> </ul>	<ul style="list-style-type: none"> <li>• NATO strategy</li> </ul>
Enhanced PNT	<ul style="list-style-type: none"> <li>• National space policy</li> <li>• Department of the Air Force Arctic strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Norway's space strategy</li> </ul>	<ul style="list-style-type: none"> <li>• NATO space strategy</li> </ul>
Launch capability	<ul style="list-style-type: none"> <li>• US space policy</li> </ul>	<ul style="list-style-type: none"> <li>• Norway's space strategy</li> </ul>	
Exchange of knowledge, education, research, development, exercises, and training	<ul style="list-style-type: none"> <li>• US space policy</li> <li>• Department of the Air Force Arctic strategy</li> </ul>	<ul style="list-style-type: none"> <li>• Norway's Arctic strategy</li> <li>• Norwegian armed forces long-term plan</li> </ul>	

### *Space Domain Awareness*

Space domain awareness is a primary strategic goal for the two nations and NATO. Norway's GLOBUS radars, located in Vardo in northeastern Norway, have provided space situational awareness for Norway, the US, and NATO since 2001.<sup>92</sup> The system will be further improved after completion of the Globus III radar, a joint project of US Air Force Space Command and the Norwegian Intelligence Service.<sup>93</sup> The system is planned to be operational in 2022.<sup>94</sup> The radar site's primary missions are surveilling, tracking, and categorizing objects in space; surveilling Norwegian interest areas in the north; and collecting research and development information.<sup>95</sup>

This cooperation and joint effort exemplify how Norway, a relatively small military space nation, can contribute to the space domain to benefit all NATO nations. Norway's geographic position and relatively mild climate make the operation possible within the Arctic region. With the Arctic becoming the new area of competition and congestion, Norway is positioned to become a critical player in the arena.<sup>96</sup> Like space domain awareness, communication is an essential area of cooperation.

### *Communications*

Secure, reliable communication in the Arctic is vital for any operation—military, civilian, or commercial. Communication between units operating

in the Arctic area and back to their command organizations is essential for command and control. US and Norwegian armed forces need broadband network and voice capability. In a remote area like the Arctic, where “fiber optic infrastructure is scarce or nonexistent,” communication via satellites is the only viable solution.<sup>97</sup> An increased US presence and a sustained presence from Norwegian forces—all with the same communication, command, and control demands—make satellite communication a perfect example of another area of needed cooperation between nations and between government and civilian actors.

Communications services in the Arctic are provided mainly by satellites in geostationary Earth orbit (GEO), with a limited coverage above 75°–80° north.<sup>98</sup> Fixed users may have broadband service up to 80° north, but the very small aperture terminals (VSAT) only cover up to 75° north.<sup>99</sup> Iridium NEXT’s low Earth orbit (LEO) satellite constellation is the only mobile satellite service provider with proper coverage in the polar region.<sup>100</sup> Like Kepler and Argos, a few other companies provide LEO connectivity, but none provide near-real-time broadband service.<sup>101</sup> Communications in the Arctic area need improving to meet the increased requirements for the allied military presence there.

The US and Norway are already working together to upgrade communications. They are involving government and commercial entities and combining international, cross-sector, and dual-use cooperation. For example, Inmarsat plans to launch two satellites in a highly elliptical orbit (HEO) in 2022.<sup>102</sup> They will provide continuous high-speed mobile broadband coverage above 65° north and work in conjunction with Inmarsat’s 13 GEO satellites.<sup>103</sup> The Norwegian Defense Department will share the cost with the US Air Force and Inmarsat.<sup>104</sup> The satellites will be available for merchant fleets, fishing vessels, and other commercial actors and provide tactical and strategic communication for government customers.<sup>105</sup> They will improve broadband coverage for US and Norwegian military forces in the area but may not deliver a satisfactory amount of data transfer in the event of a conflict.

Norway’s ambition of being independent in providing critical services for security issues combined with its emphasis on international and bilateral agreements shows the desire for government- or allied-controlled assets. Although Inmarsat is a UK-based company, future commercial sales or changes in the company structures might threaten the Norwegian military forces’ access to the service or render null the possibility of secure and classified communications. China and Russia are investing in and buying European companies. Recently, a Russian-controlled company attempted

to buy a Norwegian Rolls Royce engine maker.<sup>106</sup> However, the Norwegian government has temporarily stopped the sale due to security issues.<sup>107</sup> To depend solely on a commercial actor reduces the service's reliability in times of crisis, making increased governmental cooperation even more critical.

A government controlled and operated tactical and strategic initiative is needed to cover the US's and Norway's increased demand for high-speed communications in the Arctic. The planned ViaSat Link 16-capable LEO satellite is an example of a system under US and Norwegian government control.<sup>108</sup> Bringing Link 16 from a line-of-sight to beyond-line-of-sight system would improve the situational awareness for all on the tactical, operational, and strategic levels of a conflict.<sup>109</sup> As an Arctic nation, Norway should invest in this constellation to ensure a speedy development to achieve timely and secure communications in the Arctic for all Norwegian and allied forces. Norway is well positioned for cooperation regarding up-link and downlink through already established capabilities and can bring this capability into the cooperative effort. Intelligence, surveillance, and reconnaissance (ISR) is another area of cooperation that should be emphasized and increased.

### ***Intelligence, Surveillance, and Reconnaissance***

Space is integral to ISR operations because it is the vehicle for the provision of any usable situational awareness in the Arctic region. The Arctic's properties—large, dark, and remote with unhospitable weather—make conducting ISR operations from space the preferred and most likely the only viable solution. As Norway's space strategy states, environmental surveillance is critical. Understanding the Arctic environment and determining how and when it will change is a precursor to avoiding potential conflict. Dual-use assets for environmental surveillance have a military potential as well.

Norway has a long history of maritime surveillance of the sea in the Norwegian area of interest. Through *NorSat-1* and *NorSat-2*, the Norwegian Coastal Administration uses the Automatic Identification System (AIS) that all ships above 300 gross tons have been required to have since 2010.<sup>110</sup> The new *NorSat-3* enhances AIS surveillance with an experimental navigation radar detector (NRD).<sup>111</sup> The *NorSat* satellites are in sun-synchronous orbits and also have additional scientific purposes such as surveillance of solar radiation and space weather.<sup>112</sup> They thus provide cross-sectorial (commerce and defense sector) and dual-use (surveillance and scientific) capabilities. These satellites, combined with the coastal radars in Norway, are a vital surveillance source for Russian military ac-

tivity in the Barents area. Satellites in polar LEO orbit will help track ships in Norway's exclusive economic zone and detect ships operating in the Arctic region.

Norway is also developing new, exciting technological solutions that could improve ISR capabilities environmentally and militarily. At the Norwegian University of Science and Technology in Trondheim, a team of students and professors is working on a satellite with a hyperspectral camera, an intelligent onboard processing computer, and robotics.<sup>113</sup> The onboard camera can be slewed and provides images of small areas of interest.<sup>114</sup> The Norwegian company Kongsberg Satellite Service (KSAT) has contracted with the university to provide ground support that will enable the satellite to download images. Also, short revisit times due to its LEO orbit will allow the satellite to detect algae that is dangerous to salmon farming companies. The satellite's information can be transferred to "unmanned vehicles that can investigate the areas of interest further."<sup>115</sup> This technology could be developed and proved helpful in detecting images other than underwater algae, particularly submarines. Norway is close to the Kola Peninsula and Kola Bay, the Russian Northern Fleet's home base.<sup>116</sup> An ISR satellite combined with an unmanned aerial system deploying active sonar and confirming the satellite's findings will give the US, Norway, and NATO greater situational awareness. In addition to environmental surveillance, increased weather surveillance and forecasts are needed.

Any party with interest in the Arctic must consider the punishing weather conditions that can affect the safety of humans and machines. The US Space Force (USSF) is "considering future investments to improve weather monitoring in the Arctic."<sup>117</sup> Climate change, not only in the Arctic, requires "more timely and more precise data."<sup>118</sup> Norway's interest in research on environmental changes and improved weather forecasting aligns with the DOD and USSF's need for an updated weather satellite program, especially in the Arctic. By working cooperatively, the US and Norway stand to gain in everything from technology research to the employment of new space assets. Improved sensors reduce cost and improve capabilities. Polar weather satellites with an up-down link every 90 minutes via SvalSat—and distributed via high-speed broadband satellite—would make weather data available to many users, including commercial traffic and decision-makers in both countries.

Understanding the magnitude and speed of environmental changes in the Arctic is essential for resource conservation and situational awareness of potential strategic impacts. According to *SpaceNews*, a USSF spokes-

person confirmed that the Space Force “does not operate and is not developing capabilities specifically to monitor climate change.”<sup>119</sup> Although continued work with NASA and the National Oceanic Atmospheric Administration (NOAA) should be a focus area, cooperation between the US and Norway on environmental surveillance will benefit the intelligence and research communities and departments of commerce (fish and oil industry). It will also improve security for both nations and their allies, especially NATO. Besides enhanced ISR, the Arctic region needs enhanced PNT accuracy.

### ***Position, Navigation, and Timing***

Greater activity in the Arctic demands a heightened military presence in areal and naval assets. Thus, fully developed and accurate navigation systems are required to avoid accidents and ensure accurate data for situational awareness and weapons deployment, if needed. The high angles from a satellite in a global navigation satellite system—such as the Global Positioning System or Galileo for the Arctic user—limit the user’s accuracy, especially in the vertical axis.<sup>120</sup> The satellite-based augmentation system (SBAS) is constrained by atmospheric and topography challenges.<sup>121</sup>

One solution is to launch SBAS satellites in polar highly elliptical or low Earth orbits.<sup>122</sup> Another is to develop a medium Earth orbit constellation.<sup>123</sup> A dual-use system with future communications satellites used as SBAS assets represents the third option. Accurate, secure navigation and timing will be just as significant in the Arctic region as in the more populated areas between 65° south and 65° north as the number of cruise ships, commercial carriers, fishing vessels, oil rigs, and other commercial users increases. Therefore, it is in the interest of not only the US Space Force, DOD, and Norwegian Armed Forces to enhance PNT in the area but also that of the US Department of Commerce, Norwegian Department of Commerce and Fisheries, coast guards, and justice departments. The development of new technologies to enhance the accuracy of PNT in the region is, therefore, one area of future cooperation for the US and Norway. Launch capability is another important line of effort for both nations.

### ***Launch Capability***

Available, credible launch capability is one of Norway’s national focus areas and a focus area in the US space policy. Andøya Space will establish a launch site for small satellites to polar orbit.<sup>124</sup> The first launch is planned for the first half of 2022.<sup>125</sup> The launch capability will be up to 1.5 metric



tons to polar LEO or sun-synchronous orbit, and the Rocket Factory and Isar Aerospace will supply the initial launch vehicles.<sup>126</sup> Inclination will be from 87.4 to 108 degrees, and the remote area of Andøya provides for significant impact and dispersion areas in the Norwegian Sea.<sup>127</sup> The Norwegian government owns a large part of the company, which will be under governmental control in case of a conflict. Norway's launch capability will potentially extend to its allies, both bilateral and NATO, in the Arctic region. Andøya Spaceport will supplement the US government's existing launch capabilities. In addition to upstream space operations in launch capabilities, Norway can also provide downstream capabilities worldwide.

With Norway's geographic placement and relatively mild climate compared to the latitude, building and operating ground radars for SDA in the polar region is easier and more friendly to human existence than in Alaska, Canada, or Greenland. The world's largest ground station is SvalSat, operated by KSAT.<sup>128</sup> Located on Svalbard, an island to the north of the Norwegian mainland, it is "ideally situated at a high enough latitude to see every polar-orbiting satellite from all 14 daily transits."<sup>129</sup> Because the Norwegian government owns 50 percent of KSAT through Space Norway, SvalSat represents a reliable asset in times of conflict.<sup>130</sup> KSAT has 25 ground stations located throughout the world, including the Norwegian mainland.<sup>131</sup> A global network combined with a cybersecurity focus makes global downloading of payloads and uploading of software for satellite management possible from the company's offices in Tromsø in northern Norway.<sup>132</sup> Stronger military cooperation with the civilian side of the operation, as described in the Norwegian government's space strategy, will further improve data and cybersecurity for a military-grade system.

### ***Education, Research, and Development***

Norway has a long history as a space nation. Kristian Birkeland, a Norwegian scientist, completed his famous terrella experiment in 1896 in which he made artificial Northern Lights, known as the aurora borealis. This achievement marked the beginning of modern space operations in Norway.<sup>133</sup> The Andøya Rocket Range launched its first scientific rocket in 1962 and has since launched over a thousand rockets. Norway has several institutions for space-related education, from satellite technology to space physics. In cooperation with the University of Oslo (UiO), the Norwegian military research institute Forsvarets forskningsinstitutt (FFI) developed the Rimfax radar for the *Perseverance* rover.<sup>134</sup> Norway is a member of the European Space Agency, and the Norwegian space industry consists of around 40 companies.<sup>135</sup> Several Norwegian companies

have further developed technology used offshore and in areas from medical science to space technology, and Norwegian technology and knowledge of space and space operations are world class.<sup>136</sup> Space is also a highlighted interest in the Norwegian national strategy.

### **Suggested Combined Arctic Space Strategy**

A future US and Norwegian combined Arctic space strategy should focus on three primary efforts. The first is closing the Arctic infrastructure gap. The US and Norway need to recognize the increased strategic significance of the Arctic region. Its remoteness and harsh conditions underline the need for space operations to provide C3ISR to achieve security for both nations' interests. Gen John Raymond, chief of space operations for the USSF, states that the *Department of the Air Force Arctic Strategy* is "a really important strategy for space" as the US wants to "deter conflict from occurring both in space and through the Arctic."<sup>137</sup> As most US and Norwegian strategy documents indicate and some space and military experts argue, there is a need for cooperation between Arctic partners to "increase vigilance in this increasingly vital region."<sup>138</sup> Therefore, an Arctic space strategy must continue on this track. US and Norwegian armed forces should expand their cooperation to ensure cost sharing and shared benefits from education, research, development, and geographic position to close the gap in necessary infrastructure in the region.

Dual-use assets reduce government spending, and profitable commercial companies increase a nation's economic power. Commercial companies like SpaceX conduct technological developments to make space operations cheaper, better, and more available. The drawback of the commercial space industry is the lack of governmental control in a conflict. Therefore, allied governments must deal exclusively with companies from the involved nations and have transparent contracts and ownership control. China's One Belt, One Road initiative and Russian corporations' predatory buy-ups of European companies emphasize this point. Space capabilities controlled by companies from an adversary nation are not desirable in case of a conflict.

As a small nation with limited human resources available for a considerable and credible conventional force, Norway should continue its strategy of NATO contributions. C3ISR space assets are a sought-after capacity for NATO, especially in the Arctic area where Russia and China are increasing their presence. Therefore, Norway needs to continue developing its focus on technological development within space, cyber, and artificial intelligence. Technological development will bring new com-

mercial opportunities and be a backup industry for oil and gas production, rendering Norway's economy powerless and vulnerable. Norway's geographic position in the Arctic—with less harsh conditions than Canada, Alaska, or Greenland—makes it an indispensable choice for US bilateral collaboration and NATO partner cooperation. Its geographic position also makes Norway dependent on the Arctic region and therefore equally as interested as the US in Arctic security. With less access to livable areas in the Arctic region, the US will benefit from such cooperation. Continued closing of the infrastructure gap can and should be done in conjunction with allies and partners.

The second main effort is improved SDA in the polar area. Space as the solution for the US and Norwegian Arctic challenges is not exclusive to these nations. China and Russia have shown military and commercial interest in the region and have increased their space capability in polar orbits. Increased SDA is therefore as important as increased ISR capabilities. Since Chinese and Russian intentions in the Arctic are unknown, their objectives in space in the polar region are an area of concern for the US, Norway, and NATO allies. A robust and dependable SDA system in the polar region must therefore be another critical area of cooperation—and one that nations' strategy documents should emphasize. Nevertheless, the most important field of cooperation does not lie in technical solutions and assets but in the exchange and increase of knowledge and usage of the capabilities.

To that end, the third main effort is education and liaising. A strong, valuable, and lasting cooperation between nations rests on a shared understanding of the necessity and gains of cooperation. Since most US and Norwegian policy and strategy documents recognize the criticality of space and the Arctic, cooperation between the two nations is, as the documents also declare, wanted and necessary. This cooperation must start with a shared understanding of the requirements to operating in the region and domain. Being an Arctic nation, Norway brings Arctic know-how, and the US, being the most prominent space nation, brings space knowledge into the partnership. Consequently, the most significant cooperation between the nations should be sharing knowledge through education, liaising, research, and development.

The know-how of Arctic operations on the ground is also a valuable trade for USSF personnel. The USSF mission includes "providing space capabilities to the joint force."<sup>139</sup> Considering the Arctic region's increased strategic importance, understanding the Arctic warrior's needs and how to support them is knowledge that Norway has acquired as an Arctic nation.

The US Marine Corps has already been conducting winter training in Norway, although reduced from year round to a more evenly spaced deployment.<sup>140</sup> Understanding the challenges of operating in harsh weather—with limited (but improving) access to communication assets, the effects of radiation, and a limited PNT signal for accurate positioning and weapons delivery—is crucial for the supporting role of USSF. The US already has two students (USAF and USMC) at the multiservice Norwegian Staff Course.<sup>141</sup> One recommendation is that USSF members attend this course to increase their understanding of the Arctic. Further, Norway should continue participating in professional military education (PME) like the Schriever Space Scholars to gain space knowledge.

Though Norway is a medium-sized space nation on the civilian-end commercial side, it can still improve its military space knowledge. The increased recognition of space's significance for society at large and military operations constitutes a change in Norwegian armed forces' thinking. New space technology, doctrine, and security threats develop quickly, and Norway cannot afford to lag in this vital field. Norwegian officers at the tactical, operational, and strategic levels need PME to cooperate with our allies that are further developing space power theory and application. The establishment of the US Space Force in 2019 puts the US in the lead of NATO space nations. The growing number of American and international students in the Schriever Space Scholars program shows the DOD and USSF's dedication to space-related PME. It will be valuable for Norwegian officers to continue to attend this course either as an addition to Air Force Command and Staff College (ACSC) attendance or alternating biannually between the Schriever program or the USSF staff course and ACSC. In addition to education, building common grounds for the domains necessitates sharing a strategic and operational understanding of space and the Arctic through liaisons and exchange officers.

A Norwegian liaison position is recommended at the US operational and strategic levels to enable sharing experience and knowledge and discussing Arctic issues regarding space power application and cooperation in the USSF and Norwegian armed forces. As discussed, education will increase Norway's knowledge and competence regarding space power while the USSF gains knowledge of the Arctic region and operations therein. The main focus should initially be on the operational level to understand the possible application of space power in the Arctic during military operations. The Norwegian armed forces require an increased focus on the need to include the space domain in planning. On the strategic level, understanding US goals increases the possibility of adapting

Norwegian space strategy to gain even more mutual benefits for both nations in all operations in the Arctic space domain.

## **Conclusion**

Norway should continue to play an essential role in the US Arctic space strategy. The US and Norway are cooperating in many vital areas already, but the growing strategic significance of the Arctic also increases Norway's geostrategic importance. Norway is becoming increasingly relevant not only because of its status as an Arctic nation and alliance with NATO but also because of its space industry, knowledge, and advantages regarding satellite launch, downlink, and operations in any polar orbits. The US and Norwegian combined Arctic space strategy should focus on three primary efforts.

The first is closing the Arctic infrastructure gap. Cooperation regarding the increased need for C3ISR, improved PNT, and environmental surveillance to understand the changing climate and possibilities in the area is crucial for decision-making. Military intelligence and commercial surveillance will increase security and improve communications possibilities for emergency communication and coordination of emergency and disaster handling. The second main effort is improving SDA in the polar area. Understanding how China and Russia are using polar and sun-synchronous orbits is essential for maintaining the security of our space capability and determining Chinese and Russian intentions in the region. The third and most critical effort is fostering an exchange of educational opportunities and liaisons. Sharing knowledge about the Arctic and space requires minimal economic investment and will benefit both forces. A stronger focus on knowledge exchange and strategy development is a low-cost enhancement of the two nations' cooperation and a necessity for building further cooperation on a steady foundation. **SSQ**

### **Lt Col Kjetil Bjørkum, Royal Norwegian Air Force (RNoAF)**

Colonel Bjørkum is the commander of the 337th Squadron, RNoAF. He received his aviator wings at the Euro-NATO Joint Jet Pilot Training Program, Sheppard AFB, Texas. He is a graduate of Air War College at Air University, Maxwell AFB, Alabama, and attended the Schriever Space Scholars program at Air University.

## **Notes**

1. Karen L. Jones, Samira Patel, and Martin N. Ross, *Closing the Arctic Infrastructure Gap: Existing and Emerging Space-Based Solutions* (El Segundo, CA: The Aerospace Corporation, Center for Space Policy and Strategy, October 2019), 1, <https://aerospace.org/>.

2. Jones, Patel, and Ross, 3.
3. Jones, Patel, and Ross, 1.
4. Arctic Council, "Who We Are," accessed July 2021, <https://arctic-council.org/en/>.
5. Norwegian Ministries, *Norway's Arctic Strategy – Between Geopolitics and Social Development* (Oslo: Norwegian Government Security and Service Organization, 2017), 3, <https://www.regjeringen.no/>.
6. US Department of Homeland Security, *Strategic Approach for Arctic Homeland Security* (Washington, DC: US Department of Homeland Security, Office of Strategy, Policy, and Plans, January 2021), 7, <https://www.dhs.gov/>; and Kenneth J. Bird et al., "Circum-Arctic Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle," US Geological Survey Fact Sheet 2008-3049, <http://pubs.usgs.gov/>.
7. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 4.
8. US Department of Homeland Security, *Strategic Approach for Arctic Homeland Security*, 9.
9. Marc Lanteigne, "The Changing Shape of Arctic Security," *NATO Review*, 28 June 2019, <https://www.nato.int/>.
10. Lanteigne.
11. Lanteigne.
12. Lanteigne.
13. Lanteigne.
14. NATO, "Partners," 27 March 2020, <https://www.nato.int/>.
15. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 3.
16. Jones, Patel, and Ross, 3.
17. Lanteigne, "Changing Shape of Arctic Security."
18. Lanteigne.
19. Lanteigne.
20. Lanteigne.
21. Rolf Folland, "*Arctic Security: Deterrence and Détente in the High North*," The Arctic Institute, 30 March 2021, <https://www.thearcticinstitute.org/>.
22. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 5–6.
23. Marisa R. Lino, "Understanding China's Arctic Activities," International Institute for Strategic Studies, 25 February 2020, <https://www.iiss.org/>.
24. Lino, 2.
25. Lino, 2.
26. Lino, 3–4.
27. Jim Danoy and Marisol Maddox, "Set NATO's Sights on the High North," Atlantic Council Scowcroft Center for Strategy and Security, 2020, 74.
28. China Global Television Network, "China's Polar-Observing Satellite Obtains over 2,500 Images," 14 September 2020, <https://news.cgtn.com/>.
29. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 1.
30. President of the United States, *National Strategy for the Arctic Region* (Washington, DC: The White House, May 2013), 5, <https://obamawhitehouse.archives.gov/>.
31. Alaska Public Lands Information Centers, "Alaska's History," accessed 3 May 2021, <https://www.alaskacenters.gov/>.
32. Weather Atlas, "Monthly Weather Forecast and Climate Alaska, USA," accessed 3 May 2021, <https://www.weather-us.com/>.
33. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 3.

34. US Department of Homeland Security, *Strategic Approach for Arctic Homeland Security*, US6.
35. US Department of Homeland Security, 7.
36. US Department of Homeland Security, 7.
37. Department of Defense, "Report to Congress, Department of Defense Arctic Strategy" (Washington, DC: Department of Defense, Office of the Under Secretary of Defense for Policy, June 2019), 3, <https://media.defense.gov/>.
38. Department of Defense, 6–7.
39. Department of the Air Force, *Department of the Air Force Arctic Strategy* (Washington, DC: Department of the Air Force, July 2020), 2, <https://www.af.mil/Portals/>.
40. Department of the Air Force, 2.
41. Department of the Air Force, 2–3.
42. Department of the Air Force, 8.
43. Norwegian Ministries, *Norway's Arctic Strategy – Between Geopolitics and Social Development* (Oslo: Norwegian Ministry of Foreign Affairs, 2017), 7, <https://www.regjeringen.no/>.
44. Norwegian Ministries, 11.
45. Norwegian Ministries, 2.
46. Norwegian Ministries, 9–10.
47. Norwegian Ministries, 15.
48. Norwegian Ministries, 15.
49. Bjerknes Centre for Climate Research, "The Gulf Stream and Our Mild Climate in Norway," 5 August 2015, <https://www.bjerknes.uib.no/>.
50. Danoy and Maddox, "Set NATO's Sights on the High North," 76.
51. NATO, "Strategic Concepts," 24 September 2020, <https://www.nato.int/>.
52. NATO, "Strategic Concepts."
53. Danoy and Maddox, "Set NATO's Sights on the High North," 76.
54. Danoy and Maddox, 77.
55. For an explanation of how Canada and Denmark resist supporting NATO, see Danoy and Maddox, note 7. I'
56. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 1.
57. Jones, Patel, and Ross, 1.
58. Executive Office of the President, *National Space Policy of the United States of America* (Washington, DC: The White House, 9 December 2020), 1, <https://trump.whitehouse.archives.gov/>.
59. Executive Office of the President, 5–6.
60. Executive Office of the President, 7–12.
61. Executive Office of the President, 27.
62. Executive Office of the President, 28–29.
63. Executive Office of the President, 30.
64. Department of Defense, *Defense Space Strategy Summary* (Washington, DC: Department of Defense, June 2020), 2, <https://media.defense.gov/>.
65. Department of Defense, 6.
66. Department of Defense, 6–9.
67. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 3.
68. Department of the Air Force, *Arctic Strategy*, 8.
69. Department of the Air Force, 8.

70. Department of the Air Force, 8.
71. Paal Brekke, "Norge Som Romnasjon" [Norway as a space nation], Norwegian Space Agency, accessed 4 May 2021, <https://www.romsenter.no/>.
72. Det Kongelige Naerings Og Fiskeridepartementet [Ministry of Trade and Industry], Meld. St. 10 [Report 10], *Hoeytflyvende Satelitter – Jordnaere Formaal, En Strategi for Norsk Romvirksomhet* [High-flying satellites – terrestrial purposes – a strategy for Norwegian space activities] (2019–2020), 13 December 2019, 8, <https://www.regjeringen.no/>.
73. Ministry of Trade and Industry, 8.
74. Ministry of Trade and Industry, 9–12.
75. Ministry of Trade and Industry, 12.
76. Ministry of Trade and Industry, 12.
77. Ministry of Trade and Industry, 12.
78. Ministry of Trade and Industry, 16.
79. US Geological Survey, "SvalSat, A Svalbard, Norway Story," accessed 4 May 2021, <https://eros.usgs.gov/>.
80. Ministry of Trade and Industry, [High-flying satellites – terrestrial purposes], 17.
81. National Aeronautics and Space Administration, Mars 2020 Mission Perseverance Rover, "RIMFAX," accessed 4 May 2021, <https://mars.nasa.gov/>.
82. Det Kongelige Forsvarsdepartement [Ministry of Defense], Prop. 14S, *Evne til forsvar – vilje til beredskap. Langtidsplan for Forsvarssektoren* [Ability to defend – willingness to be prepared: long-term plan for the defense sector] (2020–2021), 16 October 2020, 108–9, <https://www.regjeringen.no/>.
83. Ministry of Defense.
84. Ministry of Defense.
85. Ministry of Defense, 21.
86. Ministry of Defense, 109.
87. NATO, "NATO's Approach to Space," 22 April 2021, <https://www.nato.int/>.
88. NATO.
89. NATO.
90. Kestutis Paulauskas, "Space: NATO's Latest Frontier," *NATO Review*, 13 March 2020, <https://www.nato.int/>.
91. Paulauskas.
92. Spacewatch Europe, "Arctic Space: Globus Radar in Norway for Arctic SSA; Space Norway Targets Military Contracts," accessed 4 May 2021, <https://spacewatch.global/>.
93. Globalsecurity.org, "Globus III," accessed 4 May 2021, <https://www.globalsecurity.org/>.
94. Thomas Nilsen, "US and Norway Upgrade Eye on Border to Northern Russia," *The Barents Observer*, 16 November 2018, <https://thebarentsobserver.com/>.
95. Forsvaret, "Oppgradering Av GLOBUS-Systemet" [Upgrade of the GLOBUS system], accessed 4 May 2021, <https://www.forsvaret.no/>.
96. Sandra Erwin, "Raymond: Space Force to Play Key Role in Military Operations in the Arctic," *SpaceNews*, 21 July 2020, <https://spacenews.com/>.
97. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 7.
98. Jones, Patel, and Ross, 8.
99. Jones, Patel, and Ross, 8.
100. Jones, Patel, and Ross, 8.
101. Jones, Patel, and Ross, 19.



102. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 9.
103. Jones, Patel, and Ross, 9.
104. Col Stig Nilsson, "Norwegian Space Approach," briefing to the Atlantic Council, 19 November 2020.
105. Jones, Patel, and Ross, 9.
106. Terje Solsvik and Kate Holton, "Norway Suspends Roll-Royce Asset Sale on Security Grounds," Reuters, 9 March 2021, <https://www.reuters.com/>.
107. Solsvik and Holton.
108. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 20.
109. Viasat, "Viasat Contracted to Deliver the World's First Link 16-Capable Low Earth Orbit (LOE) Spacecraft," 22 May 2019, <https://www.viasat.com/>.
110. Kystverket, "Ny Satellitt Vil Styrke Skipsovervåkningen" [New satellite will strengthen ship monitoring], 9 January 2018.
111. Kystverket.
112. Berit Ellingsen, "NorSat-1 and NordSat-2 Launched," Norwegian Space Agency, 12 July 2017, <https://www.romsenter.no/>.
113. Norwegian University of Science and Technology (NTNU), "The HYPSON Mission," accessed 4 May 2021, <https://www.hypso.space/>.
114. Evelyn Honore Livermore (Norwegian University of Science and Technology), interview by the author, 27 January 2021.
115. NTNU, "HYPSON Mission."
116. Globalsecurity.org, "Red Banner Northern Fleet," accessed 4 May 2021, <https://www.globalsecurity.org/>.
117. Sandra Erwin, "DoD Focus on Climate Could Shape Future Investments in Weather Satellites," *SpaceNews*, 24 February 2021, <https://spacenews.com/>.
118. Erwin.
119. Erwin.
120. Anna B. O. Jensen and Laura Routsalainen, "Challenges for Positioning and Navigation in the Arctic," slide presentation, accessed 4 May 2021, <https://www.unoosa.org/>.
121. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 11.
122. Jones, Patel, and Ross, 12.
123. Jensen and Routsalainen, "Challenges for Positioning and Navigation in the Arctic."
124. Andøya Space, "Our History," accessed 4 May 2021, <https://www.andoyaspace.no/>.
125. Ingunn Berget, vice president, Orbital, Andøya Space, to the author, email, 20 January 2021.
126. Andøya Space, "Orbital Launch," accessed 4 May 2021, <https://www.andoya.space.no/>.
127. Andøya Space.
128. Jones, Patel, and Ross, *Closing the Arctic Infrastructure Gap*, 7.
129. Jones, Patel, and Ross, 7.
130. Kongsberg Satellite Services, "About Us," accessed 4 May 2021, <https://www.ksat.no/>.
131. Kongsberg Satellite Services, "Ground Network Services," accessed 4 May 2021, <https://www.ksat.no/>.
132. Kongsberg Satellite Services, "Satellite Operation," accessed 4 May 2021, <https://www.ksat.no/>.

133. Brekke, "Norge Som Romnasjon" [Norway as a space nation].
134. Mette Jonsrud, "Radaren Rimfax: Fra UiO Til Mars For aa Finne Liv" [The Rimfax radar: From UiO to Mars to find life], University of Oslo, 28 November 2018, <https://titan.uio.no/>.
135. Norwegian Space Agency, "Norge I Rommet Og I Europa" [Norway in space and in Europe], accessed 4 May 2021, <https://www.romsenter.no/>.
136. Erwin, "Raymond."
137. Erwin, "Raymond."
138. Thomas Ayres, "China's Arctic Gambit a Concern for US Air and Space Forces," *SpaceNews*, 5 October 2020, <https://spacenews.com/>.
139. United States Space Force, "United States Space Force Mission," accessed 4 May 2021, <https://www.spaceforce.mil/>.
140. Philip Athey, "Marine Corps Announces End to Year-Round Deployment to Norway," *Marine Times*, 13 August 2020, <https://www.marinecorpstimes.com/>.
141. Morten Flagestad, senior consultant, Stabskolen, to the author, email, 17 March 2021.

# Comprehensive Security Approach in Response to Russian Hybrid Warfare

LT COL TUUKKA ELONHEIMO, FINNISH AIR FORCE

## Abstract

This article assesses why open, digitalized Western democracies are prone to hybrid warfare and analyzes versatile overt and covert mixed warfare methods in the modern information-dependent and inter-connected environment. It also draws on various hybrid warfare influence methods and explains the broader concept and essence of Russian hybrid warfare. Besides analyzing structural hybrid warfare challenges, the article assesses and proposes means and practices to mitigate, act against, and deter overt or covert hybrid offensives. The article argues that Russian mixed warfare methods in tandem create a potential threat to Western democracies' unity and decision-making. However, these Western states could mitigate and prevent the implications of hybrid warfare by increasing comprehensive security, cooperation, situational awareness, preparedness, and resilience. The article identifies that the combined use of proper coordination, cooperation, information sharing, education, and readiness among authorities, governmental and nongovernmental organizations, businesses, and citizens could diminish these multifaceted, ambiguous hybrid aggressions.

\*\*\*\*\*

## Introduction

Deception, asymmetrical methods, and propaganda have been part of Russia's warfare and strategic mindset for centuries. After the Cold War, the US and NATO shifted to counterinsurgency operations, and the global war on terrorism became synonymous with "endless wars."<sup>1</sup> In contrast, Russia and China have increased their relative status in strategic competition and learned to use all national power instruments—diplomatic, information, military, and economic (DIME)—in tandem.<sup>2</sup> Russia has narrowed the technological gap with Western militaries in conventional warfare and blatantly increased clan-

destine operations below the armed conflict level. Since the Russian asymmetric approach combines a wide variety of traditional and non-traditional war-fighting methods, many Western sources have defined it as “hybrid warfare.”<sup>3</sup>

Manifold hybrid warfare attacks challenge Western democracies’ cohesion, decision-making, and cooperation by creating a wedge with dissonance. Concurrently, strategic leaders, state authorities, and citizens encounter volatile, uncertain, complex, and ambiguous (VUCA) digital environments.<sup>4</sup> Thus, this article examines modern, open democracies’ vulnerabilities to malicious Russian hybrid warfare and explains Russian strategies to provide security actors with a framework to make recommendations for increasing readiness, countermeasures, resilience, and deterrence.

Though Russian military literature and the wars against Chechnya and Georgia reveal many characteristics of this new approach, hybrid warfare shocked Westerners when the war broke in 2014.<sup>5</sup> The unmarked “green men” occupying Crimea and harmful cyberattacks against Ukraine’s infrastructure were a wake-up call for Western decision-makers.<sup>6</sup> Subsequently, the threat of military invasion, the shoot-down of an airliner, and disinformation campaigns revealed how broad and sneaky hybrid warfare is. Russian clandestine strategies aim to disseminate uncertainty and friction (Clausewitz) in governments’ and citizens’ daily lives. The strategic fog creates ambiguity in the targeted state, complicating the tracking of the original perpetrator. It enables Russia to conceal its operations in the physical and nonphysical war-fighting domains. Russian hybrid warfare’s digital revolution creates complex threats and multifaceted challenges to open Western democracies. However, a comprehensive security approach, cooperation, and joint procedures generate an adequate foundation for increasing resilience, strengthening overall preparedness, mitigating ramifications, and deterring against hybrid offensives. This article first analyzes why contemporary Western societies are vulnerable to the influences of a hybrid strategy and draws on recent events to illustrate Russia’s use of hybrid warfare. After describing the instruments of hybrid warfare, the article assesses the essence of Russian hybrid warfare and examines and compares comprehensive security approaches and procedures to mitigate and counter hybrid warfare aggressions. Finally, based on the analysis of Russian hybrid warfare activities, the article recommends actions for security decision-makers to resist and respond to future hybrid warfare.

## **Vulnerabilities of a Modern Digital Information Society**

*A lie gets halfway around the world before the truth has a chance to get its pants on.*

—Winston Churchill

The digital revolution, global networks, lightspeed information flow, and internet dependency have dramatically changed technological opportunities to influence and manipulate. Additionally, cyber espionage, subversion, and sabotage intensify the digital mess, overwhelm cognition, and complicate decision-making. Faceless hackers conceal their subtle denial-of-service attacks, email phishing, and troll accounts in the shadows of countless bits and clandestine Internet Protocol addresses.<sup>7</sup> Social media applications have become today's spyware, propaganda amplifiers, and nonkinetic weapon platforms. Unfortunately, the human capacity to handle information has not matched the weaponized digital information flow. Consequently, cyberattacks create novel security and privacy problems for governments and citizens. Cold War megaphones and leaflets have changed to cyberattacks and smartphone tweets, spreading without geographic barriers, manipulating opinions, destabilizing cohesion, and shaping targeted states' physical and cognitive environments.<sup>8</sup> In a digital, social-media-oriented society, the spread of confusing fake news, agitating diaspora, and increasingly unhealthy polarization are dangerous weapons to separate people into "us versus them."<sup>9</sup>

The worldwide digital environment increases connectivity and links individuals and organizations to a massive amount of data. However, concurrently, the enormous flow of information—the paradox of plenty—hampers the ability to handle, assess, and comprehend it all. Thus, individuals are losing their focus, attention, and capacity to make circumspect decisions.<sup>10</sup> The cyber domain creates security threats that reveal the weaknesses of open democracies and security organizations.<sup>11</sup> Malware programs, hacking algorithms, facial recognition systems, and cyberattacks enable advanced aggressions against diverse target audiences with low costs from attackers' homes. States with aggressive physical or digital influences can utilize non-state proxy actors to conceal their involvement, making covert approaches tempting.<sup>12</sup> Even if the targeted state could detect, track, and identify the attacker, it might lack the legislative mandate to block and prevent attacks. Identification and attribution are primary deficiencies in the battle against cyber and information warfare.

Artificial intelligence (AI) technology exponentially increases the speed, precision, reach, and efficacy of saturation campaigns.<sup>13</sup> Democratic values, like freedom of speech, restrain and complicate resisting assertive hybrid warfare. Who has the authority to censor gossip or the capacity to

protect vital security interests in cyberspace? In a post-truth world, fact-checking organizations, empirical science, and investigative journalism cannot keep pace with exponentially booming fake news and deep fakes.<sup>14</sup> Sneaky adversaries disrupt online banking with denial-of-service attacks, blackmail individuals and organizations with stolen personal emails, and interfere in presidential elections.<sup>15</sup>

Altogether, digitalization, modern communications, and cybersecurity leave plenty of room for Russian hybrid warfare. Indeed, Russia knows how to weaponize the information and combine all-domain asymmetrical warfare to target a wide range of audiences: the military, the government, institutions, media, businesses, individuals, and civil society. Experts at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) have aptly recognized how the fragmentation of truth, media-industry changes, the hegemony of private media, and new technologies foster hybrid warfare.<sup>16</sup> These information domain trends and risks—combined with open democratic societies’ tendency to act by the book concerning norms and rules of law—open the gateway for internal or external aggressors to exploit vulnerabilities.<sup>17</sup> As a concept, hybrid warfare welcomes all these information-era technological developments and tendencies. Overwhelmed by gigabytes of provocative targeted hostile narrative, people and state actors are confused. It is an efficient, easy, and cheap *modus operandi*.

### Russian Hybrid Warfare: Case Studies

*The most complete and happy victory is this: to compel one's enemy to give up his purpose while suffering no harm oneself.*

—Flavius Belisarius (505–565 CE)

Clausewitz classically argued that war is a continuation of policy by other means. He also stated that the nature of war (primordial violence, hatred, and enmity) does not change, whereas the character of war does.<sup>18</sup> To the same extent, in his book *Every War Must End*, Fred Charles Iklé demonstrates how complicated the rational calculus about wars’ gains and losses are before and during the conflict.<sup>19</sup> Since Putin’s reign, Russian actions have challenged these traditional principles and theories of war by raising the armed conflict threshold. Is Russia trying to continually shake the balance of war’s cost-benefit model, blur the distinction between peace and war, and muddle the distinction among deterrence, persuasion, and coercion?

Truly, Russian hybrid warfare tries to obscure the character of warfare and, more importantly, bring ambiguity, chaos, and friction to day-to-day

decision-making, policy formulation, and society's vital functions.<sup>20</sup> The following discusses how Russia's hybrid warfare gray zone intentionally challenges Western state officials, military leaders, and citizens. It also outlines the essence and cumulative effects of hybrid warfare.

### ***Threat or Use of Military Forces***

Western media often erroneously relates Russian hybrid warfare to nonmilitary actions instead of hard military power. However, the presence and threat of military capabilities are essential for Russian coercion and hybrid warfare. Russia has aggressively increased its sphere of influence militarily to advance strategic objectives in the European theater over the last decades.<sup>21</sup> Its initiatives include reopened and reconstructed military bases, new weapons systems, an increased military footprint in the Arctic, snap exercises, blue water deployments, show-of-force strategic bomber flights, and force-projection demonstrations. These efforts, along with brutal power military campaigns in Syria and Ukraine, indicate Russia's willingness to use its military instruments to regain regional hegemony.

Anti-access/area denial (A2/AD) capability development has increased worries among NATO, the US, and European Union (EU) states. Though these "keep-out zones" are not impenetrable, Russian long-range missiles and air defense challenge any force projection from Western states.<sup>22</sup> Militarily weaker neighbor states are under constant surveillance and within weapon range. This vulnerability increases pressure, coercion potential, and Russia's capacity to gain a military advantage. Special operation forces and unmarked soldiers occupying Crimea and the subsequent military operations inside eastern Ukraine demonstrated efficient influencing without ever declaring war.<sup>23</sup> Russia's fast operation tempo, overwhelming confusion campaign, and clandestine military operations surprised the Western intelligence community. Overall, Russia modernized and made its armed forces more versatile. From A2/AD systems to nuclear weapons, it can challenge, harass, and deter US and NATO forces—at least in a significant regional-level conflict.<sup>24</sup>

Russia possesses a broad array of electronic warfare capacities. Interference and jamming capabilities blur the difference between normal conditions and conflict—typical Russian gray zone operations. Russia has harassed military and civilian traffic through widely spoofing and jamming Global Positioning System (GPS) signals in conflict zones near Russian territory and Arctic areas.<sup>25</sup> Military and commercial aircraft were exposed to GPS jamming in Scandinavia during the Russian-Belarusian joint exercise in 2017.<sup>26</sup> Similarly, ships operating in the Black Sea have re-

ported losing position keeping and receiving GPS signal errors. However, Russia's disinformation campaign denies all accusations of any Russian electronic warfare attacks against space-based positioning, navigation, and timing (PNT) services.

Russia has used electronic warfare, force projection, long-range weapon systems, and multilayered defense systems in the Syrian and Ukrainian conflicts and close to Russian territory. Experiences from conflicts and increasingly advanced joint wartime exercises (for example, Zapad 2017) demonstrate Russia's offensive A2/AD capabilities and its potential to challenge NATO.<sup>27</sup> Broad military capacity and decisive use of all necessary means bolster the Russian military as a potent instrument of power and intimidate states even without immediate geographic contact with Russia. Using the military as a vital instrument of power provides an essential grounding for other Russian instruments of power and hybrid warfare execution.

### ***Cyberwarfare***

Clandestine cyber operations—ranging from espionage to subversion, sabotage, and identity theft—challenge state security organizations and everyday internet users.<sup>28</sup> To the same extent, the Russian readiness, nerve, and arrogance to expand cyberattacks in the digital world underline its comprehensive competition against adversaries. Russia's vague undercover cyberattacks create a curtain of uncertainty, complicating recognition, mitigation, and prevention of malicious cyberattacks.

The first well-known cyberattack series halted numerous Estonian administration and business sites after Russian-led protests over a WWII memorial dispute.<sup>29</sup> Contemporary Estonia was one of the most digitalized countries, tempting Russian hackers to target the government, banks, and media.<sup>30</sup> Though Estonian experts traced the denial-of-service attacks and connected the dots to the Kremlin, Russia adamantly denied all accusations.<sup>31</sup> Hence, Russia showed cyber dominance and paved the way to continue this new *modus operandi* without disruptions or international charges.

Similar cyberattacks followed the Estonian case. During the Russian invasion of Georgia in 2008, the cyberattack target was Georgia's defense communications. Likewise, in 2015, Russian hackers distributed malware into the Ukrainian electrical grid. It caused a power interruption for millions of people and highlighted Ukraine's energy and cyber vulnerabilities as well as Russia's power.<sup>32</sup> In 2017, Russia again targeted Ukraine through its financial and federal infrastructure. However, the NotPetya cyberattack



had harmful global implications and spread quickly across Windows operating systems, affecting, for example, global transportation companies from Masters to FedEx.<sup>33</sup> NotPetya and other destructive cyber operations illustrate that people are usually the weakest link and that cyberattacks have pervasive physical and cognitive ramifications, usually with limited responses from targeted states.<sup>34</sup>

### ***Information Warfare***

Russia has a long history of demonstrating its mastery of information warfare, but the focus in Putin's regime has shifted to manipulating foreign target audiences. Admittedly, propaganda and censorship have a strong position internally. Nevertheless, Russian information warfare increasingly undermines other states' decision-making, deteriorates societal cohesion, and disputes foreign leaders' authority and competence. Authoritarian Russia has solidified its role as a modern propaganda hegemony. Conversely, democracies have problems retaliating against this new soft and hard power mixture.

Russia's state-driven media, officials, proxies, trolls, and politicians promote ideas, rumors, and conspiracy theories favorable to Russia, unconfirmed truths via official digital channels, and biased social media accounts. Open information networks and technologies give Russian influencers a fast and cheap means to spread propaganda globally.<sup>35</sup> As an authoritarian state, Russia effectively controls influencers, proxy actors, and agents to conceal the Kremlin's fingerprints. Russia and China have spent millions of dollars increasing an asymmetric, aggressive, information warfare-based "sharp power."<sup>36</sup> Their sharp power creates a hostile environment, amplifying distrust and discord among people and state institutions by piercing and penetrating political and informational environments. Thus, the Kremlin has used sharp power, which is more harmful than traditional culture-based soft power, to meddle in other nations' elections and corrupt information in recent years.<sup>37</sup>

Russia's meddling in the 2016 US presidential election is the most visible example of comprehensive information warfare. Though foreign interference efforts have always played a role in policy making, handy, cheap new technologies made organized propaganda and disinformation campaigns more efficient and widespread than ever before.<sup>38</sup> Strategic-level information warfare undermined the US-led liberal world order and the populace's belief in the democratic presidential election system, developing a clear advantage for Trump.<sup>39</sup> Russian intelligence agencies illegally intruded and interfered with Hillary Clinton's and the Democratic Na-

tional Committee's email accounts and leaked content on WikiLeaks, causing political and social discord in America.<sup>40</sup> Russian intelligence agencies cunningly exploited all modern digital networks' vulnerabilities. More importantly, the nonregulated human social media networks multiplied the effects of distortion, dispute, and distrust.<sup>41</sup>

According to the intelligence community's assessments, President Putin ordered the multifaceted 2016 US presidential election meddling campaign—demonstrating how centralized hybrid warfare is in Russia.<sup>42</sup> The all-encompassing information campaign consisted of cyber espionage and intrusions against political organizations and electoral boards, public disclosure of collected data, propaganda, Russian state-owned news agency (Russia Today, Sputnik) misinformation campaigns, and fake social media profiles controlled by professional trolls from the so-called Internet Research Agency in St. Petersburg.<sup>43</sup> One worrisome phenomenon was that information warfare targeted partisan winners and losers differently; the campaign was not directed against the whole country like the examples of Pearl Harbor and 9/11.<sup>44</sup> Social-engineered divisive information warfare increased partisanship in the US and was a detrimental sting against democracy.

### **Nonmilitary Coercion and Intimidation**

One parlous trend in the Russian tool kit is the use of nonmilitary intimidation and coercion. State actors or proxies have used various illegal methods like blackmailing, assassinations, criminality, economic extortion, and intentional immigration agitation as part of broader coercion.

Russia exploited the European immigrant crisis in 2015 to overwhelm authorities by intentionally opening usually closely controlled border crossing points into Finland and Norway. Abruptly pushing thousands of immigrants into these countries paralyzed normal operations and required additional personnel to handle the chaos. The massive influx of immigrants also challenged the abilities of essential service providers—such as border, police, military, justice, healthcare, and security personnel—to perform their duties. Further, the disorder created by Russia's targeted immigration tactics intensifies the polarization and diversion in the targeted nation. The results fan the flames of discord, inducing diaspora and fueling racial prejudices that can spark demonstrations and violence. Russia clearly demonstrated that it has the ability and means to direct chaos toward targeted state decision-makers and authorities.

Russia uses proxy forces to amplify hybrid warfare dominance, hide its tracks, and prevent legal accountability for its actions. In Crimea, the pro-

Russian nationalist motorcycle club Night Wolves paved the way for Russian special operation forces by collecting intelligence, exploiting offensive protests, and distributing propaganda.<sup>45</sup> Criminal organizations' intimidation and covert illegal influencing provide state-level deniability, therefore constituting non-state proxy actors as an integral and growing part of the future of hybrid warfare.<sup>46</sup>

Additionally, Russia employs private military companies (PMC) in the conflicts in Ukraine and Syria. Its use of PMCs surfaced after Russian Wagner fighters lost their lives in a US airstrike in Syria.<sup>47</sup> PMCs play an increasingly important role, giving Russian leadership a compelling instrument of power to multiply the effects in the cyber and military battlefields and provide the guise of plausible deniability in dirty, dangerous, and illegal operations.<sup>48</sup>

Since Putin came to power, assassinations have reappeared as a method of influence. The Kremlin has systematically denied its involvement in high-level poisonings and provided alternate evidence and conspiracy theories as distractions.<sup>49</sup> However, the evidence—the sources of poison (dioxin, polonium, Novichok) and/or Russian security services members' presence—clearly links the assassinations to Russia.<sup>50</sup> Victims have posed a significant opposition or loyalty threat to Putin's power. Though the poisonings of journalist Anna Politkovskaya, anti-Russian Ukraine presidential candidate Viktor Yushchenko, ex-Russian intelligence officers Alexander Litvinenko and Sergei Skripal, and opposition leader Alexei Navalny have not been fatal in every case, Moscow's message and direct action against any anti-Kremlin group or individual have been unambiguous.<sup>51</sup> Fear is an efficient weapon in silencing unwanted messengers.

### **The Essence of Russian Hybrid Warfare: Gerasimov Doctrine and Whole-of-Government Approach**

Though the previously discussed influence methods might seem isolated and disparate, the Russian hybrid warfare concept is a decisive cumulative approach organized by a centralized command. In hybrid warfare, several state and non-state actors combine kinetic, cyber, physical, psychological, social, and nonphysical actions to cause intimidation, instability, polarization, escalation, and powerlessness to act in a targeted state. Hybrid warfare's essence is to operate in all domains across the conflict spectrum, undermining a targeted state's relative power, cohesion, and decision-making capacity below the level of a declaration of war.<sup>52</sup> Thus, as Russian general Valery Gerasimov stated, "War in general is not declared; it simply begins with already developed military forces."<sup>53</sup> Blurring the

line between peace and war and obscuring normal conditions with the fog of war are fundamental principles in Russian hybrid warfare. Its ultimate aim is to wear out, frustrate, confuse, disintegrate, and undermine adversaries without giving them a legal or moral means to respond.

Russia exploits the principles of Chinese military strategist Sun Tzu, “gaining the material and moral advantages such [that the] battle is won before it is fought” when attacking continuously against an enemy’s vulnerabilities.<sup>54</sup> Today, Russian economic or military power is not strong enough to directly challenge the US or NATO. Hence, Putin’s concealed offensives target societies’ weaknesses (cybersecurity, legislation holes, morale, and unity) to diminish the adversaries’ relative strength in the long-term power competition.<sup>55</sup>

Hybrid warfare is a whole-of-government approach, controlled and masterminded by Russia at the highest levels.<sup>56</sup> A NATO paper observes that “President Putin is the architect of strategy, a new/old Russian strategic method that can be summed up as the conduct of war via 5Ds: destabilization, disinformation, strategic deception, disruption, and, if need be, destruction.”<sup>57</sup> As previous hybrid warfare cases reveal, Putin’s authoritarian government effectively demonstrated all 5Ds during the 2010s. Affordability, effectiveness, and authoritarianism are some reasons why Russia has shifted toward the model of hybrid warfare characterized by centralized command and decentralized operation. Attacking democracies’ weaknesses with cyber, information warfare, covert operations, and proxy forces rather than building a conventional arms race is a more effortless way to challenge US, NATO, and EU cohesion. However, it must be noted that Russia is still augmenting its conventional warfare ability by developing traditional land, air, sea, and space capabilities, the nuclear triad, A2/AD systems, cyber, and emerging hypersonic weapons.

The essence of hybrid warfare is associated with Russian general Valery Gerasimov’s chief of General Staff doctrine about nonlinear warfare and its predominant nonmilitary methods in modern conflicts.<sup>58</sup> The doctrine includes Gerasimov’s well-known illustration of Russian new-generation warfare that shows phases of a crisis and the role of nonmilitary and military measures.<sup>59</sup> The doctrine reveals how all instruments of power (DIME) have a role and how nonmilitary measures dominate (4:1 correlation) in a modern, nonlinear hybrid warfare environment.<sup>60</sup>

### ***Maskirovka*, Reflexive Control, and Centralized Command**

Admittedly, giving a single, clear definition of *Maskirovka* (deception) is difficult, but understanding its vital role in hybrid warfare from the tactical

to strategic level is essential.<sup>61</sup> Russia has expanded the traditional tactical- and operational-level battlefield *Maskirovka* for a broader, all-domain strategy and power competition concept.<sup>62</sup> Successful Russian strategic deception confuses the adversary's observe-orient-decide-act (OODA) loop and gains an advantage in time and space.<sup>63</sup> Along with using deception, centralizing command and control has created an edge in operational tempo and decision-making. In 2014, President Putin linked situation centers and created a new interagency information sharing and commanding system, the National Defense Management Center (NDCM).<sup>64</sup> The NDCM works in a national security framework connecting all critical actors, departments, agencies, and systems. The controlled, centralized whole-of-government approach creates an advantage to develop and implement comprehensive Russian defense strategies and plans.<sup>65</sup>

Russia has a long strategic military history in reflexive control that combines deception, effective persuasion, and manipulation to compel adversaries to inevitably act according to select information fed by the Russian state or proxy actors.<sup>66</sup> Reflexive control is a crucial element in Russia's hybrid warfare playbook. Instead of straightforward occupation and large-scale military force operations, Russia exploits covert and overt indirect approaches to change the targeted state's or group's behavior to one that favors Russia. Hybrid warfare subdues the adversary to cooperate either by coercion or by allowing the adversary to lead toward the desired direction.<sup>67</sup> Russian actions in Ukraine and against NATO ultimately worked according to its concept of reflexive control. Denial and deception campaigns showed the red line for NATO expansion, deterred the West from intervening in the crisis militarily, and managed to support pro-Russian separatists and public opinion in Ukraine.<sup>68</sup> In sum, hybrid warfare challenges the international community, state-level decision-makers, and individuals by increasing confusion and coercion, applying overwhelming pressure, and masking the line between conflict and peace with multiple military and nonmilitary actions.<sup>69</sup>

### **Countering Hybrid Warfare: Comprehensive Security Approach**

*Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them.*

—Jens Stoltenberg, NATO Secretary General, 2015

The following discussion analyzes countermeasures that states and organizations should implement against hybrid warfare. Above all, it explores

why comprehensive security provides a well-suited concept to improve readiness, situational awareness, resilience, and deterrence. Researchers at the Hybrid CoE compared the best hybrid warfare countermeasures among Britain, Finland, Sweden, France, Estonia, and the EU. They found shared features in the following areas: a whole-of-government / whole-of-society approach, vulnerability assessment, cyber defense, creativity in reaching out to the private sector, and improvement of situational awareness and (counter) intelligence.<sup>70</sup> The following countermeasures analysis encompasses but is not limited to Hybrid CoE's findings.

### ***Recognizing the Problem, Assessing Vulnerabilities, and Improving Situational Awareness***

First, states and security actors should identify the problem, increase understanding of hybrid warfare, assess vulnerabilities, and explore countermeasures. Russia's versatile multidomain attacks rapidly challenged politicians, senior leaders, military officers, and NGOs. However, countermeasures have developed more slowly. The symmetrical force-on-force response does not necessarily secure one's vulnerabilities or deter attackers because the defender must employ a wide array of actions concurrently in all domains and with all resources and instruments of power (DIME).

Cooperation between authorities, businesses, NGOs, and citizens aids in recognizing and understanding cumulative weaknesses and opportunities before and during attack. Situational analysis and information sharing form the primary layer of an efficient defense against hybrid attacks. A thorough assessment reveals what elements require protection, how best to influence the adversary, and which authority has the optimal resources to implement the actions. Nevertheless, most cases are usually so complicated that counteractions outweigh a single authority's resources and know-how. For that reason, the government should gather information broadly, foster interagency cooperation, and ask for other entities' help if the situation dictates. Collaboration supports connecting the dots, examining creative countermeasures, seeing the whole picture, and sensing time-critical information requirements. All of these elements are required to increase situational awareness and mitigate hybrid aggressions.

Today's complex hybrid operating environment sets high situational awareness requirements from the tactical through the strategic level across states and organizations. The EU has recognized the importance of information and intelligence sharing and the value of revealing best practices and lessons learned.<sup>71</sup> Security agencies should enhance monitoring warnings and indications. However, the main problem usually is that in-

telligence information does not spread across a broad range of stakeholders, which hampers early warning signs.<sup>72</sup> Western civilian-military intelligence exploits multiple intelligence, surveillance, and reconnaissance (ISR) capabilities, but cyberspace and the digitalized environment also require more robust counterintelligence. Some countries have recognized this need and proactively made cyber intelligence legislation changes to enhance intelligence collection within and outside the country.<sup>73</sup> Detection through indicators and warnings enables the monitoring of Russia's "known unknowns." Additionally, the systematic analysis discovers "unknown unknowns."<sup>74</sup>

One challenge with hybrid warfare is that the targeted state is continuously reactive. A hybrid attacker disturbs the decision-making process by saturating the information domain. The targeted state therefore needs to sharpen its OODA cycle to operate faster than the adversary. Maintaining situational awareness superiority and the operations tempo is exceptionally challenging for reactive defenders but not impossible. As discussed, recognizing and analyzing the situation among critical actors is the first significant step in building a coherent counteraction strategy. After a multifaceted collaborative analysis, the following essential questions arise: What should be done? Who has the overall responsibility for responding? And when is the best time to act? These crucial questions must be answered before any actions can be implemented. The following describes deterrence methods against hybrid warfare.

### ***Detering against Hybrid Warfare***

How to deter against hybrid warfare is a relevant question for tomorrow's decision-makers. Detering hybrid warfare is more complicated than deterring traditional conventional military attacks. Nevertheless, hybrid deterrence generally employs the same elements as traditional deterrence—a balance of escalation, signaling, and denial and punishment.<sup>75</sup>

States should incorporate proportional punishment methods in their arsenal because current hybrid attackers survive largely unpunished or encounter only economic sanctions.<sup>76</sup> According to Hybrid CoE research, states need to focus on future-oriented, strategic deterrence.<sup>77</sup> That is, they should increase their ability to impose costs against aggressors in addition to responding reactively and mitigating threats.<sup>78</sup> Deterrence by punishment has usually been absent against attacks below the level of armed conflict, allowing the hybrid attacker to get away without appropriate countermeasures. A shift from a responsive to a preventive role prevents further aggression by creating cost-benefit calculus problems for adversar-

ies while strengthening resistance and increasing trust among citizens and allies. All DIME instruments and the influence spectrum from soft to hard power should be on the table when deciding on deterrence, retaliation, and counteractions. Otherwise, states are handicapped by limiting themselves to using only part of their power and ability to respond. Sanctions have been imposed, but the West needs more tools to be strategically predictable while still being operationally and tactically unpredictable.

Researcher Mikael Wigell recommends democratic deterrence as a new strategic concept. In this concept, states can turn democratic vulnerabilities into strengths through implementing deterrence by denial and punishment.<sup>79</sup> More precisely, Western societies should demonstrate that security and democracy do not rule each other out but support each other hand in hand. Russian hybrid warfare specifically targets the dilemma between security and freedom of speech. However, if democracies close their societies, they will act according to the Russian reflexive control playbook and “voluntarily take a predetermined action towards censorship and totalitarianism.”<sup>80</sup> In the long run, democratic deterrence strengthens democratic values, freedom of speech, equality, and security infrastructures to improve governance, resilience, and robustness—an excellent deterrent against Russia’s actions.<sup>81</sup>

Continuous competition below armed conflict, new disruption methods in cyberspace, and the role of disinformation are trends that force targeted states to find new methods to mitigate and deny risks.<sup>82</sup> Cyber deterrence is a relatively new and unexamined field. Cyberspace is like the Wild West, where rules-based norms and countermeasures chase hostile technological and conceptual development. An Estonian cyber case demonstrates the difficulty of defining a collective response against cyberattack. Estonia asked NATO to invoke Article V (an attack on one is an attack on all). However, NATO responded that it had no retaliation options because a cyberattack was not equivalent to an armed attack.<sup>83</sup> After a decade, the same cyber-related proportionality, attribution, and retaliation problems are still on the table. States and international organizations should establish rules, treaties, and legitimacy agreements regarding cyberspace aggression, as with nuclear and conventional weapons during the Cold War. Before solving cyber-deterrence implementation, digital security legislation rules and the status of non-state actors require critical analysis.

Deterrence by denial enhances resilience by using a total defense concept encompassing a broad spectrum of collaborating security actors.<sup>84</sup> Sweden, Norway, and Finland have a tradition of this whole-of-government approach. Essentially, Finland’s comprehensive security is



more like a whole-of-society approach because—along with authorities, business operators, civil organizations, and citizens—it assists everyday resilience and security.<sup>85</sup>

**Finnish comprehensive security model.** Finland's comprehensive approach secures society's vital functions through collaboration among authorities, the business community, organizations, nongovernmental organizations (NGO), and citizens. The government released its *Security Strategy for Society* guidance, where it harmonizes national preparedness principles and directs readiness actions for different branches.<sup>86</sup> Finland's long tradition in comprehensive security (WWII total defense concept) and broad whole-of-society integration have increased interest among states and organizations struggling with harmful Russian hybrid attacks.<sup>87</sup>

Interagency collaboration and cooperation are commonplace in many states, but what makes Finland's model unique and efficient is its connectivity to state and non-state actors.<sup>88</sup> Hybrid warfare targets authorities, businesses, and organizations, increasing the role of NGOs and the private sector in the globally connected security realm. No organization or decision-maker can have situational awareness without information from other stakeholders. Thus, sharing best practices, knowledge, actions, and systems across civilian and state authorities enhances state-led security. A comprehensive approach where information flows freely between stakeholders improves identifying signals and threats early enough to start the required analyzing, assessing, and decision-making processes.

The comprehensive security approach works best to combine information and actions across central, regional, and local actors. Departments' strategic guidance should smoothly operationalize to concrete actions at the regional and local levels. Specifically, communication, cooperation, and procedures must be practiced and tested across horizontal and vertical command chains. In the Finnish model, joint preparedness is a general principle to enhance resilience, strengthen security procedures, and augment a sense of security.<sup>89</sup>

The comprehensive security model necessitates commitment, active joint planning, training, and implementation. Otherwise, the ambitious whole-of-society approach does not concretize. In a challenging, uncertain threat environment, broad cooperation, information sharing, and communication increase know-how and trust among key players, enabling better decisions, risk analysis, and the discovery of cost-efficient ways to improve weaknesses and situation-specific solutions.<sup>90</sup>

Hybrid warfare comprises various cross-domain power instruments. Correspondingly, a comprehensive security model should exploit multi-

domain and DIME instruments, including but not limited to national military defense, diplomacy, information, cyberspace, economics, internal security, physical infrastructure, psychological resilience, and leadership. When the whole-of-society model excels, responsibilities, resources, and actions align with a matrix of actors. The concept corresponds to joint military operations where a supported commander has the overall coordination responsibility and primary resources, but supporting commanders underpin joint efforts with their knowledge and resources. As a result, a comprehensive security model responds efficiently to clandestine cyberattacks, border security intrusions, or election meddling at the top and grassroots levels.

**NATO and EU countermeasures.** Also, organizations like NATO and the EU have recognized actions against hybrid warfare. NATO's immediate responses focus on cost-efficient, concrete steps to improve realistic exercises, intelligence, strategic communication, new technologies, and education.<sup>91</sup>

Sharpening early warning systems, ISR capabilities, and joint force readiness is a clear-cut requirement for the military.<sup>92</sup> Similarly, military and security providers should address vulnerabilities in cyberspace and innovate gray zone influencing. There needs to be a thorough inspection and adjustment of legislation, the rules of engagement, and identification procedures to discover and address any existing loopholes. NATO is anxious about hybrid warfare's influence in the Baltic states, where a sizable Russian ethnic population might give Russia self-justification for interfering in interstate affairs.<sup>93</sup> To counter hybrid warfare, NATO has underlined securing critical information, networks, and capabilities and finding simple ways to respond, resist, and deter. Defensive and offensive cyberspace capabilities are under states' sovereignty; however, inside NATO member states, a needed critical discussion is whether cyberattacks correlate with armed aggression.

The EU's countermeasure approach sets principles to mitigate the threat by improving understanding of hybrid warfare, recognizing countries' vulnerabilities, improving awareness, building resilience, deterring aggression, stepping up strategic communication, and promoting collaboration with EU and NATO countries.<sup>94</sup> Specifically, countermeasures mirror the states' whole-of-government model but at the organizational level. Member states have varying vulnerabilities, such as inefficient military, energy dependencies, and/or sensitive ethnicity issues. Additionally, along with national weaknesses, the EU should analyze its institutional weaknesses

and the risks threatening all member states, including cyberattacks and energy security.<sup>95</sup>

A key finding at the EU and NATO organizational levels is that ultimately states are responsible for countering the hybrid threats. Therefore, national sovereignty and sensitive weaknesses inside states complicate reactions at the more significant organizational level. Nevertheless, the EU and NATO should also improve resilience and deterrence against hybrid warfare. Developing cooperation between the EU, NATO, and their member states in exercises, workgroups, and development programs is vital to improving overall understanding and sharing best practices across security actors. One excellent example of concrete collaboration was creating the Hybrid CoE to conduct research and organize training and exercises.<sup>96</sup>

### **Recommendations**

The comprehensive security model is an overarching framework to counter hybrid warfare. However, there are plenty of single and combined measures that states and security organizations can use to counter and mitigate hybrid warfare. The following highlights actions that increase resilience at the national security level and recommends concrete, immediate responses to improve readiness and deterrence for malicious Russian hybrid warfare.

Though open societies today are digitally vulnerable and reactive, states and security providers should not acquiesce to fate in response to hybrid warfare. Rather, democracies should mitigate risks and explore countermeasures to increase overall resilience against cyber and information war. Fostering democratic values, amplifying truth-based narratives, embracing transparent governance, encouraging all-encompassing education, using critical thinking, and facilitating cooperation among authorities and businesses are essential skills in countering adversaries' aggressions.

### ***Achieving Resilience: Learning by Doing***

Authorities should train and educate personnel on the need for coordination, decision-making, and analysis when responding to threats. Since hybrid warfare targets the whole of government and society at large, states require comprehensive means to mitigate threats jointly across authorities, organizations, and citizens. Thus, it is essential to expose strategic and tactical decision-makers to solving wicked problems beforehand: sweat during peacetime saves blood in war. Officials should organize tabletop, command post, and real-life exercises using hybrid warfare cases. By

teaching and communicating, working, and coordinating with state actors, NGOs, industries, and officials, the state can develop enlightened, broad-minded leaders and operationally excellent actors to counter the fog of Russian hybrid warfare.

Moreover, joint training exponentially increases mutual trust between actors, easing and harmonizing actions during a crisis. Making sharing best practices and information a habitual skill is one beneficial outcome of joint training and collaboration. No authority, official agency, or department can handle complicated effects alone. Educating and linking civilian and military leadership to work jointly maximizes leveraging the best tools in a crisis, thus developing resilience and deterrence. All-encompassing training that includes partners fosters critical thinking. A lack of time and resources can hinder multinational training opportunities. However, even short training events and briefings among allies might innovate thinking about readiness, resilience, and deterrence. Investment in education is the most efficient way to increase the state's resilience and deterrence options in the long run.

Besides emphasizing cognitive concepts, officials should address vulnerabilities in the security infrastructure. Hybrid threat mitigation and deterrence require secure networks, virus protections, cyber defensive measures, and advanced surveillance systems, along with improved physical infrastructural security measures. When procuring military or state-owned complex systems, security specialists should have a role in considering cyberspace effects and vulnerabilities in the hardware and software. Likewise, since it is a human who usually leaves the cyber door open, organizational culture and concepts should support responsible digital behavior.

### ***Improving Information, Intelligence, and Situational Awareness***

Because there are no quick wins against dirty information warfare, that realm might be the hardest to mitigate. However, Western democracies should continue to maintain credibility, trustworthiness, transparency, and truth as weapons to educate and enlighten their citizens against modern disinformation. In the battle against information warfare, the West might suffer some short-term losses against authoritarian state aggressive narratives. However, truth and the ability to read information and media are the only ways to maintain trust, control the narrative, and influence people in the long run.

Educating people on how to analyze information and media is a resource well spent. All age groups should know an online code of conduct

and evaluate the legitimacy of media sites. At the state level, resilience against cyberattacks and data breaches increases when all employees' basic cyber knowledge is encouraged. Policy makers, spokespersons, and military leaders should be trained in strategic communication. Usually, the deeper the crisis, the more involved a human perspective should be in strategic communication and narratives. Selecting articulate, credible spokespersons to represent organizations is an excellent way to improve resilience against harmful hybrid attacks.

We need to adapt, act, and outthink more quickly than our foes. States should improve ISR connectivity among key agencies to foster shared interagency situational awareness. The government should reduce silo structure, reducing tempo and leaving decision-makers to operate with an incomplete picture. Thus, a comprehensive whole-of-government/society model would be the preferred option to increase hybrid warfare responsiveness. Organizational learning and sharing best practices should be commonplace not just in a particular department but broadly across authorities and organizations with roles in national security. We should ask questions like who else needs to know, which organization has the best resources, and how can we best counter, limit, mitigate, and deter the subsequent hybrid warfare attacks?

Undertaking such actions leads to increased requirements for situational awareness, intelligence, and decision-making. In most cases, a single state, agency, or business partner does not have all the resources or know-how to solve the problem. Therefore, interagency cooperation, information sharing, and state-level communication are vital.

However, these endeavors cannot succeed without clear commitment, organized procedures, and training. Broad countermeasures against hybrid warfare, in the long run, require that the state implement a whole-of-government approach. At best, it should involve private-sector players and the education of its citizens.

## **Conclusion**

This article analyzed Russian hybrid warfare actions and the vulnerabilities of modern digitalized societies and outlined the broader concept of hybrid warfare. It identified effective countermeasures against hybrid warfare and introduced a comprehensive security model as a critical resilience and deterrence approach.

While propaganda, asymmetric operations, and dispersal of cohesion are not new coercion methods, in today's intertwined global, uncertain, ambiguous, and automatized world, the effectiveness of these tools has

increased manifold. The challenge is especially significant in open, modern, information-driven democracies where affected individuals or institutions do not necessarily understand that they are intentionally targeted.

Russian hybrid warfare creates instability with multidomain attacks and clandestine operations. The combined impact of hybrid attacks undermines targeted states' situational awareness, cohesion, and decision-making in all war-fighting domains, including cyber and information. With this intention, Russia aims to achieve its options in a cumulative approach by competing, challenging, and targeting its adversaries below the level of open conflict or war. Attacking against weaknesses in Western legislation, morale, and unity makes an adversary relatively weaker. Diminishing an adversary is easier for Russia to accomplish than increasing its strengths. By doing so, Russia aims to increase its relative position and revive its role as a great power, at least in the Eurasian area.

President Putin and his high elite mastermind hybrid warfare in an entirely centralized way, and it truly is a whole-of-government approach. Similarly, combining a comprehensive national security approach and cooperation provides the best platform and measures for targeted states to act against, mitigate, and deter overt and covert hybrid assaults. Joint training, education, and information sharing improve resilience and preparedness. Enhancing the nation's security, resistance, and countermeasures in a complex hybrid warfare environment necessitates the transition from reactive operations to existing, well-trained, and practiced active day-to-day operational principles. Additionally, preventing further hybrid warfare attacks requires fostering state-level deterrence and retaliation measures.

Increasing awareness of hybrid warfare, Russian deception-centric thinking, and appropriate countermeasures is essential for tomorrow's decision-makers, strategic leaders, state authorities, and even citizens. Exploiting an adversary's vulnerabilities has always been part of a winning strategy, as seen in Sun Tzu and Clausewitz's writings. Indeed, Russian hybrid warfare is just another means to exploit adversaries' weaknesses. However, Western democracies and security organizations can turn the tables and counter hybrid warfare by changing their reactive mindset to taking active measures.

**Lt Col Tuukka Elonheimo, Finnish Air Force**

Colonel Elonheimo has served as the deputy chief of Air Force operations, Finnish Air Force Command; chief of flight operations, Finnish Air Force Command; and strategic plans team chief, Plans and Policy Division, Finnish Defense Command. He also held staff positions as an operational and strategic planning expert. Colonel Elonheimo is a graduate of Air War College, Air University, Maxwell AFB, and completed a two-year general staff officer's degree at the Finnish National Defense University.

## Notes

1. James A. Winnefeld, Michael J. Morell, and Graham Allison, "Why American Strategy Fails: Ending the Chronic Imbalance between Ways and Means," *Foreign Affairs*, 28 October 2020, 3, <https://www.foreignaffairs.com/>.
2. Joint Chiefs of Staff, Joint Doctrine Note 1-18, *Strategy*, 25 April 2018, GL-1, vii, <https://www.jcs.mil/>.
3. András Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report 43 (Helsinki: The Finnish Institute of International Affairs, 2015), 40–43, <https://www.fia.fi/>.
4. James W. Browning, *Leading at the Strategic Level in an Uncertain World* (Washington, DC: Dwight D. Eisenhower School for National Security and Resource Strategy National Defense University, 2013), 18–19.
5. Rácz, *Russia's Hybrid War in Ukraine*, 28–37.
6. Carl von Clausewitz, ed. and trans. Peter Paret and Michael Howard, *On War* (Princeton, NJ: Princeton University Press, 1989), 119–20.
7. Benjamin Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 230–32.
8. Laura Rosenberger, "Making Cyberspace Safe for Democracy: The New Landscape of Information Competition," *Foreign Affairs* 99, May/June 2020, 146–59, <https://www.foreignaffairs.com/>.
9. Hybrid Center of Excellence (CoE), *Trends in the Contemporary Information Environment: Hybrid CoE Expert Pool Meeting on Information*, Hybrid CoE Trend Report 4 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, May 2020), 22, <https://www.hybridcoe.fi/>.
10. Joseph S. Nye, Jr., "Countering the Authoritarian Challenge – Public Diplomacy, Soft Power, and Sharp Power," *Horizons*, no. 15 (Winter 2020): 98, <http://www.cirsd.org/>.
11. Department of Defense, *Cyber Strategy Summary 2018* (Washington, DC: Department of Defense, 2018), 1, <https://media.defense.gov/>.
12. Magnus Normark, *How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks*, Hybrid CoE Strategic Analysis 15 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, April 2019), 2–3, <https://www.hybridcoe.fi/>.
13. Ralph Thiele, "Artificial Intelligence – A Key Enabler of Hybrid Warfare," Hybrid CoE Working Paper 6 (The European Centre of Excellence for Countering Hybrid Threats, Helsinki, 6 March 2020), 6, <https://www.hybridcoe.fi/>.
14. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus, and Giroux, 2020), 11.
15. Buchanan, *Hacker and the State*, 212–13.
16. Hybrid CoE, *Trends in the Contemporary Information Environment*, 4, 7.
17. Hybrid CoE, *Countering Disinformation: News Media and Legal Resilience*, Workshop organized by the Hybrid CoE and the Media Pool, part of the Finnish Emergency Supply Organization, 24–25 April 2019, Hybrid CoE Paper 1 (Finland: The European Centre of Excellence for Countering Hybrid Threats, November 2019), 10, <https://www.hybridcoe.fi/>.
18. Clausewitz, *On War*, 87–89.

19. Fred Charles Iklé, *Every War Must End*, rev. ed. (New York: Columbia University Press, 2005), 1–16.
20. Patrick Cullen, *Hybrid Threats as a New “Wicked Problem” for Early Warning*, Hybrid CoE Strategic Analysis 8 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, May 2018), 2, <https://www.hybridcoe.fi/>.
21. Elbridge Colby and Jonathan Solomon, “Facing Russia: Conventional Defence and Deterrence in Europe,” *Survival* 57, no. 6 (November 2015): 21, <https://doi.org/10.1080/00396338.2015.1116146>.
22. Robert Dalsjö, Christofer Berglund, and Michael Jonsson, *Bursting the Bubble? Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*, FOI-R-4651-SE (Stockholm: Swedish Defense Research Agency, March 2019), 9, <https://www.foi.se/>.
23. Heidi Reisinger and Aleksandr Goltz, *Russia’s Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*, NATO Defense College Research Paper no. 105 (Rome: NATO Defense College, Research Division, November 2014), 3–5, <http://www.ndc.nato.int/>.
24. Colby and Solomon, *Facing Russia*, 22.
25. Todd Harrison et al., *Space Threat Assessment 2020* (Washington, DC: Center for Strategic and International Studies, March 2020), 25–27, <https://www.csis.org/>.
26. Harrison et al., *Space Threat Assessment 2020*, 25–27.
27. Harrison et al., 25–27.
28. William A. Perkins, “Component Integration Challenges Presented by Advanced Layered Defence Systems (A2/AD),” *Three Swords Magazine*, no. 33 (March 2018): 56, <https://www.japcc.org/>.
29. Department of Defense, *Cyber Strategy Summary 2018*, 1.
30. Emily Tamkin, “10 Years after the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?,” *Foreign Policy*, 27 April 2017, <https://foreignpolicy.com/>.
31. Tamkin.
32. Tamkin.
33. Joseph S. Nye, “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (January 2017): 48–49, [https://doi.org/10.1162/ISEC\\_a\\_00266](https://doi.org/10.1162/ISEC_a_00266).
34. US Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report* (Arlington, VA: US Cyberspace Solarium Commission, March 2020), 8, <https://sites.google.com/>.
35. Buchanan, *Hacker and the State*, 288–305.
36. Rid, *Active Measures*, 12.
37. Nye, “Countering the Authoritarian Challenge,” 105.
38. Nye, 104–5.
39. Marek N. Posard et al., *From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections* (Santa Monica, CA: RAND Corporation, 2020), 1, <https://www.rand.org/>.
40. Buchanan, *Hacker and the State*, 213–20.
41. Nye, “Deterrence and Dissuasion in Cyberspace,” 48.
42. US Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report*, 11.
43. US Office of the Director of National Intelligence, *Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Inci-*



dent Attribution" (Washington, DC: Office of the Director of National Intelligence, 6 January 2017), 1–4, <https://www.dni.gov/files/>.

44. US Office of the Director of National Intelligence, 1–4.

45. Kenneth A. Schultz, "Perils of Polarization for U.S. Foreign Policy," *Washington Quarterly* 40, no. 4 (October 2017): 21–22, <https://doi.org/10.1080/0163660X.2017.1406705>.

46. Normark, *How States Use Non-State Actors*, 3.

47. Normark, 4–5.

48. Margarete Klein, *Private Military Companies – a Growing Instrument in Russia's Foreign and Security Policy Toolbox, Hybrid CoE Strategic Analysis* 17 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2019), 3, <https://www.hybridcoe.fi/>.

49. Klein, 3.

50. Sir David Omand, "From Nudge to Novichok: The Response to the Skripal Nerve Agent Attack Holds Lessons for Countering Hybrid Threats," Hybrid CoE Working Paper 2 (The European Centre of Excellence for Countering Hybrid Threats, Helsinki, 18 April 2018), 2, <https://www.hybridcoe.fi/>.

51. Patrik Reevel, "Before Navalny, a Long History of Russian Poisonings," ABC News, 26 August 2020, <https://abcnews.go.com/>.

52. Reevel.

53. John Allen et al., *Future War NATO?: From Hybrid War to Hyper War via Cyber War*, Supporting Paper of the GLOBSEC NATO Adaptation Initiative (Bratislava, Slovakia: GLOBSEC, 2017), 12, <https://www.globsec.org/>.

54. Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russian Report 1 (Washington, DC: Institute for the Study of War, September 2015), 11, <http://www.understandingwar.org/>.

55. Antulio J. Echevarria II, *Military Strategy: A Very Short Introduction* (Oxford: Oxford University Press, 2017), 2.

56. Snegovaya, *Putin's Information Warfare in Ukraine*, 9–11; and Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4 (October 2016): 554–59, <https://doi.org/10.1080/13518046.2016.1232541>.

57. Allen et al., *Future War NATO?*, 11.

58. Rącz, *Russia's Hybrid War in Ukraine*, 48–49.

59. Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," War on the Rocks, 11 March 2016, <https://warontherocks.com/>.

60. Kofman.

61. Pasi Kesseli, ed., *Venäjän Asevoimat Muutoksessa: Kohti 2030–lukua* [Russian armed forces in transition: toward the 2030s], National Defence University Series 1, Research Publication no. 5 (Helsinki: National Defence University, 2016), 23–25.

62. Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (April 2004): 239, <https://doi.org/10.1080/13518040490450529>.

63. Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books / Little, Brown, 2004), 327–44.

64. John Allen et al., *Future War NATO?*, 12.

65. John Allen et al., 12.

66. "Russia, Reflexive Control, and the Subtle Art of Red Teaming," *Red Team Journal*. October 2016.
67. Thomas, "Russia's Reflexive Control Theory," 239.
68. Annie Kowalewski, "Disinformation and Reflexive Control: The New Cold War," *Georgetown Security Studies Review*, 1 February 2017, <https://georgetownsecuritystudies-review.org/>.
69. European External Action Service (EEAS), "Food-for-Thought Paper 'Countering Hybrid Threats,'" EEAS (2015) 731, *Council of the European Union*, 2015.
70. Gregory F. Treverton et al., *Addressing Hybrid Threats* (Bromma: Swedish Defense University, 2018), 79–80.
71. EEAS, "Countering Hybrid Threats."
72. EEAS.
73. Treverton et al., *Addressing Hybrid Threats*, 79–80.
74. "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare," Multinational Capability Development Campaign (MCDC) project, March 2019, 3–4, <https://assets.publishing.service.gov.uk/>.
75. "MCDC Countering Hybrid Warfare Project," 3–4.
76. Mikael Wigell, "Democratic Deterrence: How to Dissuade Hybrid Interference," FIIA Working Paper 110 (Finnish Institute of International Affairs, Helsinki, September 2019), 13, <https://www.fiia.fi/>.
77. Vytautas Keršanskas, *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats*, Hybrid CoE Paper 2 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, March 2020), 6–7.
78. Keršanskas, *Deterrence*, 6–7.
79. Wigell, "Democratic Deterrence," 2.
80. Jānis Bērziņš, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *Journal of Slavic Military Studies* 33, no. 3 (July 2020): 368, <https://doi.org/10.1080/13518046.2020.1824109>.
81. Wigell, "Democratic Deterrence," 2.
82. Department of Defense, *Cyber Strategy Summary 2018*, 1.
83. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 30.
84. Wigell, "Democratic Deterrence," 11.
85. Wigell, 11.
86. *Security Strategy for Society*, Government Resolution, Security Committee of Finland, 2.11.17, 1, <https://turvallisuuskomitea.fi/>.
87. "Finland's Model for Comprehensive Security Viewed Effective against Hybrid Threats," press release, National Defense University, 11 June 2017, <https://maanpuolustus.korkeakoulu.fi/>.
88. Harri Mikkola et al., *Hybridivaikuttaminen Ja Demokratian Resilienssi – Ulkoisen Häirinnän Mahdollisuudet ja Torjuntakyky Liberaaleissa Demokratioissa* [Hybrid influence and democratic resilience: possibilities and ability to combat external harassment in liberal democracies], FIIA Report 55 (Helsinki: Finnish Institute of International Affairs, May 2018), 117–20, <https://www.fiia.fi/>.
89. *Security Strategy for Society*, Government Resolution, 5.
90. *Security Strategy for Society*, 25.
91. John Allen et al., *Future War NATO?*, 15–16.

92. John Allen et al., 15–16.
93. David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica, CA: RAND Corporation, 2016), 3, <https://doi.org/10.7249/RR1253>.
94. "MCDC Countering Hybrid Warfare Project," 3–7.
95. "MCDC Countering Hybrid Warfare Project," 3–4.
96. "A Europe That Protects: Countering Hybrid Threats," European Union External Action Service, Brussels, 13 June 2018, <https://eeas.europa.eu/>.

*The Russian Understanding of War: Blurring the Lines between War and Peace* by Oscar Jonsson. Georgetown University Press, 2019, 260 pp.

This doctoral dissertation turned paperback written by Oscar Jonsson is unlike most texts in the literature of this field. Dr. Jonsson holds a PhD from King's College London's Department of War Studies and is the director of the Stockholm Free World Forum—a foreign and security policy think tank based in Sweden. While many geopolitical works superimpose (albeit often subconsciously) the assumptions of the analyst upon that which is being analyzed (mirror imaging), *The Russian Understanding of War* seeks to pierce Moscow's strategic calculus and the “nuances of the Russian language” (p. ix) to answer the question, “Has the Russian understanding of the nature of war changed, and if so, how?” (p. 4).

Jonsson frames the problem in the introduction by ensuring the audience understands the distinction between Clausewitz's “character of war” (something that perpetually evolves with technology) and the “nature of war” (something generally regarded as immutable). With the lexicon established in support of the thesis question, the author then divides his treatise into four main sections. Section 1 (“The Soviet Understanding of War”) examines the view of the collective USSR as the intellectual foundation for the Russian Federation's initial cadre of political and military leadership—with particular emphasis on the uniformity of Soviet political and military thought as an extension of Marxism-Leninism, Hegelian dialectics, and the Communist Party. Similar to Clausewitz, Lenin regarded violence and armed conflict as requisites for war. However, Lenin's understanding of “politics by other means” differed on the basis that the Soviets believed war to be a paradoxical evil that could only be eliminated by establishing the dictatorship of the proletariat worldwide. Section 2 (“The Russian Understanding of War after the Dissolution of the Soviet Union”) subsequently outlines how the Russian Federation's views regarding the nature of war evolved. It stresses the gradual yet notable departure from the traditional understanding of Clausewitz as incorporated by Lenin, Stalin, and others into Communism as the official worldview of the party and the state. Finally, section 3 (“Information Warfare”) and section 4 (“Color Revolutions”) leverage the philosophical foundation of the first two sections to examine Russia's understanding of war relative to what it perceives as two of its greatest external/internal security threats. Ultimately, “Russian threat perception is the backdrop to Russian offensive action” (p. 121).

This book is a remarkable and timely work of scholastic achievement with key insights for a geopolitical period of great power competition. Dr. Jonsson concludes that, as the title suggests, the Russian strategic calculus

blurs the lines between war and peace. He articulately and definitively demonstrates that the principal political and military elites of Russia today believe that either the nature of war has completely changed to include “non-violent” actions or that the fundamental definition of “violence” must be expanded to include the nontangible and nonlethal. In either case, the net effect remains that Moscow is corporately shifting its focus toward the political goals of war rather than focusing solely on its means (“armed violence”). Moreover, Jonsson adeptly balances what the Russian inner circle actually believes and what it states publicly, noting that formally acknowledging its perceived change in war’s nature would go against concepts that inform both international law and Russian federal law “On Defense.” (Both rely on “armed violence” as the defining element of war, and organically declaring a change in war’s nature would be tantamount to unilaterally declaring a worldwide state of war.) The thesis question and its answer are supported not through an examination of Western experts writing about Russia (i.e., from an outsider’s perspective) but through an exhaustive examination of documents and speeches produced by Russian politicians, strategists, tacticians, and oligarchs. Thus, Jonsson effectively uses primary source materials to generate insights about the Russian understanding of war while simultaneously minimizing the risk for analytical bias by allowing the Kremlin et al. to speak for themselves.

Ultimately, this book is a must for anyone seeking to navigate the strategic competition environment or those attempting to understand why Russia behaves in the manner it does. It may be tempting to examine Russia through several centuries of Czarist and Communist history. However, it is paramount for military strategists and analysts to remember that the Russian Federation is less than 30 years old and, particularly since the ascendance of Vladimir Putin, still finding its identity in the post-Cold War era. The author focuses on the findings of his research rather than the tangible implications for US or NATO policy makers. This is perhaps the only area where the book could be improved, while in fairness such a weight of effort is common practice for a dissertation contributing to the body of knowledge in support of field practitioners. Woven throughout this book is a singularly profound sentiment that must be understood by those in the US national security apparatus. Specifically, the following fallacious assumption must be purged from US/NATO policy development: “Western states believe it is up to them to choose whether they enter a war with Russia or not” (p. 157).

Simply put, the Russian government is actively engaged in what it considers a “war” against the West, albeit one fought via nonmilitary means.

As such, the West must change the way it thinks about deterrence, competition, and conflict when engaging Moscow and when seeking to cooperate with nations in Russia's near abroad. In other words, "when Western states are taking actions that they perceive as being short of war—sanctions, democracy promotion, and information operations—but that are understood by Russia as amounting to war, there is a risk of unconscious and/or unintentional escalation" (p. 2). Regardless of whether or not one accepts that the nature of war has changed, the semantic aspects of that philosophical and academic debate must not overshadow the real and potentially dire consequences of ignoring how Russia thinks and conducts operations. As articulated by Sun Tzu, those seeking to overcome must first "know thy enemy."

Capt Jayson M. Warren, USAF

*Rebranding China: Contested Status Signaling in the Changing Global Order* by Xiaoyu Pu. Stanford University Press, 2019, 152 pp.

Author Xiaoyu Pu is an assistant professor of political science at the University of Nevada, Reno. This book is part of a series addressing diverse contemporary security challenges in Asia. In *Rebranding China*, the author claims that China has a duality status struggle—resulting from its rapid growth and development—that receives little attention by scholars and practitioners. Is it a developing country, a benign regional leader, an aspiring global leader, an unwilling global leader, or an emerging superpower? Is it playing a zero sum game with the international community or growing within the existing global order? The author asserts that China projects mixed messages to its domestic and international audiences and needs to better articulate its preferred status. Pu believes that how a country crafts its preferred image is vitally important. Sending mixed or confusing status signals can lead to geopolitical friction, distrust, and deep suspicions of China's real intent by its own people and the global community at large.

The author meticulously builds a case for China's poor status signaling by presenting many examples of how China exhibited confusing and sometimes contradictory foreign policy practices. He notes that China has a multiple audience dilemma, which gives incentives to maintain several identities with conflicting roles. China wants to be loved and feared at the same time. The challenge facing China is that all of its audiences receive China's status signaling at the same time.

China presents a rapidly rising and emerging power image to its domestic audience but a developing country image to international audiences. It demands accommodation on geopolitical interests such as the

Spratly Islands and South China Sea claims yet wants to be considered a developing country on economic matters. When seeking opportunities from international institutions, China uses emerging power status (its strengths in resources, population, and economy) while at the same time shirking social/welfare responsibility to the global community when convenient, thus emphasizing its weaknesses as a developing country.

Pu explains that China wants depth of interconnectedness with its neighbors, thereby creating reliance on and interdependence with China. China sends two messages within East Asia. The first is “don’t fear us,” and the second is that China’s rise mutually benefits its neighbors. China professes to bring peaceful order to the region through multilateral economic and security institutions such as the Shanghai Cooperation Organization, the Asian Infrastructure and Investment Bank, and the Belt and Road Initiative.

China claims it does not seek to overthrow the existing world order. After all, it is a primary beneficiary of the international system. However, the author notes that China is becoming more politically aggressive in regional/global posturing. It frequently leverages self-serving statecraft on national interest in an assertive and coercive manner with its neighbors. China is fearful of a US military presence in the Asia-Pacific region and wants Asian security left to Asians. A problematic by-product of China’s haphazard status signaling is evidenced by how the US interprets it. The US sees China wanting to displace a US presence in the Asia-Pacific by expanding its global economic/security influence and being the regional hegemon. This is leading the US to rethink its strategy toward China.

Pu ultimately views China as a rising power with minimal threat to the global community. China sees its domestic image as more important than its international status. The author suggests that a rising power’s domestic audience is more important than its international audience. China’s status signaling is contested because the country’s population and leadership do not have consensus on China’s position on the world’s stage. The Chinese Communist Party (CCP) promotes the idea that it is the only legitimate political force that can defend China’s honor and the only entity capable of holding China together.

The author believes that for China to compete as a rising power with the US, the CCP/China needs to be a better leader in the international normative order. Being a better leader entails a well-communicated grand strategy supported by policies that reflect the strategy in both action and intent. China’s dilemma is how it must project an international image of conflicting roles in ways that promote its national interests without an-

tagonizing or sending misperceptions that result in mistrust and fear by its own people, neighbors, and the world at large.

Pu superbly supports his thesis through countless well-articulated examples drawn from the literature and thought-provoking analysis. Arguably, the most notable contribution the author makes to the body of knowledge is in introducing status signaling into the international relations literature. His signaling model, supported by his rigorous examination and application, helps frame how foreign policy behaviors are shaped by rising powers. It can also be seen as a means for information communication to appropriate political figures to either change or continue various status beliefs they may claim.

This book is best read by international relations/affairs, political science, and Chinese scholars as well as applicable governmental entities, including military leaders and Asia-Pacific specialists. It is also a relevant read for those interested in learning how rising powers struggle to shape their domestic and international identity and grow from their mistakes.

Dr. David A. Anderson  
Professor of Strategic Studies  
US Army Command and General Staff College

*Russia Abroad: Driving Regional Fracture in Post-Communist Eurasia and Beyond*  
edited by Anna Ohanyan. Georgetown University Press, 2018, 200 pp.

When I was in high school, during the long-ago 1990s, my geography teacher had the class color a map of Europe using different hues to delineate regions. He specifically instructed us to color a portion of Eastern Europe dark red and label it the “shatter belt region,” a geographic area defined by the cultural and political clash of Western Europe, Russia, and the Arabic/Ottoman Middle East. A decade later, numerous reports and articles announced the dangers of “failed states,” ungoverned or lightly governed spaces that lacked the ability to police themselves, often harbored terrorists, and spread chaos throughout the regions in which they festered. Then, just a couple of years ago, we heard the warning of “frozen conflicts,” internal warfare or proxy combat that delegitimized any attempts a given state takes toward maintaining a central government, typically in the context of Russian actions in former Soviet states. The generational irony undergirding each of these labels is the seeming inevitability of globalization and increased regional interconnectedness that defined the era. These failures of governance, no matter the label, seemed an anachronistic outlier. After a generation in which the reality of state and regional fracture has not lessened, however, one has to wonder, Will the global community always be bedeviled by the specter of failed governance projects?



Anna Ohanyan, editor of this collection of essays titled *Russia Abroad*, argues yes. Failed or fractured states have existed for as long as we have sought to define the nation-state, a type of photo negative of those qualities we assess “successful” states in the international order to possess. Ohanyan, a distinguished professor of political science at Stonehill College, believes that we should concern ourselves less with how fractured states buck global trends toward interconnectedness and more with understanding the factors that drive fracture within the state. At their core, fractured states lack the intergovernmental reach, resiliency, and respect to execute full governance within their borders, thus preventing the establishment of a future foundation for regional connections that reach beyond, and through, borders.

While Ohanyan advances a holistic theory that, she believes, one can apply globally to understand troubled regions, the focus of her current work, as the title suggests, is on the “new” concept of regional fracture or frozen conflicts in Russia’s near-abroad. The actions taken by Putin’s Russia to destabilize its neighbors, while significant in the moment, are indicative of a set of centuries-long Russian/Soviet imperial policies that look to incorporate these borderlands into a greater Russian empire, contributor Robert Nalbandov states. While these policies intended to capture these regions in Russia’s imperial sphere, they also weakened local governance to preclude any revolutionary or separatist movements. This internal weakness persisted in the wake of the Soviet Union’s collapse and also set the conditions for Russia’s reentry, desired or otherwise, into the region during the 2000s and 2010s.

While the majority of contributors outline the role that recent Russian actions have played in destabilizing Eastern Europe, the Caucasus, and Central Asia, they also highlight other trends that contribute to state and regional fracture. They point to the outsized role played by nongovernmental organizations, moneyed and cultural elites, refashioned or recast histories, and persistent cultural norms in maintaining or exacerbating state weakness and regional fracture. Contributors all extended this model beyond Russia’s near-abroad, examining how Russia’s continued neo-imperial reach emphasizes long-simmering feuds and political instability. Dimitar Bechev (Western Balkans) and Mark Katz (Syria and the Levant) overlay Ohanyan’s theory of regional fracture with the other contributors’ Russo-focused theory of the legacy of Russian overreach, giving legitimacy to Ohanyan’s framework in areas beyond the post-Soviet hinterlands.

At times, the authors unwittingly also illuminate areas where the reality of state fragility and regional fracture draw similarities across seemingly unlike groups. In one of the most striking examples, David Lewis charts

how the rise of illiberal regionalism provides a means for the states of Central Asia to create an identity in the chaos of post-Soviet fracture and neo-liberalism (p. 119). “Illiberal regionalism” is defined as how the “focus on the role of shared ideas, norms, and beliefs provides a framework for some limited regional cooperation with a common discourse that is sharply at odds with the liberal norms that underpin most of Western theories of regionalism.” As Lewis notes, this regionalism often comes with the ascension of authoritarian “strongmen” who rely on a masculine, ethnographic sense of cultural unity in the face of uneven economic and social change. The perceptual rise of authoritarianism and illiberal democracy across the globe would seem an extension of what Lewis describes, and plumbing the depth of this thinking would add to a growing research field.

Ohanyan’s current work, beyond a thoughtful collection of intellectually rich essays, also provides a striking (and needed) counterpoint to a narrative of globalization that, while tested in the past, still holds sway today. *Russia Abroad* provides an interesting context to assess state fragility and regional fracture relative to Russia’s current machinations in its near-abroad. However, the ability to take the book’s theory of regional fracture and “mean-test” it globally is critical to understanding how states are, and are not, incorporated into an assumed global order. Further, it is critical to diagnose the seams and fractures in internal governance and identify those trends or vulnerabilities that may force them to widen. Finally, knowing how powerful interlocutors can pluck these fissures like harp strings, playing chaotic tunes of state collapse, will become a central part of building state and international resiliency toward illiberal agents—something likely to define the twenty-first century.

LTC Andrew Forney, USA

### **Mission Statement**

*Strategic Studies Quarterly* (SSQ) is the strategic journal of the Department of the Air Force, fostering intellectual enrichment for national and international security professionals. SSQ provides a forum for critically examining, informing, and debating national and international security matters. Contributions to SSQ will explore strategic issues of current and continuing interest to the larger defense community, and our international partners.

### **Disclaimer**

The views and opinions expressed or implied in SSQ are those of the authors and should not be construed as carrying the official sanction of the Department of the Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

### **Comments**

We encourage you to e-mail your comments, suggestions, or address change to [StrategicStudiesQuarterly@au.af.edu](mailto:StrategicStudiesQuarterly@au.af.edu)

### **Article Submission**

The SSQ considers scholarly articles between 5,000 and 15,000 words from US and international authors. Please send your submission in Microsoft Word format via e-mail to

[StrategicStudiesQuarterly@au.af.edu](mailto:StrategicStudiesQuarterly@au.af.edu)

### **Strategic Studies Quarterly (SSQ)**

600 Chennault Circle, Building 1405

Maxwell AFB, AL 36112-6026

**Tel (334) 953-7311**

View and Subscribe to *Strategic Studies Quarterly* at

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

### **Free Electronic Subscription**

Like SSQ on Facebook at <https://www.facebook.com/StrategicStudiesQuarterly>

*Strategic Studies Quarterly* (SSQ) (ISSN 1936-1815) is published by Air University Press, Maxwell AFB, AL. This document and trademark(s) contained herein are protected by law and provided for noncommercial use only. Reproduction and printing are subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the SSQ editor for assistance.