A Virtual Think Tank (ViTTa®) Report

September 2019

Kinetic and Non-Kinetic Tactics of Competing Powers Over the Coming Decade

Deeper Analyses
Clarifying Insights
Better Decisions

NSIteam.com

Produced in support of the Strategic Multilayer Assessment (SMA) Office (Joint Staff, J39)

Author

George Popp

Editors

Sarah Canna and George Popp

Please direct inquiries to George Popp at gpopp@nsiteam.com

What is ViTTa?

NSI's Virtual Think Tank (ViTTa) provides rapid response to critical information needs by pulsing a global network of subject matter experts (SMEs) to generate a wide range of expert insight. For the Strategic Multilayer Assessment (SMA) Future of Global Competition and Conflict project, ViTTa was used to address 12 key questions provided by the project's Joint Staff sponsors. The ViTTa team received written response submissions from 65 subject matter experts from academia, government, military, and industry. This report consists of:

1. A summary overview of the expert contributor response to the ViTTa question of focus.
2. The full corpus of expert contributor responses received for the ViTTa question of focus.
3. Biographies of expert contributors.

Cover image: https://ak9.picdn.net/shutterstock/videos/12961529/thumb/1.jpg

Table of Contents

Question of Focus

[Q2] What kinetic (e.g., weapon systems) and non-kinetic (e.g., disinformation campaigns, financial market manipulation, political tampering) tactics are and will be used by competing powers domestically and abroad to undercut US interests over the coming decade?

Subject Matter Expert Contributors

Bogdan Belei (Harvard University), **Lieutenant Colonel Jeffrey Biller** (US Naval War College), **Dr. Patricia J. Blocksome** (US Naval War College), **Dr. David T. Burbach** (US Naval War College), **Dean Cheng** (Heritage Foundation), **Dr. Nicholas J. Cull** (University of Southern California), **Michael Fabey** (Jane's Fighting Ships), **Dr. Michael W. Fowler** (US Air Force Academy), **Peter E. Harrell** (Center for a New American Security), **Dr. Peter Layton** (Griffith University), **Dr. Martin Libicki** (US Naval Academy), **Dr. Julia Macdonald** (University of Denver), **Dr. Jahara Matisek** (US Air Force), **Dr. Sean McFate** (National Defense University), **Dr. Lukas Milevski** (Leiden University), **Robert Morgus** (New America), **Dr. Christopher Paul** (RAND Corporation), **Linda Robinson** (RAND Corporation), **Dr. Jaganath Sankaran** (University of Texas at Austin), **Dr. Jacquelyn Schneider** (Hoover Institution), **Dr. Peter Schram** (Vanderbilt University), **Dr. Steve S. Sin** (University of Maryland START), **Dr. Robert S. Spalding III** (US Air Force), **Nicolas Véron** (Bruegel and Peterson Institute for International Economics), **Valentin Weber** (University of Oxford), **Ali Wyne** (RAND Corporation)

Summary Overview

This summary overview reflects on the insightful responses of twenty-six Future of Global Competition and Conflict Virtual Think Tank (ViTTa) expert contributors. While this summary presents an overview of the key expert contributor insights, the summary alone cannot fully convey the fine detail of the expert contributor responses provided, each of which is worth reading in its entirety. For this report, the expert contributors consider what kinetic and non-kinetic tactics are and will be used by competing powers domestically and abroad to challenge the United States and its interests over the coming decade.

Kinetic and Non-Kinetic Tactics of Competing Powers Over the Coming Decade

The tactics and techniques, both kinetic and non-kinetic, used by competing powers are evolving and will continue to evolve over the coming decade. United States supremacy in both kinetic and non-kinetic domains will be challenged as technological advancements continue to make it easier and more affordable for competitors across the globe to acquire and implement new technologies that enable them to more effectively compete across more domains.[1] It is unlikely, however, that the United States will lose its superiority in terms of kinetic tactics and conventional military capabilities. Contributors suggest, therefore, that the United States is likely to face its most significant challenges in non-kinetic spheres, as its competitors will likely have little interest

[1] See contributions from Belei, Blocksome, Fowler, Layton, Robinson, and Wyne.

in engaging in large-scale conventional conflict in which they would almost certainly operate at a significant competitive disadvantage.[2]

Instead, the strategies of competing powers are more likely to "focus on achieving their aims via methods that are deliberately intended to frustrate the United States preference for decisive warfare."[3] Moreover, as Dr. Michael Fowler of the US Air Force Academy articulates, in an attempt to mitigate the United States' conventional military advantages, competitors will likely "gravitate towards methods that are less reliant on physical destruction and place more emphasis on creating psychological effects" (i.e., exhaustion, denial, and subversion). Such unconventional methods to competition and conflict provide adversaries an avenue to achieving objectives while avoiding potentially costly conventional conflict and circumventing international conventions designed to prevent such conflict. As Dr. Patricia Blocksome of the US Naval War College notes, "only an unintelligent adversary would fight the United States in a conventional battle; what is far more likely is that the United States' adversaries will non-kinetically attack the systems on which the United States relies."

Ultimately, the contributors suggest that the operational environment over the coming decade is likely to be characterized by an increasing use of non-kinetic, asymmetric, and non-physical tactics across an increasing number of competitive domains, particularly the cyber and cyber-cognitive domains, by a widening set of potential adversaries.

Non-Kinetic Tactics: What to Expect from Competing Powers Over the Coming Decade

Contributors highlight an array of non-kinetic tactics that are likely to be used by competing powers over the coming decade to challenge the United States and its interests, including: information operations, political and economic influence operations, cyber operations, and proxy operations.

Information Operations

The most frequently cited tactic that competing powers will use over the coming decade to challenge the United States and its interests is information operations.[4] Information operations, as Dr. Jahara Matisek of the US Air Force explains, are the "tactical and strategic use of information and data to gain an advantage in various domains, and to achieve an objective—all without having to fire a shot." Information operations provide an avenue for competitors to challenge more dominant adversaries, like the United States, asymmetrically while avoiding costly escalation but still achieving important objectives.[5] Technological advancements have made it easier for competitors, large and small, to use and exploit information to challenge their adversaries. The development of social networks and online media platforms, for example, has provided competitors with "much more direct, targeted vectors [to use] disinformation" to influence large populations and challenge the United States and its interests.[6] This trend is likely to continue over the coming decade as the "ongoing revolution in the

[2] See contributions from Blocksome, Fowler, Robinson, and Wyne.
[3] See contribution from Blocksome.
[4] See contributions from Biller, Burbach, Cheng, Cull, Fabey, Fowler, Harrell, Layton, Matisek, McFate, Paul, Robinson, and Spalding III.
[5] See contribution from Paul.
[6] See contribution from Burbach.

way information is gathered, analyzed, and utilized (i.e., weaponized)" continues and "significant attack vectors" continue to emerge in the process for competitors to exploit.[7]

Competing powers are using and will continue to use information operations to disrupt, subvert, and exhaust their adversaries, both domestically and abroad.[8] Contributors highlight Russia, in particular, as a notable example of a competing power that is currently doing just that. To challenge its adversaries at the domestic level, Russia uses information operations to foment "societal disruption" and "chaos" amongst adversary populations. Russia's approach to information operations, as Dr. Peter Layton of Griffith University explains, "has been to amplify divisive social issues by employing wide-ranging disinformation attacks across a nation's political spectrum. Whether certain groups are supportive of Russian policies is immaterial, the key issue is to drive them to being more confrontational towards other groups." To challenge its adversaries at the international level, Russia uses information operations, particularly disinformation and propaganda, to create "division" and "disunity" between the United States and its allies and "disrupt" the current United States-led global order.[9] Finally, Russian meddling in foreign elections, particularly the 2016 United States elections, offers an example of how Russia uses information operations to challenge its adversaries (i.e., the United States and its allies) at both domestic and international levels by attempting to manipulate populations and social networks, sow disruption and chaos within foreign populations and amongst the international community, and subvert international rules and norms.[10]

Countering adversarial information operations efforts, however, may prove challenging for the United States given inadequacies in the international laws and norms governing such activities. Lieutenant Colonel Jeffrey Biller of the US Naval War College highlights this challenge, noting that, "despite the realization by the United States and its allies that information operations pose a serious threat to national and economic security, the perception by malicious actors is that coordinated response strategies have been slow to develop and unevenly implemented, resulting in the belief that information operations can be conducted with little risk. This combination of a target rich information environment and the ability to conduct operations with little perceived risk promises that information operations against the United States will continue to increase in the foreseeable future." Linda Robinson of the RAND Corporation offers a similar assessment, asserting that "the manipulation of the information environment using social media and other informational conduits enabled by worldwide communications and the largely unregulated information space is likely to continue apace or increase exponentially in those countries not sealed off by aggressive government firewalls."

Political and Economic Influence Operations

Political and economic influence operations are also frequently highlighted by contributors as tactics that competing powers will use over the coming decade to challenge the United States and its interests.[11] Political and economic influence operations consist of the use of political and economic levers of power by a competing

[7] See contribution from Biller.
[8] See contribution from Fowler.
[9] See contributions from Cull and Fabey.
[10] See contributions from Burbach and Matisek.
[11] See contributions from Blocksome, Burbach, Cheng, Fabey, Harrell, Morgus, Paul, Robinson, Schram, Sin, Spalding III, and Véron.

power to compel and/or pressure an adversary to take actions that they may otherwise not take.[12] In the political realm, competing powers will use influence operations to challenge the United States and its interests both domestically and on the international stage. Domestically, competitors will target Americans with political influence operations aimed at destabilizing the United States' "societal fabric" and eroding trust in United States institutions.[13] On the international stage, competing powers will use political influence operations to attack the United States' credibility and global influence, undermine the legitimacy and influence of international institutions and rules, and increase their own regional spheres of influence while isolating the United States from those regions of interest.[14] In the economic realm, competing powers will also use an array of economic influence levers to pressure and challenge the United States domestically and on the international stage. Examples of such economic influence operations are likely to include aggressive activities such as trade restrictions, tourism and travel restrictions, boycotts, regulatory harassment, sanctions, and financial market manipulation.[15]

Ultimately, the use of political and economic influence operations by competing powers to challenge the United States and its interests is and will remain a central element of global competition over the coming decade. As Blocksome concludes, "the current concept of 'great power competition' can be understood as political [and economic] warfare on the grand scale."

Proxy Operations

Contributors also highlight the use of proxy forces to pursue aggressive interests and objectives as a tactic that competing powers will use over the coming decade to challenge the United States and its interests.[16] Proxy forces are partners (both state and non-state) that a competing power can use to conduct competitive activities, challenge adversaries, and pursue strategic objectives on their behalf while not having to be directly involved in or associated with the actual on-the-ground activities.[17] Using proxy forces can be beneficial to competing powers, as it 1) creates plausible deniability (i.e., covertly supplied aid to proxies makes it difficult for adversaries to know if they are competing against the proxy as a solo actor, or if they are actually competing against both the proxy and a supporting actor), 2) increases operational reach (i.e., the use of proxies can expand competition or conflict to new areas of the globe; a competitor may be strong in one region, but if they partner with proxies in other regions, they can increase their ability to challenge an adversary in unexpected locations), and 3) decreases the potential risks and costs associated with challenging powerful adversaries (i.e., by sending resources and advisors to a competitive environment, but not committing forces, the costs are far less; and the risk of blowback is limited in the case of operational failure, as proxy failure would not produce the critical threat that would result if the supporting actor's own forces failed).[18]

Contributors offer several examples of how proxy forces are and will be used by competing powers over the coming decade to challenge the United States and its interests. Biller notes that China and Russia have effectively exploited proxy operations in a variety of contexts, particularly in the cyber domain, by supporting

[12] See contribution from Blocksome.
[13] See contributions from Blocksome and Sin.
[14] See contributions from Blocksome, Morgus, and Sin.
[15] See contributions from Cheng, Harrell, and Spalding III.
[16] See contributions from Biller, Blocksome, Cheng, Fabey, Fowler, McFate, and Robinson.
[17] See contribution from Blocksome.
[18] See contribution from Blocksome.

"informal groups, operating with loose ties to state organs and with varying levels of complicity, [to] carry out operations fulfilling national strategic goals without legal attribution back to [the] state actor." Biller believes that such activities are likely to continue as "the laws governing when proxy actor operations can be attributed to a state is another area of customary international law that is largely undeveloped in terms of information operations." Michael Fabey of Jane's Fighting Ships highlights China's use of maritime militia and civilian contractors as proxy forces at sea, which, he explains, helps China maintain "escalation dominance" in its surrounding waters. Robinson suggests that non-governmental organizations and civil society groups, such as social clubs, cultural institutes, and religious organizations, may be weaponized over the coming decade through Chinese and Russian "soft power" infiltration. Funding and manipulation of these groups by competing powers, Robinson notes, would create deniable means to accomplish aggressive objectives by using local nationals. Dean Cheng of the Heritage Foundation believes that competing powers may exploit private military companies as a means of pursuing competitive strategic goals while also distancing themselves from direct engagement and association with their adversaries. Finally, Dr. Sean McFate of the National Defense University observes that, over the coming decades, private citizens with extreme wealth could wage "wars without states" by hiring mercenaries to create "military forces and wage wars for any reason they want, no matter how petty."

Cyber Operations

Cyber operations are also frequently highlighted by contributors as a tactic that competing powers will use over the coming decade to challenge the United States and its interests.[19] Cyber operations provide competing powers with a low cost, high value asymmetric approach to challenging the United States below the threshold of conventional armed conflict. Cyber operations, notably, also present an avenue through which competing can support and conduct information operations, political and economic influence operations, and proxy operations. Competing powers, such as China, Russia, North Korea, and Iran, are already using cyber operations to challenge United States interests and increase their leverage against the United States and other international powers.[20] Contributors expect these efforts to only increase and intensify over the coming decade—as Blocksome notes, "we are already in the midst of a cyber arms race." The challenge for the United States, therefore, will be to develop "a better understanding of the norms and rules of engagement in this arena…in order to develop concepts of operations," as "the reluctance of states to establish international legal norms governing cyberspace has created a permissive atmosphere where malicious actors believe they can operate with impunity."[21] Ultimately, as Peter Harrell of the Center for a New American Security concludes, "the low cost of these efforts, comparatively muted United States response to date, and ability to raise a degree of uncertainty over the attribution of attacks makes it virtually certain that America's adversaries will continue these types of [cyber operations] tactics over the coming decades."

Kinetic Tactics: What to Expect from Competing Powers Over the Coming Decade

Contributors highlight fewer kinetic tactics that are likely to be used by competing powers over the coming decade to challenge the United States and its interests. This is likely due to the fact that contributors generally foresee the future of global competition and conflict as being characterized more so by competing powers

[19] See contributions from Biller, Blocksome, Burbach, Cheng, Fowler, Harrell, Morgus, Sin, Spalding III, and Weber.
[20] See contribution from Harrell.
[21] See contributions from Biller and Blocksome.

employing non-kinetic tactics to challenge the United States than conventional kinetic military tactics, with which they would almost certainly be at a significant competitive disadvantage. However, while the United States is likely to maintain its superiority in conventional military realms, its conventional military capabilities and operations will not go unchallenged.

Targeting Vulnerabilities Within Conventional Military Capabilities and Systems

Contributors highlight efforts to target vulnerabilities within the United States' conventional military capabilities and systems as a tactic that competing powers may use over the coming decade to challenge the United States and its interests. The integration of conventional military capabilities with new technologies (e.g., GPS for navigation and targeting, satellite and Internet communications, and the use of software programs to coordinate and communicate between military assets) have, on one hand, been "huge force multipliers" for the United States. On the other hand, however, the integration of these technologies into critical United States military capabilities have made conventional forces dependent on them, to the point where a loss or failure of those technologies could "cripple" those forces.[22] New vulnerabilities emerge, therefore, as "the more networked a system becomes, the more that any attack on that system could lead to catastrophic failures within the system."[23] Blocksome details what she describes as a "key feature" of these new vulnerabilities: "they are highly asymmetric; an adversary need not have anywhere near the same combat capabilities as the forces they are taking on. A few highly trained technical personnel with computer servers and Internet access could take down the GPS system on a billion-dollar aircraft carrier." Ultimately, as Blocksome concludes, while the integration of technological advancements into its conventional military capabilities has helped the United States maintain supremacy in conventional military realms, "the technological reliance of the United States military provides adversaries a massive opportunity to destroy or attrite United States fighting capability."

Advanced Weapon Systems and Unmanned Military Capabilities

The development of advanced weapon systems and unmanned military capabilities is also highlighted by contributors as a tactic that competing powers will use over the coming decade to challenge the United States and its interests.[24] Continued development of these capabilities, contributors suggest, will help competing powers minimize the gap that the United States has maintained over them in terms of conventional military capabilities and superiority over conventional military domains. Dr. Steve Sin of the University of Maryland START considers challenges that the United States is likely to face from continued development of advanced weapon systems by competing powers, arguing that "though strategic competitors may not field as large of a number of units equipped with these advanced weapon systems as the United States, they will certainly aim to field a large enough force equipped with these systems so that they can attain and maintain domain superiority against their regional neighbors and rivals while simultaneously allowing them to attain and maintain limited-duration domain parity against the United States." Blocksome focuses on challenges that the United States is likely to face from continued development of unmanned military capabilities, particularly remotely piloted systems, which she explains are increasingly becoming available to a widening range of competitors, including non-state actors. As the commercial availability of remotely piloted systems increases, more competitors will be able to use such

[22] See contribution from Blocksome.
[23] See contribution from Blocksome.
[24] See contributions from Blocksome, Schneider & Macdonald, and Sin.

systems to operate in the air and on the sea, thus presenting new competitive challenges to the superiority of the United States and other regional powers in the air and sea domains. As Blocksome explains, "for those states possessing conventional forces, the rise of remotely piloted systems for all presents several new threats. For those actors who did not previously possess certain air or sea capabilities, the rise of remotely piloted systems presents a huge leap forward in terms of the capabilities they will be able to command."[25]

Anti-Access/Area Denial (A2/D2) Weapon Systems

Lastly, contributors highlight the continued development and implementation of anti-access/area denial (A2/D2) weapon systems as a tactic that competing powers are likely to use over the coming decade to challenge the United States and its interests.[26] A2/D2 weapon systems provide competing powers an avenue for challenging the United States in the realm of conventional military capability, in which the United States has maintained superiority, by countering the United States' ability to use competitively advantageous long-range precision strike capabilities.[27] Moreover, as A2/D2 weapon systems continue to advance and become increasingly exploitable by competing powers over the coming decade, the United States may also face significant challenges to its "forward presence" and "power projection" from competitors capable of employing these weapon systems.[28]

[25] See also the contribution from Schneider & Macdonald.
[26] See contributions from Fowler and Sankaran.
[27] See contribution from Fowler.
[28] See contribution from Sankaran.

Subject Matter Expert Contributions

Bogdan Belei

Research Associate, Belfer Center for Science and International Affairs (Harvard University)
17 March 2019

The relationship between technological advancement and the tension between liberal and authoritarian governance systems will present a great challenge for the United States in the coming decade. In both kinetic and non-kinetic spaces, Washington will encounter new capabilities and tactics (i.e. autonomous weapons systems, advanced space capabilities) that will lead to new competitive environments. Simultaneously, the United States is likely to experience eroding advantages in existing competitive spaces (i.e. financial markets, conventional weapons systems.) The emerging theme in a competitive, multi-polar world is the convergence of interests among competing political systems, and the political advantages that authoritarian systems currently hold in global, economic competition.

Artificial intelligence is a general purpose technology. In 2017, President Putin said, "Artificial intelligence is the future… Whoever becomes the leader in this sphere will become the ruler of the world."[29] The Chinese government has eagerly pursued a national strategy and allegedly committed tens of billions of dollars toward the development and deployment of AI. Meanwhile, the United States lags behind significantly. According to the National Science Foundation, the United States' federal spending on basic and applied science amounted to approximately 1.7% of all federal spending and 0.3% of U.S. GDP in 2017—figures that greatly pale in comparison to when America's investment in science peaked in 1965 totaling at 3.6% of federal budget spending. As competing powers pursue technological superiority, or at the very least competitive parity, their progress has the potential to erode the United States' current advantages in both military and economic spheres. Washington should heed these timely warnings and reinvest in America's core strength—innovation.

As other countries advance their technological ambitions and pursue new frontiers, the openness of the United States' economy will increasingly become a target for adversaries. Today, the United States is wholly unprepared to monitor and analyze venture investments, controlling interests, and technology transfers involving foreign investors. The U.S. government needs to increase institutional capabilities to properly monitor foreign investors seeking to gain intellectual property and experience with critical technologies.[30] Recent U.S. scrutiny of companies like ZTE or Huawei has shown increasing attention to this important issue.[31] The resulting outcomes will likely force foreign companies to diminish their dependence on foreign technology, while maintaining access to foreign markets.[32]

Even assuming that the United States continues to hold a competitive edge across today's emerging tech, there will be ongoing domestic debates over the role and values of technology in our society. Technological progress in the United States is often reflective of the country's social norms and values. During the Vietnam War, the development of Agent Orange by Dow Chemical contributed to rising dissent within the anti-war movement.[33] Similarly, in recent months, employees at Google protested the company's Project Maven contract with the Department of Defense. While the intentions and merits of these protests can be debated, their presence is

[29] Jill Dougherty and Molly Jay, "Russia Tries to Get Smart About Artificial Intelligence," (Wilson Quarterly, Spring 2018), https://wilsonquarterly.com/quarterly/living-with-artificial-intelligence/russia-tries-to-get-smart-about-artificial-intelligence/.
[30] Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," (Defense Innovation Unit Experimental (DIUx), January 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.
[31] Diane Bartz and Christian Shepherd, "U.S. Legislation Steps Up Pressure on Huawei and ZTE, China Calls It 'Hysteria'," (Reuters, January 16, 2019). https://www.reuters.com/article/us-usa-china-huawei-tech/u-s-legislation-steps-up-pressure-on-huawei-and-zte-china-calls-it-hysteria-idUSKCN1PA2LU.
[32] Gregory Allen, "Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security," (Center for a New American Security, February 2019), p. 3, https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041.
[33] Kevin Roose, "Why Napalm Is a Cautionary Tale for Tech Giants Pursuing Military Contracts," (New York Times, March 4, 2019), https://www.nytimes.com/2019/03/04/technology/technology-military-contracts.html.

evidence of the heightened barriers tech deployment in the United States. As Washington and Silicon Valley compete with adversaries to acquire vast amounts of data or expanding capabilities for analysis (i.e. facial recognition software, predictive analytics, satellite imagery analysis), there will be increasing tension between U.S. domestic values and U.S. global competitive interests. Foreign adversaries are likely to exploit this tension accordingly.

Competition over technological advancement in artificial intelligence, quantum computing, and other emerging technologies will be a leading factor in any shifts in the balance of power among competing powers. History shows that countries first to market, or to the battlefield, with new products can capture the bulk of the benefits, yielding long-term gains for their national interest. Regardless of whether a "whole-of-government" approach to today's technologies is possible, this realm of competition will force the United States to significantly reconsider its social, economic, and military lines policies and practices to the ubiquitous nature of these technologies.

Lieutenant Colonel Jeffrey Biller

Military Professor, Stockton Center for International Law (US Naval War College)
1 March 2019

The next decade is likely to see an increase in information operations by both state and non-state actors. Although this trend will be driven by a number of factors, the reluctance of states to establish international legal norms governing cyberspace has created a permissive atmosphere where malicious actors believe they can operate with impunity. Unless the United States and its allies believe this permissive atmosphere is to their ultimate advantage, it is in the national interest to press hard for the development of international laws related to information operations in general, and cyber-operations in particular.

Although information has always constituted an important instrument of power, there is an ongoing revolution in the way information is gathered, analyzed, and utilized (some would say weaponized). Global information networks enable massive intelligence gathering efforts, aided by increasingly effective analytical algorithms capable of operationalizing that data. However, these very characteristics, interconnectedness and automated analysis, have opened significant attack vectors exploited by state and non-state actors alike. These attack vectors have demonstrated themselves to be lucrative in terms of their intelligence, strategic, and even pecuniary value.

Despite the realization by the United States and its allies that information operations pose a serious threat to national and economic security, the perception by malicious actors is that coordinated response strategies have been slow to develop and unevenly implemented, resulting in the belief that information operations can be conducted with little risk. This combination of a target rich information environment and the ability to conduct operations with little perceived risk promises that information operations against the United States will continue to increase in the foreseeable future.

There are many reasons why countering information operations has proven difficult. Technical reasons include the open, insecure design of the Internet and the ability to mask the origin of cyber operations. Cultural reasons include a hesitancy to permit governmental access to private networks and continued complacency by both the public and private sector in maintaining proper "cyber hygiene." However, there are also significant legal reasons why foreign actors, state and non-state, will continue to challenge the United States and its allies in the information environment.

International relations is undergirded by a rules-based system of conduct generally referred to as public international law. Much of this law is found in the vast array of international agreements. Multilateral treaties, most prominently the United Nations Charter, provide a framework for resolving disputes between states, particularly in peacetime. In armed conflicts, the Geneva Conventions and similar treaties provide the basic rules for the parties to the conflict. Given the increasingly rapid development of information networks, and the decreasing willingness of states to enter into new treaties, it is unsurprising that rules governing information operations in the cyber domain are quite rare. However, a second source of public international law exists that could be utilized to provide a framework governing information operations.

Customary international law includes those legal obligations created by the international community that develop over time and through the practice of states. The manner in which states conduct themselves, combined with statements from official state organs, known as *opinio juris,* create legal obligations states are then bound to follow. The United States recognizes many areas of customary

international law governing both peacetime, such as maritime boundaries, and armed conflicts, such as limitations on targeting. An example in the information operations context can be found in the 2016 speech by then Legal Advisor to the State Department, Brian Egan. In this speech, Egan maintained that interference by cyber means in a state's ability to hold elections would constitute a violation of international law. As such, a violation of this law would potentially allow the United States to take response options, such as countermeasures, against the malicious actor.

Unfortunately, Egan's 2016 speech constitutes a fairly rare example of cyber-related *opinio juris*, resulting a legal landscape for information operations with little in the way of defined international legal obligations. For example, although it is widely accepted that a cyber-operation resulting in damage to objects or injuries to persons would constitute a use of force, prohibited by Article 2(4) of the United Nations Charter, information operations are conducted almost exclusively below the level of a use of force. These below the use of force operations are governed almost exclusively by customary international law. Thus, we end up with the often-referenced "grey-zone," that global competition space below the level of armed conflict, which is largely ungoverned by international law.

Further complicating global information operations is the ability to operate using proxy forces. Global competitors such as Russia and China have effectively utilized proxy actors in a variety of contexts, particularly cyber. Informal groups, operating with loose ties to state organs and with varying levels of complicity, can carry out operations fulfilling national strategic goals without legal attribution back to a state actor. The laws governing when proxy actor operations can be attributed to a state is another area of customary international law that is largely undeveloped in terms of information operations.

States certainly have the ability to move international law in a direction of increased definition. Efforts such as the United Nations Group of Governmental Experts, with the charter to define international law applicability to cyber-operations, have started the process. However, states could be much more proactive in making those statements of *opinio juris* required to advance the existence of more defined legal obligations. Indeed, the existence of defined obligations permit more forceful responses by the United States and its allies to malicious breaches of those obligations, and with greater weight of approval by the international community.

It is fair to ask whether this is a strategically desired outcome. After all, what is required under the law for the goose, is also required for the gander. A more defined legal landscape will necessarily limit operational options by the United States and its allies. The United States may be a very rich target for malicious cyber operators, but it also wields the greatest offensive capability in the domain. As an example of this dilemma, the United Kingdom's Attorney General recently gave a speech outlining the United Kingdom's views on cyber operations under international law. These views constitute a very permissive understanding of the law regarding offensive cyber operations. Thus, a later United Kingdom statement claiming Russia had repeatedly violated international law through cyber operations was viewed with skepticism. Most of the operations listed were of the type their Attorney General has just claimed to be permissible under international law.

Given the increased occurrence of large-scale cyber-operations such as Wanna Cry and NotPetya, the next decade will be pivotal in the emergence, or lack thereof, of customary international law regarding cyber-operations. The United States may choose to move the law in a direction similar to the United Kingdom regarding cyber operations. This will certainly afford greater operational flexibility in conducting offensive cyber operations. However, the long-term consequence of this decision will be to cement the "grey-zone" of cyber operations into the law. Malicious actors will likely increase their operations against the United States, firm in their knowledge that the United States has limited response options under international law.

Dr. Patricia J. Blocksome[34]

Assistant Professor, National Security Affairs (US Naval War College)
12 March 2019

Emerging Trends in Global Competition and Conflict

Three emerging global trends will drive changes in the character of global competition over the next decade: nonconventional warfare, technological permeation, and gender.

I. Trend: Nonconventional Warfare

Nonconventional Warfare will be the key characteristics of global competition and conflict over the next decade. States and non-state actors will continue to compete on the global stage, but due to the conventional warfighting superiority of Western nations, and the US in particular, adversaries have no desire to partake in large-scale conventional warfare against the US. Rather, their strategies will be focused on achieving their aims via methods that are deliberately intended to frustrate the US preference for decisive warfare. While the specific stratagems and tactics chosen by each actor will vary according to their capabilities and preferences, two broad themes have already emerged, and these themes are likely to amplify in the coming decade: proxy warfare and political warfare.

Proxy Warfare

Proxy warfare refers to the use of partners (both state and non-state) to carry out hostilities at the instigation of actors who are not directly involved in the conflict. Proxy warfare has many benefits: deniability, operational reach, and risk limitation. Covertly supplied aid to proxies means that activities can be deniable; truly successful covert support means that your adversary does not know if they are fighting your partner as a solo actor, or if they are actually fighting both you and your partner. Not all proxy warfare is completely deniable; actors usually have some idea of what is going on, but the nature and depth of the involvement are often at least somewhat disguised. In terms of operational reach, the use of proxies can expand conflict or competition to entirely new areas of the globe. An actor in competition or conflict may be strongest in one region of the globe, but if they partner with proxies in other regions, they can dramatically increase their ability to hurt their adversary in unexpected locations. Proxies also offer risk limitation; the desires of the actor's polity will shape that actor's ability to commit that polity to war; if you are sending your youths to conflict, their families are going to care. However, if you are sending resources and advisors to a conflict, but not committing your own forces, the domestic costs of that conflict are likely far less. In addition to the domestic support risk, proxy warfare also offers risk limitation in terms of blowback, especially when proxies are involved on both sides. If your proxies are fighting their proxies and your proxies are losing, that is not the critical or existential threat that would be present if your own forces were losing.

The downside risks to proxy warfare can also be understood in terms of deniability, operational reach, and risk limitation. In terms of deniability, covert support to a proxy can be discovered by the adversary, and if it is, this risks escalation between the supporting actor and the adversary, as it is now clear as to who is actually responsible for the conflict. Second, the extension of operational reach provided by proxies can lead to principle-agent problems; due to the nature of the relationship, proxies will never be as reliable in terms of command or control as forces that you own. This can lead to disconnects between what the supporting actor wants the proxy to do, and what the proxy actually does. Finally, use of proxies may actually increase risks in certain areas. First, support to proxies that are not ideologically aligned with your domestic population may lead to political blowback, in the form of questions about why you are supporting this specific proxy. Second, the creation and training of proxy forces begs the question of what happens with that proxy force when you no longer support it. Will the proxies be left undefended against their adversaries in a conflict you initiated? If this happens, it may be far more difficult to recruit new proxies in the future, given your history of abandonment. Or, will the unsupported proxies find a new sponsor? If so, that new supporter could turn what were formerly your proxies into your adversaries.

[34] The views expressed in this submission are those of Dr. Blocksome and do not reflect the official policy or position of the Department of the Navy, Department of Defense, or the US Government.

Political Warfare

In general terms, political warfare refers to the use of political influence to compel an adversary to take actions they would otherwise not take. Political warfare, while it deemphasizes military action, is not entirely non-military; the threat or intimidation offered by military capabilities is certainly within the realm of political warfare, though the actual employment of those forces in combat is quite limited. Political warfare is a Cold War term; in that historical usage, it referred specifically to the clash of ideologies between communism and capitalism. However, the narratives in contemporary political warfare are not quite so clear-cut. Rather than being understood as an epic ideological struggle between two diametrically opposed ideas on world governance, contemporary political warfare encompasses several narrative clashes, to include nationalism, populism, religious ideologies, and liberal institutionalism.

The current concept of 'great power competition' can be understood as political warfare on the grand scale. Both Russia and China have accepted at least some form of capitalism; however, both are at least somewhat revisionist in terms of their acceptance of the liberal institutional tenants of the current global system. Arguably, Russia seeks to undermine current institutions such as NATO, while China seeks more to gain power and status by either offering challenges within the current institutions, or by creating new institutions that are very similar to current ones, but in which China assumes the leadership role (e.g. Asian Infrastructure Investment Bank vs. World Bank). The rise of nationalism in countries around the globe is a correlate trend; international institutions such as the EU, NATO, the UN, and the World Bank require some acceptance as to the limits of state sovereignty, while narratives of nationalism and some forms of religious ideology focus on the expression of near-absolute state sovereignty.

Political warfare applies not only to the clash between overarching views on the shape of international order, but also to the means by which competition and conflict are carried out in terms of military strategy and operations. At the operational or campaign level, political warfare refers specifically to the ways in which competitions will occur. In this sense, political warfare encompasses whole-of-government and/or whole-of society responses to a competitor. Within the military, this type of operation would encompass mission sets such as civil affairs, psychological and information operations and deception operations, as well as the use of normal military activities (exercises, patrols, etc.) for the specific purpose of sending a message to a competitor. Attributed to Senator Hiram Johnson, the phrase "truth is the first casualty of war" may be particularly applicable to contemporary military conflicts, where the informational aspects of the operation, the narrative battles, are far more important that the actual kinetic activities.

II. Trend: Technological Permeation

The technological permeation of competition and conflict refers to the continually increasing use of technology as an enabler across the spectrum of conflict. The use of technology to carry out warfare is nothing new; what is new are the specific ways in which technology will be adapted in the coming decade, and the vulnerabilities that these adaptations present.

New Abilities, New Vulnerabilities

Conventional militaries have embraced the new capabilities provided by technology, to the point where operating without technology would cripple their forces. Innovations such as GPS for navigation and targeting, satellite and internet communications, and the growing use of software programs to coordinate and communicate between military assets are huge force multipliers—when they work. The more networked a system becomes, the more that any attack on that system could lead to catastrophic failures within the system. All of these technological systems, however, present new vulnerabilities to adversaries. A key feature of these vulnerabilities is that they are highly asymmetric; an adversary need not have anywhere near the same combat capabilities as the forces they are taking on. A few highly trained technical personnel with computer servers and internet access could take down the GPS system on a billion-dollar aircraft carrier.

According to Sun Tzu, the epitome of skill is to subdue one's adversary without fighting. The technological reliance of the US military provides adversaries a massive opportunity to destroy or attrite US fighting capability via cyber or electronic warfare. Only an unintelligent adversary would fight the US in a conventional battle; what is far more likely is that the US's adversaries will non-kinetically attack the systems on which the US relies.

Robots for All

Military technology is no longer a luxury owned only by wealthy states. The rise of commercially available remotely piloted robotic systems means that even non-state actors can acquire and use robotic systems to their advantage. In line with the first theme presented in this paper, nonconventional warfare, weak state and non-state actors will likely not use remotely piloted systems to challenge conventional forces head on. Rather, they will use remotely piloted systems to achieve effects that degrade conventional abilities. Non-state actors will be able to build airpower and seapower through the use of remotely piloted systems. By doing so, they will be able to challenge local air and sea superiority. The US military is used to easily establishing air and sea superiority; these domains will no longer be uncontested.

Robot technology will also enable the development of combined arms operations, with weak actors now bringing in their own close air support, as ISIS did in the second battle of Mosul. In the sea, remotely piloted submarines could provide a cost-effective way to threaten, or even deny area access to, conventional naval forces. For those states possessing conventional forces, the rise of remotely piloted systems for all presents several new threats. For those actors who did not previously possess certain air or sea capabilities, the rise of remotely piloted systems presents a huge leap forward in terms of the capabilities they will be able to command.

Cyber & Space

The development of cyberspace, and the increasing use of space for support to military operations means that these two domains are highly likely to increase in importance in future conflict or competition. We are already in the midst of a cyber arms race, and a space arms race seems plausible, as well. The question is not so much if there will be competition and conflict in these two domains, but rather what shape that engagement will take. The norms for warfare in cyber and space have yet to be developed. We do not yet have a law of armed conflict applicable to cyber, and though discussions on this topic are ongoing, the US needs a better understanding of the norms and rules of engagement in this arena, as well as in the arena of space, in order to develop concepts of operations. In addition to developing a view as to what cyber and space warfare activities are legitimate, the US must also consider what specific skills and training cyber and space forces need, and how personnel trained in these areas will coordinate and liaise with air, sea, and land forces.

III. Trend: Gender

The rise of the #MeToo movement is an example of how gender relations are likely to be a cultural flashpoint. There are two ways in which conflict over the role and treatment of women is likely to affect global competition and conflict: though both in society as a whole, and specifically within military forces.

Gender as a Force of Instability

The primary challenge caused by the trend toward equal treatment of women is in societal disruption, or culture wars, as arguments over the cultural 'place' for women can lead to unrest. The increasing discontent with traditional cultural treatment of women is not only a Western phenomenon; women's rights movements are active around the globe. The protests and accountability associated with this movement can directly affect the ability of a government or military to be effective; the investigation and removal of senior officials for inappropriate behavior can hinder the effectiveness of organizations. Particularly, organizational attempts at cover-ups of inappropriate behavior of senior officials can prove damaging to societal trust in those organizations. Such an event may provide a catalyst for change, and providing a disenfranchised gender with power in a population may offer possibilities for changes in diplomatic ties.

Female Combatants

Interestingly, non-state actors have a long history of using females as combatants, particularly for what might be described as special operations; women are often able to infiltrate into denied areas where men cannot. The internal and external cultural environments in which non-state actor female combatants are used can provide both domestic, "Our females care enough to fight, why don't you?" and external, "You are so evil that even our women are fighting you!" messaging. State actors have a more limited history of females as combatants, though generally women did and do participate, usually in limited quantities. In terms of forces available, the full

integration of women into combat roles offers increased capacity for actors who seek to grow their military forces. Particularly in states with declining populations of those who desire or who are able to serve, the inclusion of women into the military may provide a decisive advantage in terms of total combat power. Integrating women more fully into

The end of gender discrimination in militaries, however, also poses some risks. The first is that military personnel which are unable to adapt to changing gender roles may act out in ways that harm the force. Incidents of sexual assault, sexual harassment, and gender discrimination will occur; as described above, these incidents may provide fodder for adversarial information operations. However, the obverse is also a risk; should an actor which prides itself on its own human rights, and lectures others about them, deny females the right to serve in combat roles, this action could also provide material to an adversary, who would be able to highlight the hypocrisy between words and deeds. Interestingly, one additional advantage of gender-inclusive forces is the increased ability to work with dissimilar societies. This seems counter-intuitive, but the US's experiences in Iraq and Afghanistan, where the pressing need to interact with females in highly gender-segregated societies led to the creation of female engagement teams and combat support teams, demonstrates this advantage.

A final note: while this section has focused on gender, very similar arguments exist in discussions of sexual identity and orientation, however, that trend that will likely take on more importance into the future, while issues related to gender are more contemporaneously important.

Dr. David T. Burbach

Associate Professor, National Security Affairs (US Naval War College)
12 March 2019

Political Influence and Manipulation – Growth Industries for Competitors

Russia and China will pursue non-military influence operations against the U.S. and its allies, seeking to sway foreign policies in their favor, weaken countries by encouraging social tensions, and to reduce the appeal of the democratic model by pointing to hypocrisy and dysfunction.

In some ways the U.S. and important allies are more vulnerable to influence operations now than during the Cold War. To influence mass publics, social networks and online media provide much more direct, targeted vectors for disinformation. Revelations about Russia's 2016 election interference may have given American society somewhat stronger 'antibodies' against foreign influence campaigns, but research by political scientists, psychologists, and mass communication scholars finds that many trends in the information ecosystem are not encouraging. Manipulation through social networks may be even more effective in developing countries where publics have less experience as critical consumers of information and where propensity to believe conspiracy theories is often high.

Manipulation of elites in partner nations and even in the U.S. is also attractive to China and Russia. Unlike Cold War adversaries, Russia and China – as well as other autocratic nations, notably Persian Gulf monarchies -- are major players in global trade and finance and are in a position to dispense large incentives at their targets of influence. Of particular note is that the U.S. political system is more open to foreign penetration than ever given the tremendous expense of modern campaigns and the easing of campaign finance and political corruption rules in the wake of the *Citizens United* and *McDonnell* Supreme Court decisions. Blackmail or public discrediting of Western elites in order to influence foreign policy is also likely to become an even more common tactic, using material stolen online or even high-quality audio-video forgeries as that technology matures.

U.S. planners should also consider the possibility of wartime adversary disruption operations. Talk of 'cyber attacks' during a conflict against a capable adversary often imagines kinetic-like effects: 'hacking' to cause electrical blackouts, disruption of industrial plants and infrastructure, etc. Adversaries will likely make use of information operations too. Online propaganda about the conflict itself will be present, but consider more subtle tactics like spreading rumors that a nuclear or chemical accident has happened on a U.S. military base, that the U.S. government is about to detain ethnic Chinese, or preparing to conduct mass arrests of anti-war protestors. Hacking into civil defense alert systems could pay off handsomely by creating panic (e.g., the Hawaii false missile alert, but during wartime).

These are not purely hypothetical ideas. The DoD's 2015 Jade Helm exercise in the U.S. Southwest had to be curtailed because of public suspicion which we now know was greatly amplified by online Russian provocateurs. The Russians have been even more aggressive with such tactics in their "near abroad." The U.S. government should give more attention to how to "harden" U.S. society against adversary social disinformation and disruption during a conflict without resorting to unacceptable restrictions on online media freedom and civil liberties.

Dean Cheng

Senior Research Fellow, Asian Studies Center, Davis Institute for National Security and Foreign Policy (Heritage Foundation)
13 March 2019

Authoritarian states will try to simultaneously block off foreign access to their own populations (including firewalls and state-run media), while also attacking other states' populations through social media, disinformation campaigns, in-situ elements (foreign student demonstrations, or posting on social media, for example). They will also employ various elements of economic pressure, including sanctions, boycotts, regulatory harassment (e.g., daily health and safety inspections), as well as financial market manipulation (including through cyber).

They may also exploit private military companies (PMCs), in order to distance themselves from direct engagement/association. Similarly, "little green men" and "little green ships" may be supplemented by "little green drones." Other quasi-kinetic options may include cyber attacks on satellite constellations (including their ground terminals and control elements).

Dr. Nicholas J. Cull

Professor, Annenberg School for Communication (University of Southern California)
28 February 2019

My expertise is in the role communication in international relations. I write as a historian of propaganda and a theorist of contemporary soft power and public diplomacy. Looking ahead I see escalating challenges in the field of soft power/media. Both China and Russia have learned from the final decades of the 20th century that media is the great driver of a global presence and the foundation of what Joseph Nye termed Soft Power. They believe – wrongly in my judgement -- that informing a population of a state's virtue and undermining confidence in alternative systems is more important than the state actually being virtuous. Russia's approach tends towards the more nihilistic of the two – encouraging audiences to mistrust any alliance, ideology or source of information. This strategy makes sense because of the perception that Putin represents the strongest person on the stage. The theory is that when nothing else is certain, one gravitates to absolute power. Russia internally has narratives of exceptionalism and messianic destiny as what some call 'the third Rome', but these are seldom shared internationally. China in contrast purports to have a universally applicable system of values, and we know from the internal party journals that they conceptualize some quarters of the world – especially Latin American and Africa -- as culturally empty vessels to be filled from a Chinese reservoir in much the same manner as nineteenth century Europeans saw the same regions. Ironically one of the most subversive responses to Chinese power would be to educate people in the regions of interest to Beijing with the skills to be able to read the Chinese discourse and understand exactly how they are conceptualized.

I see the Russian danger as essentially one of disruption – using media for a divide and conquer game. Russia is not the cause of the divisions, but it is determined to be the beneficiary. The Chinese game is more significant in the longer term as it is creating its own informational infrastructure. While the ratings for Chinese state media are low, their external channels are present in many markets where profit-dependent western broadcasters are now absent or receding. Kenya is an important case in point. More than this, China is developing an important role in global newsgathering. Xinhua has so many bureaus in so many places that the cash-strapped western news system will be obliged to pick up stories from Xinhua sources simply for logistical reasons. In recognition of the power of Xinhua, in late 2018 the Associated Press entered into a partnership with them to gain access to the Chinese market. Congress has

expressed concern that the agreement may provide a further point of access for Chinese state influence.

The biggest danger in the Russian and Chinese challenge is their ability to base what they are doing on genuine grievance and real examples of western hypocrisy. Moscow regularly works with the argument of 'what about-ism' which is to say rebutting allegations by directing attention to an allegedly similar failing on the other side. It is difficult, for example, to lecture Moscow or Beijing on issues of corruption when oligarch money is so obviously welcome in London and New York.

The west needs to work to close-up its most obvious avenues of attack, and to establish what I have termed 'reputational security'. By this I mean that part of a state's ability to survive a challenge in the international system relies on its ability to be known for things that are admired so that a challenge to that state would be seen as an issue of concern by the international community. Ukraine did not have reputational security in 2014. Many smaller or newer countries such as Kosovo and Kazakhstan are now working hard to establish reputational security. Reputational Security has both a cultural and an ethical component. A perception of moral ambiguity – corruption, unilateralism, human rights abuses – undermines reputational security. Historically removing the sources of reputational insecurity has been a foundation for successful public diplomacy. Eisenhower's global communication initiative was severely weakened by the Soviet ability to point to racial inequality in the United States. As Mary Dudziak has documented, the administration saw the danger and came to understand that the issue of Civil Rights was a Cold War priority. My own work has shown how for much of the 1960s the Civil Rights movement could be integrated into US public diplomacy as a real-time Civics lesson – showing how a free country addresses its problems in an open and admirable way, building reputational capital for the future.

For small countries threatened by great power politics I think it is essential that the be encouraged to develop reputational security, most especially those elements which rest on adherence to the norms of Human Rights. The existence of global standards of human rights – codified in a transnational effort in 1948, including input from Chinese and Russian scholars and traditions – is one of the great assets in the coming struggle. It is essential that these standards are not conflated with or allowed to be become geographically specific as 'Euro-Atlantic values' or 'Judeo-Christian' values but are understood and represented as inherent to all and not somehow 'conferred'. Part of this process will involve an exercise in humility and honesty on the part of the United States and its allies – admitting that we too are on a journey and don't have all the answers.

Michael Fabey

Americas Naval Reporter (Jane's Fighting Ships)
US Editor (Jane's Fighting Ships)
6 March 2019

Given the context in which the questions are presented and the phrasing "used by competing powers," it appears that there is no intention to capture any insights on the kind of warfare being waged in Iraq and Afghanistan. I'd also suggest that while North Korean missiles represent a major potential and fleeting threat to US forces, those weapons by themselves do not fit into the category of concern, although they should be considered as part of the overall power-completion calculus I plan to discuss later. In the current context, then, it's probably best to focus the discussion on Russian and Chinese designs against US and its interests.

Of the two, Russia is the more likely to not only incite various actions against the US, but also to escalate them. This is due, in part, to Vladimir Putin's goal to create chaos and disrupt the American-led global order. Indeed, Putin's Russia has done just that, using through direct disinformation campaigns and political tampering within US borders, the success of which has created disunity among traditional political allies on both sides of the Atlantic and disrupted financial markets.

As far as kinetic tactics go, Russian actions in the Baltic, in Syria and Crimea have already created concerns among other nations about American interest or influence in the region. There is great doubt, though, about whether Russian forces would confront those of the US head -on, other than the buzzing of American ships or aircraft by Russian aircraft.

One major exception to this would be in the realm of undersea warfare. US strategists remain wary of Russian submarine forces, and for good reason. The Russian boats have both stealthy in operation and deadly with their weapons loadout. The 2015 Office of Naval Intelligence report underscores the capability of those warships and the US Navy identified concerns about the Russian submarine

force as its main reason for reestablishing the 2nd Fleet in the Atlantic. Antisubmarine systems and forces are priorities for both the US and NATO now.

More likely than a Russian submarine attack on US naval forces or shore facilities would be Russian "auxiliary" and special-purpose submarines, which it can use for kinetic attacks against or non-kinetic exploitation of fiber optic communication cables and other undersea infrastructure.

Of course, the Russian strategic ballistic missile force also represents an enormous threat to the US. While that threat has been dampened through decades through various treaties and an accustomed sense of understanding. The greater concern now, though, are Russian long-range cruise missiles, including hypersonic cruise missiles.

China presents a more complex, strategic and long-term concern for the United States. Unlike Russia, China does possess strong financial foundations for extensive and extended military funding. It maintains many mutually beneficial trade relationships, including its now-contentious one with the United States. But as previous regional and even global conflicts have shown, economic attachments do not preclude military maneuvers.

Having said that, it's unlikely China will take any direct military actions with the US in the immediate and near term. Unlike Russia, China does not seek chaos in the US-run order of things – Beijing simply wishes to replace Washington as the center of the order and return the Middle Kingdom to its rightful ruling spot as the center of the world. Chaos, then, would not suit Chinese ambitions.

However, non-kinetic operations along similar lines Russia has employed will also benefit China. Beijing, for example, used state-controlled media to release operational capabilities milestones for such weapons as the so-called "carrier-killer" DF-21 series ballistic missiles. Reaching initial operational capability does not mean the same thing for Chinese weapons systems or platforms as they do for the Pentagon, but such announcements in the Chinese "press" were given the same kind of recognition even though the DF-21D had not completed any realistic at-sea testing for arguably the hardest surface maritime kill shot ever attempted. In so doing, they created doubt in US lawmakers and military strategists about the vulnerability of US carriers in the Western Pacific, forcing the US Navy to prove the ships were still worth the trouble there. It was a masterful stroke of combining actual weaponry – the DF-21D – with an exaggerated reality afforded by the state-run media to nearly win a major battle: keep US carriers out of the region. Classic Art-of-War thinking.

The Chinese are also masters of so-called "gray-zone" activities," including those maritime militia, civilian contractors, and the coast guard. Those forces are protected by the Chinese sensor and long-range precision weapon complex, which give the Chinese escalation dominance in their-seas territories. The greater problem for US and allies is not their inability to operate in places like the South China Sea, but rather their inability to manage escalation in these oceans against China's gray-zone operations without similar forces of their own.

There is growing evidence China is starting to take deeper dives into the social media platforms for disinformation purposes, although it still would go against the Chinese grain to launch the type of political disruption ops conducted by the Russians. Instead, the Chinese have preferred to infiltrate in a more "benign" way, trying to insert themselves in various levels so they can manipulate and persuade. Unlike Russia, they prefer not to leave any footprints per se. They don't want the target government to even know how pervasive and influential they are. To see how well China can accomplish such a campaign, see Clive Hamilton's recent book "Silent Invasion." Through such means, China can exert a subtle but substantial force than can weaken a country's resolve (to, say, remain committed to the Asia Pacific) or drive a wedge between allies (such as Australia and the US).

And the US is helping the Chinese cause by reducing its own influence and presence in the region. Take, for example, the US decision to cancel sets of exercises on and around the Korean Peninsula to help with American-North Korean negotiations, a move that has. While North Korea benefits from such cancelations, China also does – and doubly so because there's little doubt Beijing helped coach North Korea and getting such a concession. Indeed, China has made it clear it has North Korea's back and interests in the negotiations and Xi Jinping is using North Korean missiles as his own pawns (or Go pieces) in his global game with the US.

Of course, as mentioned earlier, China has its own missile arsenal. But if it can use the weapons – or the threats of those weapons – of another to achieve goals, it will.

The big question in the region is if – and when – China might use true kinetic weapons against the US. The People's Liberation Army Navy has already begun to take more aggressive actions to halt to pause US freedom-of-navigation operations. When might such incidents escalate to something more physically confrontational? China is on course to deploy a handful of carrier strike groups in the region – when might one of those take on US counterpart?

The answer is not right away. The truth is that while Chinese modern forces come close to matching those in the US, there are not there yet. Nor do the Chinese forces possess the savvy to operate on a wartime footing like those of the US. While the US would certainly suffer major losses in the initial volleys of any conflict like that, China would, too – and the proven US ability to reconstitute forces and bounce back would likely be the deciding factor.

Still, there are lot of ifs there. And as China continues to improve its forces, especially its joint-service operations, combining ships, aircraft, space and unmanned systems in a way that would most certainly threaten US Western Pacific forces, the Asian giant becomes a greater threat to America and its allies. At the same time, Chinese "sea-cred" and self-esteem is also growing, nearly reaching the point where it thinks it can succeed in a battle against the US. As the country showed in in the late 1970s by invading Vietnam against the wishes of the Soviet Union, China will take the surprise military initiative against superpower when it suits Beijing to do so.

China's market and financial "manipulation" is being done in plain sight. It is becoming the world's trade monitor in a manner that has come to rival the US, even as China continues to be a partner for America and one of its biggest foreign debtholders. China does not seek geopolitical world domination in a manner like the old Soviet Union, it instead seeks to replace the US as the global financial arbitrator. What keeps China from achieving that goal now is that there is still a lack of convertibility that keeps the Yuan from becoming a reserve currency, as well as concerns about China's lack of transparency regarding government debt.

Dr. Michael W. Fowler

Associate Professor, Department of Military and Strategic Studies (US Air Force Academy)
6 March 2019

The Changing Character of War

The character of war has changed. The tools of compellence have not changed. Yet, countries are changing their tool of preference. Conventionally-focused Western militaries prefer to train for wars of annihilation. These shock and awe operations rely upon an overwhelming advantage in firepower and technology that produce quick, decisive, and efficient results. Instead of countering with traditional conventional force, they will choose methods that are focus on producing psychological effects: a combination of exhaustion, denial, and subversion.[35]

The annihilation method to warfare can be effective in a conventional conflict, particularly when one side has far superior fire power or expertise. Lop-sided engagements include U.S. operations in Grenada and Panama and Israel's victory in the Six-Day War. When the adversary is less cooperative or the advantages less one-sided, attempts at annihilation can be mitigated by using methods of exhaustion. It is not unusual for annihilation approaches to have initial battlefield successes that fail to win the war. Examples include Germany's early successes in World War II against France and most of Europe, Soviet operations in Afghanistan, Iraq's early successes in the Iran-Iraq War and its later invasion of Kuwait, and U.S. operations in Iraq and Afghanistan. After success in the initial phase of the operation, each case eventually devolved into a war of exhaustion, a slog-fest that ate up material and manpower.

In the near future, it is highly likely that the use of annihilation methods will be limited to those cases in which the aggressor has an extremely significant combat advantage and it is highly unlikely that a third party will intervene to change that relative advantage. As long as the United States maintains superior military capabilities, adversaries are likely to avoid a traditional conventional conflict. Conventional U.S. operations in Iraq (both Desert Storm and Iraqi Freedom) demonstrated the risk of relying upon massive but

[35] Michael Fowler, "Ways of War: Constructing a Compellence Strategy," Burke, Fowler, and McCaskey, Military Strategy, Joint Operations, and Airpower (DC: Georgetown University Press, 2018).

minimally trained armies to face lower numbers of highly-trained forces with advanced weapons.

To mitigate U.S. military advantages, adversaries will gravitate towards methods that are less reliant on physical destruction and place more emphasis on creating psychological effects. These methods of exhaustion, denial, and subversion have long been the tool of choice for non-state actors (i.e., terrorists, insurgents, illicit traffickers and transnational criminal organizations). Now, several states (e.g., Russia and China) publicly advocate for and are employing these unconventional warfare methods as a way to achieve national security goals while circumventing international conventions designed to prevent conflict.

Exhaustion. Exhaustion targets morale through a combination of kinetic attacks and information operations. Exhaustion seeks to create the perception of "the improbability of victory or the unacceptable cost" of continuing operations.[36] Exhaustion exploits the inefficiency of maintaining large or multiple fronts. At the operational level, wide area security and deterrence operations require forces to be prepared at all times for multiple means of attack from a variety of directions and methods. Defending everywhere at once is expensive. Tactics such as hit and run guerrilla warfare drain the opponent's time, treasure, and talent to cause a "death by a thousand cuts." Whether it is for counterinsurgency, counterterrorism, or deterrence, deployed operations require a substantial amount of time and treasure. Arguably, this makes military forces less ready for conventional warfare as their resources, training, and employment are diverted to other tasks.

Exhaustion requires operations to be designed to make the opponent use a disproportionate amount to resources. Russian actions in the Crimea and Chinese actions in the South China Sea are relatively inexpensive. On the other hand, the United States maintains a long logistical tail to deploy and sustain forces abroad. Meanwhile, using shows of force and large military exercises are unlikely to intimidate the United States. However, they can be far more effective against smaller powers who then goad the United States into over-reactions and costly deployments. U.S. and allied freedom of navigation operations in the South China Sea as well as aircraft and armor deployments in Eastern Europe provide a tripwire for escalation but are in such small numbers that the force itself is unlikely to have a deterrent effect. Certainly, presence has its own effect as Russia and China are unlikely to directly attack U.S. forces and risk escalation. It is less clear if the deployments have any impact on Russian and Chinese ongoing unconventional warfare activities.

Denial. Anti-Access, Area Denial is designed to prevent the U.S. military from using its tremendous advantage in long-range precision strike capabilities. Denial focuses on creating large buffer zones while exploiting U.S. dependence upon and vulnerabilities in space and cyber. Advanced cruise missiles and anti-ship missiles create space as it forces extended operations from remote bases or ships.

Despite demonstrated kinetic anti-satellite capabilities, China's rapid expansion of its space program decreases the probability of employing weapons that result in massive space debris and potential degradation of their own satellite networks. Instead, they are more likely to focus on less kinetic, but equally disruptive tactics such as lasers, electronic warfare and, computer network attacks on satellite ground stations.

Chinese and Russian efforts at denial use military capabilities but add a healthy supplement of diplomatic and economic power. For example, Chinese diplomatic and economic efforts in the South China Sea have softened efforts to enforce the United Nations Convention on the Law of the Sea. While not the only factors, Chinese efforts helped facilitate a cooling of United States-Philippines relations. Meanwhile, China's Belt and Road Initiative to build airports and ports across South Asia provides China additional basing and resupply options while simultaneously limiting U.S. options in the area.

Subversion. Typically done using non-kinetic information operations, subversion intends to get the enemy to turn upon itself. Technology has and will continue to dramatically improve the effectiveness and efficiency of subversion. Russian meddling in U.S. (and other) elections is intended to undermine people's belief in the democratic process. Russia's fomenting of rebellion in east Ukraine gave Russia both the opportunity to seize Crimea while derailing Ukraine's inclusion into the European Union and NATO. Propaganda is not new. But, old school radio, television, and print propaganda could be dismissed by adversaries when the state source was obvious. However, the opaque attribution of computer network attacks gives Russia some claim of deniability while sowing confusion among its targets.

Dedicated cyber teams at both the state and non-state levels leverage the continuing spread of social media to cause subversion.

[36] J. Boone Bartholomees, "The Issue of Attrition," Parameters (Spring 2010), 9.

Evolving automated intelligence (AI) capabilities will improve their ability to target susceptible individuals based upon complementary ideologies, money challenges, ego, search for adventure, and people disgruntled with the current political and/or economic system.[37] This will improve multiple capabilities including their efficacy to catfish for identity theft, recruit spies, and motivate "lone wolf" operations. With today's technology, training spies and operatives can be done remotely.

Security Cooperation. Some argue that Western militaries should withdraw from peripheral security challenges and focus resources on defending against existential threats. While ensuring national sovereignty should be a top priority for any military, such an isolationist approach would leave many national security objectives at risk. One economic alternative to counter unconventional warfare is through security cooperation.

Security cooperation includes an array of activities including arms sales, weapons transfers, military and/or police training, advising, personnel exchanges, and infrastructure development. Since the turn of the millennium, global arms transfers increased 50%.[38] Critics argue that this trend represents a militarization of foreign policy and a waste of resources that would be better suited to improving combat capabilities.[39] Yet, cooperation via security assistance is now a common element in the strategist's toolbox across a multitude of countries.[40] Security cooperation is increasing as potential partners can be taken by a competitor that is less selective about good governance issues such as corruption and human rights.

Security cooperation with non-state actors enables states to intervene while circumventing the traditional thresholds of sovereignty. For example, Russia's supplying of trainers and advanced air defense systems to the rebels in Eastern Ukraine created much consternation in Europe. However, Russia's denials of involvement and their claims of self-determination of ethnic Russians being discriminated in Ukraine short-circuited the international conflict response process. Plus, security cooperation obfuscates the traditional notion of formal alliances. Security cooperation is an investment in another country's future. Even without a formal defense agreement, this economic investment represents a national security interest. In many cases, arms transfers come with their own financing. A change in regime could threaten the repayment of that loan.

Conclusion. In a way, the approaches and methods of warfare have regressed to the days of the Cold War with emphasis on indirect warfare through proxies and the geo-political scramble for client states and overseas bases. At the same time, technological developments have re-invented this type of warfare and improved its reach and potential effectiveness. Russia and China have proven adept at employing unconventional warfare, setting a standard that other U.S. adversaries are sure to follow. The combination of exhaustion, denial, and subversion can be an effective combination to mitigate annihilation strategies. One method to counter this approach is through effective security cooperation operations. Of course, security cooperation is not a panacea but is replete with its own set of operational challenges.[41]

Peter E. Harrell

Adjunct Senior Fellow (Center for a New American Security)
8 March 2019

We have already seen two major powers—Russia and China—and a number of middle powers, including Iran and North Korea—engage in a range of cyber attacks and online cyber influence operations in order to increase their leverage and inflict harm on U.S. and allied interests and to sow divisions within the U.S. The low cost of these efforts, comparatively muted U.S. response to date, and

[37] Taylor Stan and Daniel Snow, Cold War Spies: Why They Spied and How They got Caught (New York: Oxford University Press, 2015); Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCLS," Studies in Intelligence Vol. 57, No. 1 (March 2013), 7-17.
[38] Dyfed Loesche, "The World's Arms Exports," Statista (Feb 20, 2017), at: https://www.statista.com/chart/8163/the-worlds-arms-exports/.
[39] Gordon Adams and Shoon Murray, eds., Mission Creep: The Militarization of US Foreign Policy? (Washington, DC: Georgetown University Press, 2014).
[40] Fowler, "Constructing Effects: a Strategic Theory of Security Cooperation," in Burke, Fowler, and McCaskey, eds., Military Strategy, Joint Operations, and Airpower (DC: Georgetown University Press, 2018).
[41] Jahara Matisek, "The crisis of American military assistance: strategic dithering and Fabergé Egg armies," Defense & Security Analysis 34, no. 3 (2018): 267-290.

ability to raise a degree of uncertainty over the attribution of attacks makes it virtually certain that America's adversaries will continue these types of tactics over the coming decade. U.S. and allied networks, especially corporate networks, remain shockingly vulnerable to these types of attacks despite the volume of the attacks and the severity of the consequences in numerous high-profile cases. While hardening U.S. defenses and increasing deterrence may help mitigate some of the worst of these attacks, the reality is that both cyber attacks and online cyber disinformation and influence campaigns will remain a popular tactic over the next decade.

China is likely to continue expanding its use of coercive economic measures, such as trade restrictions, tourism and travel restrictions, informal boycotts, and similar measures, over the coming decade. As my CNAS colleagues and I wrote in a 2018 report on *China's Use of Coercive Economic Measures*, China has significantly expanded its use of coercive economic measures over the last decade and is showing clear evidence of learning across cases. As China's relative economic power increases and as China maintains the assertive posture that has defined Chinese foreign policy for the past several years, Chinese coercive economic measures will play an increasingly prominent role. This is likely to constrain both the choices of U.S. allies in Asia, such as South Korea and Japan, and of major multinational corporations concerned about incurring Beijing's ire.

To date, China has generally refrained from deploying coercive economic measures against the U.S. in the context of foreign policy and geopolitical disputes. For example, while China has repeatedly threatened to impose retaliatory sanctions against U.S. companies involved in the sale of weapons to Taiwan, China does not appear to have followed through on these threats. (China has, however, imposed retaliatory tariffs on the U.S. and taken action against U.S. companies in the context of trade disputes).

Over the next decade, however, China is likely to be more willing to directly impose coercive economic measures against the U.S. and U.S. companies in the context of foreign policy and geopolitical disputes. This is due to a combination of China's increasing foreign policy assertiveness and the likely continued growth of China's economy, which will give China a greater degree of comfort in its capacity and ability to deploy such measures.

In general, I expect that China will continue to use the types of measures it has been using—import/trade restrictions, restrictions on Chinese tourism, direction to Chinese SOEs to disfavor certain countries and companies, rather than expanding into new areas, such as widespread financial market manipulation. China appears to assess its current toolkit as reasonably effective and as involving few unexpected or collateral costs, encouraging continued use, rather than experimentation with other tools that may have unexpected and/or larger collateral costs.

Dr. Peter Layton

Visiting Fellow, Griffith Asia Institute (Griffith University)

22 February 2019

The operating environment across the next ten years will continue to be shaped by the ongoing information technology revolution. This revolution influences what kinetic and non-kinetic weapon systems and tactics are available to be used in the near-medium future. While there are many possibilities, two issues are of interest.

Firstly, the type of kinetic and non-kinetic weapon systems encountered may be less predictable as the emerging fourth industrial revolution (4IR) may mean new or evolved weapon systems emerge rather unexpectedly. With advanced manufacturing and information technology connectivity, prototype warfare is moving from idea to practicality. Focusing on specific possible future weapon systems may be less useful then being able to respond faster to the unexpected. Secondly, the use of non-kinetic weapon systems in terms of societal disruption and influence operations appears set to become more common, sophisticated and ambitious. They may prove attractive to many, particularly authoritarian states.

Prototype Warfare in the Fourth Industrial Revolution

The emerging 4IR now allows the large-scale adoption of the prototype warfare concept. The idea is to rapidly field a variety of low-cost, less complex systems and then replace these with improved variants or something totally new on a regular basis. In that, 'short-life cycle capabilities' might be a more accurate term. SOF already use prototype warfare type concepts but generally only on a

diminutive scale and for restricted purposes. Scaling up the idea would see short-life items produced under 4IR being a small part (10%?) of the overall national military force structure, augmenting the long-life, complicated platforms.

In prototype warfare the designs are selected for production based on meeting short-medium term needs; this implies some generic capability shortcomings. To ensure rapid time-to-service, new capabilities will generally be of limited complexity and therefore probably single role not multi-purpose. Aspects of the 4IR innovation process further reinforce the push towards simplicity. Given this, prototype warfare concepts might produce tailored capabilities suitable mainly for particular roles or missions in specific geographic areas. This raises the possibility of optimising a force deployed in the field on an almost daily basis: "consider the implications if a commander had the ability to select from a catalogue of weapon systems while planning for a mission and they were manufactured based on her specifications."[42]

This introduces several problems for defending forces. Firstly, the systems being defended against are designed and optimised for the specific situation not to be a one-size-fits-all multi-role platform. In general, an optimised system will perform better in the given situation for which it is designed. If the defenders use multi-role systems they may be at a disadvantage from the start. Secondly, the systems being faced – being situational dependent - may not have been encountered before. Little may be known of them. Indeed with the 4IR process, even if they have been faced earlier they could have been further customised and had technical deficiencies or operational weakness removed. Thirdly, innovative systems may use novel tactics. With limited time to respond, the defenders may be out-thought and have no readily at hand satisfactory tactical response. Tactical defence responses then would have to be broad in nature, which is inherently difficult to do. Lastly, the force being defended against will be heterogeneous. A countermeasure against one system will most likely not work against another. Prototype warfare is inherently hard to counter.

For the commander of the attacking force, there is a further advantage in that the prototype warfare capabilities in being inexpensively produced will be semi-expendable, maybe even disposable. They may not need to be carefully husbanded for the next fight and instead can be used in riskier situations than a large expensive platform can be. Moreover losses of prototype warfare equipment may be able to be readily made good if developed under the 4IR process.

Prototype warfare is not restricted to national military forces. In the 4IR there is an accelerated diffusion of ideas and technology globally. Islamic State has already demonstrated a form of prototype warfare in Iraq. Islamic State:

"did something that no terrorist group has ever done before… design their own munitions and mass-produce them using advanced manufacturing techniques. Iraq's oil fields provided the industrial base - tool-and-die sets, high-end saws, injection-molding machines - and skilled workers who knew how to quickly fashion intricate parts to spec. Raw materials came from cannibalizing steel pipe and melting down scrap. ISIS engineers forged new fuzes, new rockets and launchers, and new bomblets to be dropped by drones, all assembled using instruction plans drawn up by ISIS officials. …[This] provides a disturbing glimpse of the future of warfare, where dark-web file sharing and 3-D printing mean that any group, anywhere, could start a homegrown arms industry of its own."[43]

Thought needs to be given to how to combat adversaries using prototype warfare processes, techniques and tactics. Today, countermeasures to individual weapon systems can take years to devise, trial and bring into service. The emerging 4IR now means that attention also needs to be given to countering short-life cycle capabilities. The next ten years may see a veritable deluge of them.

Societal Disruption and Colour Revolutions

Societal disruption operations using information technologies may become more common, sophisticated and ambitious. There seem three broad types of strategy that might be used and for which counters may need consideration.

The simplest way is to induce chaos in a society. There seem two broad approaches. The Russian approach has been to amplify divisive social issues by employing wide-ranging disinformation attacks across a nation's political spectrum. Whether certain groups are supportive of Russian policies is immaterial, the key issue is to drive them to being more confrontational towards other groups.

[42] Robert Kozloski, 2017, 'The Path to Prototype Warfare", War On The Rocks, 17 July, https://warontherocks.com/2017/07/the-path-to-prototype-warfare/ [Accessed 21 February 2019]

[43] Brian Castner, 2017, 'Exclusive: Tracing ISIS' Weapons Supply Chain—Back To The US', Wired, 12 December, https://www.wired.com/story/terror-industrial-complex-isis-munitions-supply-chain/ [Accessed 21 February 2019]

Wikileaks's Julian Assange advocates a different approach. Societal disruption is achieved not by attacking society but by weakening the government, making it less able to govern and thereby unleashing currently repressed forces.[44]

The second strategy is to support some useful interest group but this is technically more difficult to do remotely than sow chaos. The particular individuals who compose the useful interest groups need to be both located and engaged, now mainly in cyber space. Certainly, terrorist groups like ISIS have been able to discern and target useful individuals but this has been on a small scale and using human-intensive techniques. Now though the emerging era of big data and artificial intelligence is making the large-scale manipulation of sizeable interest groups feasible and normal.

The third strategy is to change people's minds; this is not easy technically although recent technology developments may revise this assessment. There are two general approaches. The easiest is an indirect one: creating a false reality. Given this seeming new circumstance, people will themselves mentally adjust to meet it. Creating new realities though is resource intensive. Russia is active and successful in this field exploiting political parties, ethnic minorities, NGOs, public broadcasting, social media and religious groups. It would be difficult to achieve beyond border countries.

A more complex approach is using a modified form of agentic constructivism encompassing ideational collapse and replacement. This strategy includes acting top-down through ideational elites but determining who these individuals are is problematic. Partly offsetting this is that this target audience may not be large. Moreover, the new approaches of big data, data mining and micro-targeting potentially offer technological solutions to finding and influencing chosen individuals. Recent developments in so-called deep fakes may further support such a strategy. Deep fakes use artificial intelligence to produce highly realistic videos that seemingly can show anyone making any statement desired – or indeed acting in particular ways: "political leaders can be made to appear to say anything at all, and they will sound and look exactly as they do in real life."[45]

The three strategies suggest what is possible across the next ten years. Countering these will require some intellectual effort and resourcing.

Dr. Martin Libicki

Keyser Chair of Cybersecurity Studies (US Naval Academy)
19 February 2019

The Rise of Chinese Surveillance?

Among the many consequences of the ongoing information technology (IT) revolution, the growth of surveillance capabilities may be particularly signal. IT advances enhance surveillance in several ways: it facilitates the production of improved sensors, it enables high rates of communications among them, it provides a platform (the Web) for collecting data, and, via artificial intelligence (AI), it permits the operators of surveillance systems to draw subtle and meaningful conclusions about who they surveil.

Surveillance can be good or bad. In the hands of Western forces, it has improved the efficiency, for instance, of counter-terrorism operations by allowing high-value targets to be differentiated from the populations they hide in. Surveillance may also have contributed to declining crime rates in the United States. But in other hands, surveillance is a tool of state repression. Chinese practice in recent years has illustrated as much: developments include the suppression of Uighurs in Xinjiang and social credit scores (like U.S. credit ratings but with political factors).

Surveillance systems have long ceased being do-it-yourself affairs, especially if implemented at nation-scale (or world-scale). Large companies are involved, both in the United States and abroad. In the United States, social media companies (e.g., Facebook) carry out

[44] Julian Assange, State and Terrorist Conspiracies, 10 November 2006, p.3, https://cryptome.org/0002/ja-conspiracies.pdf, [Accessed 21 February 2019].
[45] Alina Polyakova and Spencer P. Boyer, The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition, Washington: The Brookings Institution, pp. 12-13

Web-based (*vice* sensor-based) surveillance in order to characterize customers to better target adds to them (but as the Cambridge Analytica affair indicates, also for resale). As more household items become networked, the opportunity for global controllers attract the likes of Amazon, Google, and Apple; their products may provide a foundation for private residence surveillance. But many other sectors are also involved. They include cybersecurity companies whose talents at finding malware can be re-purposed to finding politically sensitive material. They also include router companies that make the boxes that networks are built atop.

One such company is Huawei, a $100b (annual sales) company which is accelerating its drive to dominate the market for fifth generation (5G) mobile telecommunications. Huawei, of late, has faced strong government-induced headwinds in Western markets. Ostensibly, cybersecurity is the reason given for the U.S. asking its allies to avoid Huawei in their infrastructure: either because of undocumented eavesdropping circuits (and/or code) in their product (of which no evidence has been presented to the public) or because, as a Chinese company, Huawei would be unable to resist a PRC request to install them. But there are also concerns that if a Chinese company were to control the key technologies associated with 5G, they would also be able to influence or dominate a range of technologies associated with advanced networks – not least being those associated with advanced control systems, to include advanced surveillance systems. Arguably 5G technologies may be overkill for cell phones themselves (Japan's NT&T currently has no plans to use it other than in dense areas such as train stations). But 5G is being touted as a platform to integrate RF-emitting devices that collectively constitute the Internet of Things. Integration would allow AI to optimize the interactions among these devices (think, for instance, the interaction between cars and highways) and foster collective machine learning to that end.

It is not easy to predict whether 5G market control would lead to a wider and more strategic market control of related products and services. Microsoft, for instance, leveraged its control over PC operating systems (Windows) into control over office applications (Microsoft Office), and, to a lesser extent, browsers (Microsoft Explorer). One reason that Windows allowed Microsoft to dominate computer applications while DOS did not is that Windows had many function whose adroit use benefited its applications; DOS had far fewer. Supposedly, Microsoft made its function calls available to all application developers, but it is plausible that Microsoft Office bet their development dollars on the success of Windows while its competitors did not – and possible that Microsoft Windows had capabilities not revealed to competitors of Microsoft Office. From a standards perspective, the question therefore would be whether Huawei would build to standards that do not give its other subsidiaries or partners a decided advantage over unaffiliated competitors in related spaces. Without further research (and imagination – since many relevant applications are undreamt of), this is a difficult question.

The other key question is whether Huawei's 5G networks contain the DNA to shape surveillance systems in ways favorable to the values of the Chinese Communist Party. This question also has no easy answer. In theory, a government can shape whatever surveillance systems it buys to its needs and values. In practice, unless it is sophisticated, it chooses from a limited array of options provided by the vendor. Would a Huawei-centered state surveillance system be sensitive to PRC values in ways that a Western firm would not? If so, what kind of instructions-set code would reify such values – or would the Chinese be the recipient of such surveillance in ways that would allow them to suppress the expression of anti-China sentiment even when the national government purchasers of such equipment had no such intention?

Dr. Jahara Matisek

Major (US Air Force)
Assistant Professor, Military and Strategic Studies Department (US Air Force Academy)
Non-Resident Fellow, Modern War Institute (US Military Academy)
8 March 2019

Adversarial Information Warfare Undercutting America[46]

One of the biggest threats to the United States (U.S.) is information warfare (IW). IW is the tactical and strategic use of information and

[46] This article was made possible by contributions from Cadet Connor G. Grant, my Research Assistant in the Department of Military and Strategic Studies, U.S. Air Force Academy, Colorado.

data to gain an advantage in various domains, and to achieve an objective – all without having to fire a shot.[47] Near-peer adversaries such as Russia and China, and violent non-state actors (VNSAs) like the Islamic State (ISIS), all employ variants of IW to further their own causes and to weaken the 'soft' power of the U.S. Such IW is a difficult threat for the U.S. military to adapt to, as it requires American civil society to be resilient against misinformation, disinformation, and *schismogenesis* (true but divisive information that polarizes opinions on both political extremes) campaigns by anti-American adversaries.[48] Moreover, antiquated laws, such as the Posse Comitatus Act of 1878, make it difficult for the U.S. Armed Forces to deploy resources in defense of the American homeland. The greatest danger with IW, however, is that information age era and commensurate technology enables every aspect of the human condition to be weaponized, making everything and everywhere a battlespace: War is everywhere but nowhere all at once.

As it currently stands, 8 of the 17 U.S. intelligence agencies have detailed how the 2016 American election was meddled and tampered with through a concerted IW effort by the Russian government.[49] Defeating and deterring Russian IW in future elections appears to have worked in the 2018 elections, but it is also just as likely that Russia is saving new tactics and techniques to undermine confidence in the 2020 presidential elections. In Eastern Europe, Russia has been waging a disinformation campaign in order to influence the hearts and minds of the Ukrainian public (and neighboring states) in an effort to prevent NATO expansion into its traditional sphere of influence. Russian IW success in Ukraine also built on lessons learned with how IW was employed in the 2008 Russo-Georgian War.[50] Similar IW efforts are being employed by the Chinese government to undercut U.S. allies in the Pacific, such as Australia and New Zealand. China has been covertly funding and grooming scholars, politicians, and public intellectuals, to be pro-Chinese in hopes that this will translate into policies that might weaken U.S. ties in the region, such as trying to disrupt the 'Five Eyes' intelligence sharing program.[51]

On the other spectrum of IW, VNSAs such as ISIS and Boko Haram upload videos on the internet (and social media) that show torture, beheadings, burning people alive, and other atrocious murders, to aid in the spread of terror while trying to recruit new members.[52] While ISIS, and other VNSAs like the Taliban and Al-Qaeda, do not pose an existential threat to the U.S., their activities are widely broadcasted to domestic audiences in America (and her allies). This results in an over-reaction by publics throughout the West, compelling political and military leadership to spend more time and resources on a problem that is not commensurate with the *actual threat* posed. More troubling, VNSAs inspire 'lone-wolf' terrorist attacks, as has been seen in the U.S., Britain, France, Germany, and elsewhere. In many of these cases, it has led to exaggerated public fear and a media frenzy, resulting in policies that undermine democratic freedoms and institutions.[53]

While IW is as old as the Peloponnesian War, its effectiveness has substantially improved in the Internet-of-Things era, as many societies and economies are dependent on the cyber domain to operate and function, with most infrastructure highly dependent on connectivity. The critical factor now, is the low barrier to entry, as even low income countries are seeing their citizens get on-line. Indeed, as of 2019, approximately 54.8% of residences in the world had access to the internet, which means the ability of adversarial IW to infiltrate the U.S. and many allied countries will increase, as will its effectiveness to cause societal problems in target states.[54] This is because potential adversaries need only a social media account, and possibly a bank of computers and 'bots', to successfully (and cheaply) wage IW that shapes new narratives in a target society, in hopes of undermining societal unity and good policy debate – and possibly even public resolve to fight a war.

While the bulk of IW in the future will be carried out on-line, other examples include falsified documents, fabricated newspaper

---

[47] Roger C. Molander, Andrew Riddile, Peter A. Wilson, and Stephanie Williamson, Strategic information warfare: A new face of war (Santa Monica, CA: RAND, 1996).
[48] Jayamaha, Buddhika B., and Jahara Matisek. "Social Media Warriors: Leveraging a New Battlespace." Parameters 48, no. 4 (2018): 11-23.
[49] Karen Yourish and Troy Griggs, "8 U.S. Intelligence Groups Blame Russia for Meddling, but Trump Keeps Clouding the Picture," The New York Times, August 2, 2018, https://www.nytimes.com/interactive/2018/07/16/us/elections/russian-interference-statements-comments.html
[50] Emilio J. Iasiello, "Russia's Improved Information Operations: From Georgia to Crimea," Parameters 47, no. 2 (2017): 51-64.
[51] Jahara Matisek, "Is China Weaponizing Blockchain Technology for Gray Zone Warfare?" Global Security Review, September 28, 2018, https://globalsecurityreview.com/china-weaponizing-blockchain-technology-gray-zone-warfare/
[52] William Reno and Jahara Matisek, "A New Era of Insurgent Recruitment: Have 'New' Civil Wars changed the Dynamic?" Civil Wars 20, no. 3 (2018): 358-378.
[53] Mark S. Hamm and Ramón Spaaij, The age of lone wolf terrorism (New York: Columbia University Press, 2017).
[54] "The Inclusive Internet Index 2019: Executive summary," The Economist: Intelligence Unit, 2019, https://theinclusiveinternet.eiu.com/assets/external/downloads/3i-executive-summary.pdf

articles, propaganda, and deep fakes (creating false audio and video of an important figure saying or doing something). The information domain is an arena that is very difficult to maintain control of, especially in Western democracies, and this IW will sow disinformation and division.[55] While China appears to have asserted itself in the information domain through its 'social credit rating system', keeping citizens in-line with Communist party views, such authoritarianism will not bode well for the future of China.[56] The most talented and educated Chinese citizens will likely immigrate to liberal democracies, such as the U.S., in hopes of escaping such tight societal control. While Chinese policies will allow the state to be safely in control of the Communist party, this will result in 'brain drain', as Chinese citizens will immigrate to the U.S. (and other Western states), contributing to the economic and technological success of these welcoming countries.

While IW rarely generates conversation about the future of warfare, this is merely a product of threat-under-inflation, whereby the military-industrial complex views IW as generating little profit to be made, and the U.S. military views its primary mission as training and equipping for a conventional war against a near-peer adversary. With IW being relegated as a backwater for military operations, there will be a need to focus on furthering developing American capabilities to defend against such IW operations in a way that does not hurt traditional values of freedom and privacy. Similarly, countering IW will be important as mobilizing the American public to support U.S. military operations – kinetic and non-kinetic – against adversaries will be dependent upon creating public narratives and policy debates that are devoid of foreign influence.

Dr. Sean McFate[57]

Professor (National Defense University)
7 March 2019

You mentioned that a constant state of low-level conflict is a key characteristic of this age of durable disorder. Are there other emerging global trends that coincide with this age of durable disorder?

Dr. McFate: Yes, there are quite a few. Durable disorder is the overall systemic threat that is giving rise to what we are seeing around the world. We can spend all day on who/what is the biggest threat (i.e., China, Russia, genocide, global warming, etc.), but if you look at global actors, they are all grasping durable disorder, and are learning how to fight in it. We could talk about what that fight looks like and what victory looks like in that fight, but there are many features of durable disorder. One of the emblematic features of durable disorder is the return of mercenaries and private warfare. Mercenaries are returning, and when you privatize war, it changes warfare. Our national security establishment is deeply unready for that. When you privatize warfare, it is sort of like Clausewitz meets Adam Smith. And this is, again, the warfare of Machiavelli. There are strategies to deal with mercenaries that are unknown to most of us in DC, and we need to develop our understanding of them.

Additionally, once you have a persistence of mercenaries, the super-rich can become superpowers. Random billionaires, Fortune 500s, megachurches, etc., which are already more powerful than most states in the world, can hire military forces and wage wars for any reason they want, no matter how petty. This introduces the concept of private wars. In the future, there will be private wars. And our paradigm of warfare, whether it is Clausewitz or international humanitarian law, does not even recognize this type of warfare. If you look at the Rwanda genocide or the drug cartel wars, those are wars without states. But to a traditionalist, they cause cognitive dissonance—Rwanda is basically an 800,000-person homicide. Ultimately, our strategic way of thinking needs to be updated for this new threat environment and the actors that will fight in it.

You mentioned mercenaries and privately funded warfare, but what other kinetic and non-kinetic tactics are and will be used by competing powers domestically and abroad to undercut US interests over the coming decade?

---

[55] Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War," Foreign Affairs, December 11, 2018, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

[56] Charlie Campbell, "How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens," TIME, 2019, http://time.com/collection/davos-2019/5502592/china-social-credit-score/

[57] Dr. McFate's contribution consists of excerpts from a longer interview session. For access to the full interview session, please contact George Popp (gpopp@nsiteam.com).

Dr. McFate: It is important to think about old rules of war versus new rules of war. For example, Russia has always sought to disunite Europe and NATO and the EU. In the old rules of war, utility of force was supreme, so what Russia would do is have huge military exercises at the East-West border of Germany, (150,000 troops with aircraft—an invasion force) and they would tell NATO, "Don't worry. It is just a military exercise." And, of course, that would threaten NATO and would have ripple effects, which would please Moscow. Today, war is moving from Clausewitz to Sun Tzu. An example of a present-day scenario for how Russia acts to disunite Europe may start with it deliberately bombing civilian centers in Syria. This creates a tidal wave of refugees that hits the EU and causes Brexit and a rise of right-wing national politics. This, combined with information warfare, is disuniting Europe. Russia has weaponized refugees. That is one example. Another example is that, under the old rules of warfare, if Russia wanted to conquer something, it would use tanks or troops or other conventional means to take over territory in Hungary or Czechoslovakia. Today, what Russia does, in Ukraine or Crimea for example, is it uses weapons that give Russia maximum plausible deniability.

Warfare in the future is going underground. It is becoming epistemological, telling truths from lies determines winners and losers. In the global information age, plausible deniability is more powerful than firepower. Russia today uses means like Spetsnaz, mercenaries and proxy militia (e.g., the Wagner Group or the Donbas Battalion), and a lot of propaganda. And while the West was still trying to figure out what exactly was going on in Crimea, Russia had already created a ghost occupation that was a fait accompli by the time Western policymakers were prepared to do something. So, that is an example of the new rules of war, where information and non-kinetic weapons are more powerful than blitzkriegs.

Following the discussion, Dr. McFate provided additional written inputs to supplement the interview session.

Dr. McFate: I wanted to double-back on a trend that is understudied yet has profound security implications: the privatization of war and how it's changing warfare. Mercenaries and their masters distort warfare in shocking ways, and facilitate wars without states. This will re-distribute power in international affairs, further eroding the Westphalian order and contributing to durable disorder.

We're not prepared to fight in a world where private warfare is rampant. For example, last year, 500 mercenaries attacked our best troops and aviation in east Syria and it took us four hours to beat them back. Four hours. What happens when we have to fight 5000 mercenaries? The threat is worse than people assume.

How does privatizing war change warfare? If conflict is commoditized, then the logic of the marketplace and the strategies of the souk apply to war. In other words, private war has its own logic: Clausewitz meets Adam Smith. This introduces new strategic possibilities known to CEOs but alien to military leadership, putting us at risk. Conventional war strategy may not work in private wars. Last year I had a Minerva grant to study strategies for private warfare. Here's a brief overview, separated between clients and force providers:

Strategies for Buyers (Demand Side):

- Bribe your enemy's mercenaries to defect.
- Retain all mercenaries in the area to deny your enemy a defense.
- Renege on paying mercenaries once they complete a military campaign.
- Give a larger mercenary unit a short-term contract to chase off or kill your unpaid mercenaries.
- Manipulate the winds of war by buying all the mercenaries available, driving prices up, then dumping them on the market, driving prices down.
- Engage in market defamation of specific mercenary units as a tool of accountability or blackmail.
- Rent new capabilities on the fly, such as a special forces team or attack drones, giving you maximum operational flexibility and unpredictability.
- If you have the money, outspend your rivals by waging an unlimited war of attrition. Mercenaries have a bigger recruiting pool than national armies, which are limited to their country's citizenry. The mercenary labor pool is global. This is especially useful when fighting a state committed to conventional war.
- Drive your adversaries into bankruptcy by stoking a mercenary arms race.
- Hire mercenaries as agents provocateur to draw others into a war of your choosing.
- Hire mercenaries for covert actions, maximizing your plausible deniability. This is useful for conducting wars of atrocity: torture, assassination, intimidation operations, acts of terrorism, civilian massacres, high-collateral-damage missions, ethnic cleansing, and genocide.

- Conduct false-flag operations: secretly hire mercenaries to instigate a war between your enemies, while keeping your name out of it.
- Hire mercenaries for mimicry operations to frame your enemies for massacres, terrorist acts, and other atrocities that provoke a backlash.
- Buy a large number of mercenaries, march them into your enemy's territory, and then release them, unpaid. Out-of-work mercenaries become bandits and will sow anarchy, accomplishing your mission on the cheap (unless your enemy hires them to attack you).
- Knowing the high danger of a mission, misrepresent it so that mercenary casualties will be extreme. Once they have achieved the mission, cut them loose and do not pay them. They will be too weak to challenge you.
- Hire multiple mercenary units to pursue the same objective without telling them. They will use different strategic approaches and sometimes work at cross-purposes. Reward the first unit that completes the mission and cut loose the rest, unpaid (hedging strategy).
- Hire multiple mercenary units to kill one another, thinning out their numbers and making them easier to control or swindle.

Strategies for Force Providers (Supply Side):

- Employ the shakedown strategy: blackmail or threaten the client for more money at a crucial moment.
- Start or elongate a war for profit.
- Negotiate and accept bribes from a client's enemies not to fight. Raise the price and offer to turn on your client, offering to stage a palace coup d'état.
- Bribe your enemy's mercenaries to defect, saving you battle costs.
- Secretly cut a deal with your mercenary opponents. Negotiate an outcome that benefits all mercenaries at the expense of clients.
- Engage in market defamation of clients as a tool of accountability or blackmail.
- Between contracts, become bandits for profit and artificially generate demand for protection services.
- Buy smaller mercenary units and incorporate them into your growing private army, giving you market power.
- Manipulate key military information that influences clients' business decisions in favor of your interests.
- Sell out your client to his enemy.
- Practice extortion and racketeering: Threaten to lay waste to a community unless it pays you protection money. Establish payments on an ongoing basis and raise prices whenever possible.
- Play multiple clients off one another to foster mistrust that leads to more war.
- Engage in Praetorianism: hold your client hostage and bleed him dry of wealth for as long as possible. Look for a new host when finished.
- Establish a warlord kingdom to extract wealth from an area. This is especially useful in highly volatile regions rich in natural resources.
- Capture a high-value asset like an oil field or a small city and sell it back to its owner. When complete, ask for a contract to protect it from others like yourself.
- Steal your client's assets.
- Kill off your competition to become a monopolist and raise prices.

Dr. Lukas Milevski

Assistant Professor (Leiden University)
2 March 2019

This two-part discussion considers, first, strategic asymmetries facing US military power in theater, and second, geopolitical asymmetries undermining US interests and the ability to express and support those interests on the world stage. Both parts are viewed over time, from the past then projecting into the future.

Strategy relies on the generation of asymmetries for advantage to achieve the desired consequences.[58] One can interpret statecraft similarly, albeit in a more peaceful and broader arena. The purpose of asymmetry is to minimize the ability of the opposing party to act usefully to its own advantage in the given environment.

The United States has done an excellent job since the 1980s of generating basic military asymmetry which has yet to meet any truly peer competitor. This is still true today despite concerns regarding the rise of current relatively peer, and future fully peer, competitors such as Russia and China. Regardless of their true status, these competitors cannot assume parity—their only prudent assumption is to believe that US military advantage endures and to prepare against that standard. It is widely recognized that US military advantage rests on a relatively narrow basis of predominantly information technology systems, which govern functions within individual weapon systems plus facilitate links between and among weapon systems, necessary to exploit their full range of technical and tactical potential. These IT systems together constitute, if not necessarily weakness, then certainly an aggregation of critical nodes whose disruption or destruction would disproportionately affect US military power.

To counter US military asymmetry, competitors must generate their own asymmetries which the US has already had, could yet have, and over time certainly will have trouble facing. This process has been in play since the 1990s, as the Gulf War and interventions in the prolonged collapse of Yugoslavia shook both Russian and Chinese military observers. Many existing counter-asymmetries already target US information dominance. These counter-asymmetries are not necessarily weapon systems, although some can be (e.g. Russian electronic warfare systems). Asymmetry can also be generated through new organization or new tactics—guerrilla warfare has been a consistent asymmetry plaguing the United States in Afghanistan and Iraq over nearly two decades despite the United States' technical advantages in gathering and employing information. Asymmetries, including those based on organization and tactics rather than weapon systems, have allowed strategic actors which are not at all rivals, let alone peer rivals, to stymie US strategy and policy for years on end.

Fortunately it is possible to follow, despite the veil of linguistic barriers, censorship, and perhaps outright propaganda and disinformation, the development of weapon systems meant to provide potential competitors with general or niche asymmetric advantages over the United States. Such research, development, and procurement decisions take years to mature and come to completion. It is possible to watch priorities change as defense budgets, particularly in Russia under the impact of sanctions and other forces, feel the pressure. Nonetheless the budgetary emphasis remains on weapon systems aimed at providing asymmetric counters to, if not asymmetric advantages against, US capabilities. Russia in 2018 made budgetary decisions in favor of modernizing existing weapon systems over procuring next generation systems such as the T-14 Armata or Su-57. Under financial pressure, Russia is providing relatively small investment in forces approximately symmetrical to US capabilities—although one should not underrate those symmetrical forces, as Russia still may have more battle-ready tanks than all of NATO combined and more MLRS than either the US or China, for example. Nonetheless, Russia is still funding asymmetrical capabilities such as electronic warfare, air defense, and a variety of missiles.

It is more difficult to track, much less assess, organizations and tactics for their potential to contribute to asymmetry generation. However, the US is now in the somewhat privileged position, previously occupied over decades by its competitors, of watching them, particularly Russia, employ not just some of these systems, but also the organizations and tactics required to use them effectively, on campaign in the Donbas or in Syria. Military exercises are another valuable source of intelligence on potential organizations or tactics for achieving asymmetry.

Asymmetry in competitor statecraft to undercut US interests is a far broader question and more relevant to China, whose economic might far exceeds Russia's. (This discussion is also relevant to question 11, not addressed separately.)

China in particular follows culturally specific notions of statecraft and strategy which emphasize what may be translated as "the propensity of things," the idea that conditions should be constantly shaped so that the eventual engagement, whether a battle or contest between non-military forms of power, is an easy victory because the context would not allow any other outcome.[59] This does not imply that there is a central plan to undermine the United States globally by threatening or using every potential military and non-

[58] Lukas Milevski. "Asymmetry is Strategy, Strategy is Asymmetry", Joint Force Quarterly 75 (October 2014), 77-83.

[59] François Jullien. The Propensity of Things: Toward a History of Efficacy in China. Janet Lloyd, trans. (New York: Zone Books 1995), chapters 1 and 2 are of particular interest here.

military instrument, but rather that China is willing to do so to shape the environment to its general advantage, presumably most often to the general disadvantage of the United States, now or in the future, when interests clash. Gambits such as building artificial islands or harassing non-Chinese ships in the South China Sea are examples of trying to shape the environment, as are the many Chinese loans provided to African countries. Whether or not such disparate environments ever become theaters of active competition, let alone conflict or war, is immaterial to the Chinese—they are perfectly happy implicitly to dominate regions without ever having to fight for them.

The Russian approach is more openly aggressive, founded upon both exacerbating existing divisions and, whenever possible, creating new divisions within and among their rivals. These divisions may be political, racial, social, etc. and primarily achieved not just through disinformation in the literal sense of providing false information, but also by misrepresentation of who is providing that information or contributing to a particular public debate. For example, the Russian firm Internet Research Agency sought to suppress the black vote in the United States during the 2016 presidential elections by creating active social media accounts posturing as part of this community and encouraging electoral boycott, among other tactics to lessen the political impact of the black vote.[60] The Russians also meddle in European politics, from bankrolling far-right parties in western Europe and Russian parties in the Baltic states to encouraging Brexit. Further still, Russian money encourages and spreads corruption in Western institutions, including political and financial institutions.

The main common feature of both the Chinese and Russian cases is ambiguity over who is acting, for what purposes, etc. It is not readily apparent that the Chinese are deliberately undermining US interests in a region, perhaps because they are only expanding their own interests, which shape the environment to give Beijing levers that make that environment inimical to US interests if necessary. Similarly, it is not readily apparent that it is Russia, which is causing, not just exacerbating, the many divisions which exist in the United States, if indeed most of its targeted tensions already exist independently of Russian interference.

The Chinese will exploit any potential environmental leverage and the Russians any potential weakness. Both types of non-military pressure, shaping the environment versus openly undermining, aim to inhibit the American (or other) political decision-making required to contest either Chinese influence or Russian actions. The ideal is to prevent a US response altogether by taking aim at the political level of decision-making, which is the prime mover for any strategy to contest China or Russia.

Robert Morgus

Senior Policy Analyst, Cyber Security Initiative and International Security Program (New America)
5 March 2019

Kinetic and Non-Kinetic Tactics of Near-Peer Competitors

In the context of great power competition over and through the internet, our near-peer competitors leverage a set of tools in a number of forums in pursuit their objectives. Importantly, in large part because of their systems of governance and economy, China and Russia are more able and adept at leveraging quasi- and non-governmental assets in pursuit of national goals than the U.S. and our friends. Despite some differences in motivation and approach, both China and Russia leverage diplomacy, cyber means, and trade in pursuit of their national goals.

China

A range of diplomatic, information, and trade activities emanating from China suggest a concerted effort on the part of the Chinese state to export its model for the digital space. While the activities of Chinese companies appear to comply with an overarching strategy of expanding Chinese digital influence, it is unclear how much of this compliance is driven by business or market incentives versus state pressure, noting that the two need not be mutually exclusive. The Chinese government's approach to global competition is characterized by the notion of expansion without conflict and shaping global institutions and rules.

[60] See Jason Parham. "Targeting Black Americans, Russia's IRA Exploited Racial Wounds", Wired.com, 17 December 2018, https://www.wired.com/story/russia-ira-target-black-americans/, accessed 18 February 2019.

Activities to watch:

- Regulatory exchanges,
- Participation in standards bodies,
- Technology exports,
- Telecommunications investments.

Diplomacy

In global forums, Chinese activities in the United Nations General Assembly around an information security code of conduct have received the most attention, other activities, particularly in technology standards bodies, are worthy of note. At the International Telecommunications Union, for instance, a Huawei executive chairs the study group tasked with developing standards for next generation (5G) telecommunications standards. Likewise, Chinese nationals and state employees are prominent in the only telecommunications standards body to actually publish a 5G standard to date, 3GPP. Similarly, at the Internet Engineering Task Force, the body that publishes standards particularly relevant to the internet protocols, China has gone from a near non-participant in the late 2000s to the second largest participant last year.[61]

In addition to increased participation in key standards bodies, China has increased its bilateral engagement with crucial third-party countries. These bilateral engagements include traditional diplomatic outreach and attempts to secure trade and investment deals as part of the Belt and Road Initiative, but also more direct transfers of ideas and frameworks through training seminars for regulators, policymakers, and lawmakers in Africa and Southeast Asia.[62]

Cyber

The Chinese government conducts public messaging campaigns in key markets to support economic and political objectives. These campaigns can come in the form of traditional advertisements willing consumers to buy Chinese products, but also take more opaque forms, as Beijing has invested in buying foreign media outlets and training foreign journalists to "tell China's story well, and properly disseminate China's voice."[63]

In addition, Chinese entities engage in state, quasi-state, and non-state economic espionage pointed at the theft of high tech intellectual property.

Trade

Chinese telecommunications companies Huawei and ZTE are already major providers for internet technologies worldwide. Their comparatively cheap products give them an advantage in markets that are not able to prioritize cybersecurity over cost savings, as is the case in much of the developing world. More research is needed on to understand the relationship between telecommunications projects and investment and the spread of regulatory, legal, and normative frameworks.

Russia

The Russian government views international relations as a state of perpetual conflict occurring along a continuum. For the Kremlin, the current rules and institutions that underpin global order often clash with Russian interests and values. Thus, rather than reshaping the rules or coopting institutions, as is the Chinese approach, Russia seeks to undermine the legitimacy of institutions and rules.

Activities to watch:

- UN initiatives around cybersecurity and information security,
- Information operations,
- Surveillance exports.

[61] https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/four-opportunities-for-states-new-cyber-bureau/
[62] https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism
[63] http://chinamediaproject.org/2017/09/29/the-fable-of-the-master-storyteller/

Diplomacy

Russia's primary diplomatic objective is to reassert Russia's right to sovereignty over the digital space within its borders. For Russia, the global rules governing the internet have been carefully crafted by western powers. It is therefore a primary objective of the Russian state to not only assert It is therefore a primary objective of the Russian state to not only assert Russia's sovereignty over the network within its borders, but to also "make other countries, especially the United States, accept" this right.[64] National laws, like the recently proposed amendment to the Federal Law on Communications, provide Russia with national legitimacy to do so. However, the Kremlin still seeks to normalize strict information control at the international level through initiatives like their proposal at the 2018 UN General Assembly to create a treaty reasserting national sovereignty over the internet and various cybercrime initiatives.[65]

Cyber

Through a combination of influence operations in key areas and persistent offensive cyber operations, Russia has successfully demonstrated the fragility of the global internet ecosystem, while also achieving other aims (like turning the power off in Eastern Ukraine in the dead of winter). This demonstrated fragility has increased policymakers' interest around the world in reasserting the role of governments in controlling the environment more tightly.

Trade

In comparison to China, Russia's trade reach is relatively modest. Nonetheless, Russia has successfully cultivated markets of its surveillance exports in its near abroad, parts of the Middle East, and Latin America. Russian companies like Prrotei and Peter-Service, for example, provide technology to help internet service providers in countries with legal and regulatory frameworks similar to Russia's SORM system comply with those regulations to monitor and filter traffic.[66]

Dr. Christopher Paul

Senior Social Scientist (RAND Corporation)
1 March 2019

Influence campaigns will be a significant strategy and tactic. Most of the time when we think about influence, we think about persuasive communication. However, if influence is getting others to do what you want, the kinds of activities that can be undertaken as part of influence is quite broad. Paul Watzlawick famously observed that "one cannot not communicate" and we all know that "actions speak louder than words." Clausewitz' equally famous dictum that "war is politics by other means" could be interpreted to suggest that war is just another form of influence. Similarly, Soviet-era Russian active measures included a wide range of efforts to manipulate perceptions (including covert broadcasting, media manipulation, disinformation and forgeries), but also included funding for front groups, purchasing the services of influential agents, incitement, assassination, and other forms of political violence.[67] All of these activities were influential.

This discussion will focus on communication-based influence campaigns. However, the problem of influence is bigger than just communication, and I encourage a broader interpretation and accept that on some fundamental level everything is about influence and almost everything a state does contributes to influence. Deterrence, compellence, coercion, and similar conceptions are all about influence. Further, while they have a communicative component, threats fundamentally involve capabilities outside of communication. All of the instruments of national power (diplomatic, informational, military, and economic) can contribute to influence.

Countries and non-state actors use communication-based influence operations for myriad reasons. Some countries use influence

[64] Andrei Soldatov and Irina Borogan, The Red Web, p. 223
[65] https://nsiteam.com/social/wp-content/uploads/2019/01/AI-China-Russia-Global-WP_FINAL_forcopying_Edited-EDITED.pdf, p. 88.
[66] https://nsiteam.com/social/wp-content/uploads/2019/01/AI-China-Russia-Global-WP_FINAL_forcopying_Edited-EDITED.pdf, p. 89.
[67] Abrams, Steve, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," Connections: The Quarterly Journal, Vol. 15, No. 1, 2016, pp. 5-31.

operations because they believe that they have been used successfully in the past (with Russia as an example), while others see them as their only means to countering an adversary like the United States, an adversary that maintains such a dominant conventional military capability that it is often not feasible to contest the U.S. in traditional warfighting domains. This is also why some of these same states invest considerable resources in cyberwarfare.[68]

Both states and non-state actors see influence operations as an asymmetric approach that can avoid escalation while still achieving important objectives. And while there is a strategic approach followed by some countries in the influence realm, with years of planning and lag time involved in amassing a reservoir of capabilities to be able to project influence in a particular country or region, there is also an opportunistic element, wherein countries respond to events on the ground as they happen in real time. Once again, Russia appears to be the dominant actor in this space, seeking to extend its reach into the Baltics, the Balkans and throughout Central and Eastern Europe to be able to respond to events as they unfold. Iran is now following a similar path as it works to extend its influence by building stronger networks in Africa and Latin America. In some cases, these efforts are viewed as a complement to actions in the kinetic realm. Over the course of the past several years, an emerging literature that discusses what some scholars and analysts have referred to as the 'gray zone,' an area of neither peace nor war, has contributed to this debate.[69] Conflict in the gray zone is comprised of actions undertaken by a range of adversaries actively attempting to minimize both the scope and scale of combat.[70] Driven by the perceived success of Russian information operations and propaganda, influence operations have become a key component of gray zone strategies.

Many of the key characteristics, capabilities and especially vulnerabilities of various actors' influence strategies are related to the ability of these actors to successfully adopt new technologies as they emerge. For actors possessing less technical acumen than their allies or adversaries, technology which is similar to something already in use is easier to absorb because it requires the least change in order to adopt and put into use.[71] As "deep-fakes" and other Artificial Intelligence (AI)-enabled capabilities related to the future of influence become more commonplace, they are likely to diffuse among state and non-state actors alike. The ability of an actor to correctly understand new streams of knowledge and harness this knowledge is determined by the relationship between the new knowledge and what the group and its members already know.[72] In some ways, this is a case of "the rich get richer" because, like China and Russia, the infrastructure is already in place to exploit new techniques and forms of knowledge.

Humans have come a long way from our earliest social communications, primitives telling each other stories around campfires. However, our neurocognitive processes date to that era. Our preference for story in cognition and memory, and our assessments of credibility at the neurophysiological level, predate any communication technology at all. The contemporary information landscape, with phone, video, and effectively instantaneous digital text communications enables a wide range of influence effects. Evolving technology will only create more. There are a host of potentially impactful technologies. These include the further development of "bots" (machine driven communications), the video fabrication technology called "deep fakes," the intersection of big data and influence in precision marketing, the harnessing of non-verbal cues and precision targeting in neuropolitics, and the compounding threat of automation, AI, and machine learning coupled with any of these other technologies.

First, consider "bots" and other machine-driven communications (MADCOMs). The present has a heavy bot population; as of 2017, an estimated 15% of Facebook "users" were in fact bots.[73] This proportion grows in the future and spans all social media and text-based digital engagement. "Ten years from now, you won't be able to tell whether you're interacting with a human online or not. In the

[68] Chad C. Serena and Colin P. Clarke, "America's Cyber Security Dilemma—and a Way Out," Defense One, December 22, 2016, https://www.defenseone.com/ideas/2016/12/americas-cyber-security-dilemma-and-way-out/134105/?oref=d-river

[69] The terminology is often debated. Mark Galeotti has referred to variations of 'gray zone conflict' as 'guerrilla geopolitics,' 'non-linear war,' 'hybrid war,' and 'special war,' at various points. See Mark Galeotti, "The 'Gerasimov Doctrine' and Non-Linear War," In Moscow's Shadows, July 6, 2014, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

[70] Adam Elkus, "50 Shades of Gray: Why the Gray Wars Concept Lacks Strategic Sense," War on the Rocks, December 15, 2015, https://warontherocks.com/2015/12/50-shades-of-gray-why-the-gray-wars-concept-lacks-strategic-sense/

[71] Shanti Gopalakrishnan and Paul Bierly, "Analyzing Innovation Adoption Using a Knowledge-Based Approach," Journal of Engineering and Technology Management, Vol. 18, 2001, pp. 107–130.

[72] Bronwyn H. Hall and Beethika Khan, Adoption of New Technology, Cambridge, MA: National Bureau of Economic Research, 2003.

[73] Rid, Thomas, Hearings Before The Select Committee On Intelligence United States Senate, "Disinformation A Primer In Russian Active Measures And Influence Campaigns," March 30, 2017.

future, most online speech and content will be machines talking to machines."[74]

The proliferation of inauthentic "persons" as interlocutors has potentially dire social consequences. In addition to being inauthentic and potentially undermining trust in environments in which they reside, bots impact influence, now and in the future. They can be used to inflate a real person's follower or "like" counts, making them appear more popular than they are and mobilizing influence through "social proof," they can add weight in online conversations and on message boards, can be used to attack others, manipulate public opinion, and manipulate search results rankings.[75]

Deep fakes "make it possible to create audio and video of real people saying and doing things they never said or did."[76] Though early efforts were easily detectable as fraudulent, quality is improving, and threatens an "arms race" with technology designed to detect such fakes (for example, an early detection algorithm noted that deep fakes, as amalgams of a clips of a real person, often failed to blink realistically often; however, knowing that this is a possible means of detection, deep fakers have compensated and added blinking at appropriate frequency).

While currently deep fake technology requires a fair amount of sophistication and is in the hands of only expert programmers and academics, it will not stay that way, and is likely to diffuse and democratize rapidly.[77] Deep fakes pose several threats to individuals, organizations, and societies. Among the laundry list of potential risks is the potential alibi deep fake ubiquity could provide to bad actors: if caught misbehaving on film, a bad actor might deny the truth of their behavior, instead asserting that it was fabricated.[78]

The idea behind precision marketing is to get just the right ads in front of just the right individuals in a way that meets everyone's interests: producers get their products and services displayed to those most likely to want/need/buy them, advertisers serve producers well and are rewarded for the success, and consumers are exposed to products and services they are likely to desire. The system works by exploiting big data jointly with other technologies to identify very small market segments and put the right ads in front of them. Unfortunately, when disinformation operators leverage this system for precision propaganda as part of an influence campaign, the incentive and reward structure no longer aligns favorably for everyone, and is not in the public interest. Precision marketing (or precision propaganda) relies on five key ingredients: behavioral data collection, digital advertising platforms, search engine optimization, social media management software, and algorithmic advertising technology.[79] Although the use of precision marketing advertising for propaganda purposes is not in the public interest and does not serve the interests of all stakeholders, there are perverse incentives that make it profitable or beneficial to some stakeholders (specifically the propagandists and the advertisers). Because of these perverse incentives, expect the use of precision marketing tools for influence campaigns to increase.

Advancements in neuroscience have the possibility of changing the influence landscape, too. The nascent field of neuropolitics includes consultants using a host of biometric techniques (EEG and various electrodes and monitors, but also simple cameras to capture eye movements, expressions, etc.) in order to evaluate emotional state and to measure responses to messages or campaign spots.[80] The goal is to discern voters' intentions from subtle signals they are likely unaware they are producing. Neuropolitical consultants can already diagnose the presence or absence of six core emotions using a camera.[81]

The prospect of autonomous warfare has been discussed for decades, but most of these discussions have focused on the physical

[74] Chessen, Matt, The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, and Threaten Democracy and What Can Be Dona About It, Washington, D.C.: Atlantic Council, 2017.
[75] Treré, Emiliano. (2016). "The dark side of digital politics: Understanding the algorithmic manufacturing of consent and the hindering of online dissidence." IDS Bulletin 47.1; Woolley, Samuel. (2016). "Automating Power: Social Bot Interference in Global Politics," First Monday 21(4); Kollanyi, Bence, Philip N. Howard, and Samuel C. Woolley. (2016). "Bots and Automation over Twitter during the First US Presidential Debate." Project on Computational Propaganda.
[76] Chesney, Bobby, and Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, Social Science Research Network, July 14, 2018, p. 1.
[77] Chesney, Bobby, and Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, Social Science Research Network, July 14, 2018.
[78] Chesney, Bobby, and Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, Social Science Research Network, July 14, 2018.
[79] Ghosh, Dipayan, and Ben Scott, Digital Deceit: The Technologies Behind Precision Propaganda on the Internet, Policy Paper, January 23, 2018.
[80] Svoboda, Elizabeth, The "Neuropolitics" Consultants Who Hack Voters' Brains," Technology Review, August 16, 2018.
[81] Svoboda, Elizabeth, The "Neuropolitics" Consultants Who Hack Voters' Brains," Technology Review, August 16, 2018.

domain. Crude automation has long existed in in the information environment in the form of digital communication networks that are programmed, but modern automation has gone much further and is poised to continue advancing. Coupled with several of the technologies above, however, the promise (and threat) from AI and machine learning is considerable.

In this space, thoughtful application of AI makes everything faster, more comprehensive, and better. For bots and MADCOMs, AI and machine learning quickly improve the verisimilitude of artificial personas, making it harder to discern whether an interlocutor is human or not.[82] Similarly, machine learning can be applied in the generation of deep fakes, learning from real video or learning from efforts to detect deep fakes.[83]

In fact, one of the biggest potential game changers from AI comes from advances possible in letting two different machine learning systems compete with and learn from each other. Called "generative adversarial networks," or GAN, the technique employs two neural networks simultaneously.[84] One works to mimic reality (a seed dataset of real conversations or video), while the other works to assess the extent to which the first succeeded in mimicking reality. They then proceed in an (incredibly rapid) iterative fashion, each learning from the other and making rapid improvements. [85]

There is a significant threat at the intersection of MADCOMs, AI, precision targeting, and neuropolitics. Imagine a set of neural network driven bots, that, instead of experimenting iteratively with other neural networks (like in a GAN) are instead experimenting with interactions with real human targets. Using precision targeting and big data to identify initial targets and primed with initial hypotheses about what kinds of messages and engagements might move these individuals, a well-designed autonomous network could engage through multiple bot personas and then track responses (either just the target's conversational response, or, if a webcam could be activated, biometric markers).[86] The system could track, correlate, and apply machine learning techniques to identify which specific phrasing and messages resonated most with individuals with certain characteristics based on this experimentation, and thus target subsequent individuals with not only custom tailored persuasive messages, but with *iteratively incrementally improving* custom tailored persuasive messages. An automated and machine learning-driven system would not necessarily be constrained by the kind of experimental approaches that existing influence experts might try based on their own experiences, perhaps finding atheoretical techniques and cues that just "work."[87] Taken all together, this is scary. Machine-scale engagement (so able to interact with and monitor responses from tens of thousands of people at once); able to learn from all of those interactions (so with ever-improving ability to impersonate a real person); learning from actual generated responses (or non-responses; the system still learns if it says something that leads you to stop taking to it); connected to and correlated with big data for micro-segmenting (so, not just learning how to influence a single individual, but learning how to potentially influence others like that individual); and with an experimental mindset, turning each success and failure into a refinement for future efforts.[88] An adversary taking this approach could quickly become increasingly effective at manipulating attitudes and behaviors.

Linda Robinson

Senior Researcher (RAND Corporation)
13 March 2019

Our research found that both state and nonstate actors pursue their aims through a robust set of nonkinetic means, and that these may be effectively employed to destabilize, subvert, and coopt states. These measures can by themselves constitute an effective means of achieving aggressive objectives. They may also be a precursor to overt war, used to prepare the battlefield for more

[82] Telley, MAJ Chris, "Influence at Machine Speed: The Coming of AI-Powered Propaganda," Mad Scientist Laboratory: TRADOC G2 Blog, May 24, 2018.
[83] Chesney, Bobby, and Danielle Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, Social Science Research Network, July 14, 2018.
[84] Goodfellow, I.J. et. al., Generative Adversarial Networks, https://arxiv.org/abs/1406.2661 10 June 2014.
[85] Adams, Terrence, "AI-Powered Social Bots," Cornell University Library, June 16, 2017.
[86] Telley, MAJ Chris, "Influence at Machine Speed: The Coming of AI-Powered Propaganda," Mad Scientist Laboratory: TRADOC G2 Blog, May 24, 2018.
[87] Wu, Katherine J., "Google's New AI Is a Master of Games, but How Does It Compare to the Human Mind?," Smithsonian.com, December 10, 2018. As of December 21, 2018:
https://www.smithsonianmag.com/innovation/google-ai-deepminds-alphazero-games-chess-and-go-180970981/
[88] Telley, MAJ Chris, "Influence at Machine Speed: The Coming of AI-Powered Propaganda," Mad Scientist Laboratory: TRADOC G2 Blog, May 24, 2018.

expeditious outcomes. Finally, they may be used in combination with conventional military means in a hybrid warfare mode.

In our study, Modern Political Warfare: Current Practices and Possible Responses[89], we documented a range of practices across the diplomatic, informational, military and economic (DIME) spectrum that were short of conventional war but effectively advanced the actor's aggressive objectives. Apparently benign activities may be used to conceal more actively hostile activities or recruit actors for potential malign uses. The use of quasi-governmental or nongovernmental organizations including cultural institutes, social clubs, religious organizations is a significant means seen in the use of "soft power" by Russia, Iran and China. Advisory and logistical support may be given to paramilitary groups or militias. The weaponization of social and nongovernmental groups such as these is likely to continue and even increase as they represent stealthy methods to recruit local nationals and penetrate societies using local nationals to carry out the hostile activities. The manipulation of the information environment using social media and other informational conduits enabled by worldwide communications and the largely unregulated information space is likely to continue apace or increase exponentially in those countries not sealed off by aggressive government firewalls. Finally, in the kinetic sphere weapons development trends include the development and employment of a suite of nonlethal technologies that accomplish military objectives, including electromagnetic pulse, laser, microwave weapons. The recent apparent attacks on diplomats in Cuba and elsewhere suggests the type of stealthy hostile measures that might be increasingly employed in the future. Cyber attacks that disable critical infrastructure and defense systems represent a likely major feature of future hostilities. The future may involve much less kinetic warfare but equally destructive nonkinetic warfare.

Modern Political Warfare: Current Practices and Possible Responses found that state and nonstate actors tend to adapt a particular DIME approach to political warfare that draws on their own cultural and organizational strengths. While recognizing these differences, the study identified a number of common attributes that characterize the current practice of political warfare. These may be expected to continue or increase. They are:[90]

- Political warfare employs diverse elements of power across the DIME spectrum
- Political warfare relies heavily on unattributed forces and means
- The information arena is an increasingly important battleground, and success is often determined by perception rather than outright victory
- Information warfare works in various ways (e.g., amplifying, obfuscating, and sometimes persuading; cyber tools exacerbate effects)
- Economic leverage and coercion are increasingly preferred tools
- Political warfare often exploits shared ethnic or religious bonds and internal seams
- Political warfare extends rather than replaces traditional conflict, and can achieve aims at lower cost (alternative and antecedent)
- Non-state actors can conduct political warfare with unprecedented ability

Note on terminology

There is a need for further examination and clarification of the lexicon for the suite of measures employed in the competition and conflict space below the level of conventional or thermonuclear war. Numerous terms are used, sometimes interchangeably, which complicates analysis of what is an inherently complex, multifaceted and ambiguous form of warfare. Our RAND study sought to frame this challenge for further study to reach a consensus among the research and policy stakeholder community:

- "Political warfare is but one term among many that describes the arena of conflict short of conventional warfare. Chinese analysts have employed the term "unrestricted warfare," Russian officials have used "soft power" and "new generation warfare," and a variety of terms are in use by U.S. officials, including "gray zone conflicts," "hybrid warfare," "asymmetric warfare," and "irregular warfare." The latter term has been officially defined in U.S. military doctrine and Department of Defense (DoD) directives, but one impetus for a new nomenclature is to place emphasis on the nonmilitary and nonlethal elements of this form of warfare. Those elements may be readily combined with conventional warfare, but the focus of this

[89] RAND (2018). https://www.rand.org/pubs/research_reports/RR1772.html
[90] Robinson et al., Modern Political Warfare: Current Practices and Possible Responses (RAND, 2018), Chapter 6, pp. 219-244. https://www.rand.org/pubs/research_reports/RR1772.html

examination is on the less obvious, more ambiguous forms of conflict that may catch policymakers unaware if they are insufficiently attuned to these methods and their abilities to sow conflict, weaken, destabilize, disrupt, and, in some cases, create more dramatic consequences, as seen in Russia's rapid annexation of the Crimea without resorting to all-out warfare. This examination of political warfare does not presuppose that this term is necessarily the most apt appellation for current nonconventional contests of power, but it employs the term as a matter of historical record and convenience to bound the study. to the nonmilitary and nonlethal military methods used. By the same token, measures short of war may be usefully employed to deter conflict or prevent it from escalating or worsening."[91]

Dr. Jaganath Sankaran

Assistant Professor (University of Texas at Austin)
8 March 2019

Kinetic weapons that might be able to undercut US interests can be broadly classified as A2/AD systems. Many of them such as ballistic and cruise missiles have existed for a while, but are now operating with some improved technology. In some instances, advanced variants such as hypersonic missiles, if they attain operational maturity, might significantly impact US forward presence and power projection capabilities. It also seems that many of the weapon systems that went offline after the Cold-War such as anti-satellite weapons are gaining prominence again with China and Russia. All of these weapons will dilute U.S. military capacity.

Among non-kinetic tactics, coercion against allies (using the methods described above) might pose the greatest challenge to US interests. If competing powers are able to force/entice allies and friends to distance themselves from the U.S., it might significantly impact the hard and soft power of the U.S. The diplomatic capabilities of the U.S. should be directed to prevent such an outcome.

Dr. Jacquelyn Schneider and Dr. Julia Macdonald

Dr. Jacquelyn Schneider
Hoover Fellow (Hoover Institution)

Dr. Julia Macdonald
Assistant Professor, Josef Korbel School of International Studies (University of Denver)

4 March 2019

Unmanned Capabilities and the Future of Great Power Competition and Conflict

With the 2018 National Defense Strategy, the U.S. has pivoted away from the wars it has equipped and planned for since 9/11. Over those 17 years, the U.S. has devoted significant resources in technologies, tactics, and campaigns to fight an asymmetric adversary whose threat feels increasingly remote to an insulated U.S. population. Unmanned technology has become central to the United States' military and foreign policy in these wars and the U.S. has doubled down on unmanned systems in its warfighting strategies. But what will the role of unmanned technology be as the U.S. focuses on great power competition and conflict? What are the characteristics of unmanned technology that make them unique to other weapon systems and how might they be optimized in competition prior to conflict and then in the transition to conflict?

In this analysis, we argue that in great power competition prior to armed conflict—in which political cost and escalation is privileged over battlefield objectives—unmanned systems have the most impact by mitigating political cost and decreasing risk to operators. However, in the transition to conflict with great powers, unmanned systems must optimize on economic cost and create mass instead

[91] Robinson et al., Modern Political Warfare: Current Practices and Possible Responses (RAND, 2018), xiv. https://www.rand.org/pubs/research_reports/RR1772.html

of mitigating political cost. This leads to two trajectories for unmanned weapons development: expensive and exquisite remotely-operated unmanned platforms for gray zone competition and cheap, expendable autonomous unmanned platforms for great power conflict.

First, what makes unmanned technology unique? There are a series of warfighting characteristics that help us understand the missions and roles that different weapons play in campaigns: range, precision, firepower (lethality), mass, maneuver. Some of these characteristics are independent of whether or not a human is inside the machine. For instance, precision and firepower are more closely linked to the weapons and sensors on-board than human operators. However, what unmanned technology provides over manned counterparts are potentially unique opportunities for range, mass, and maneuver. Additionally, unmanned technologies provide the additional benefit of insulating operators and political decisionmakers from risk. However, each of these characteristics competes with the other and therefore its helpful to examine history of revolutionary technology to understand which characteristics DoD decisionmakers should privilege as they invest in weapons with unmanned characteristics.

In order to draw from historical lessons, we turn to Krepinevich's work on military revolutions which identifies ten revolutions, ranging from the infantry revolution to the information revolution. In examining these revolutions, we find that range and maneuver are in themselves insufficient characteristics to create a theory of victory in a military revolution. Additionally, no previous military revolution has privileged human or political risk over the economic cost of warfare. Instead, technologies or strategies that created military revolutions introduced extraordinary advancements in lethality or firepower (often in conjunction with range) or changed the calculus of the economics of warfare to dramatically advantage early adopters of the military revolution.

Interestingly, despite the focus on building longer and longer-range weapons throughout history, states have been largely unable to maintain superiority or successfully conquer territories with these weapons. For every attempt to remove the man from the battlefield, counter-weaponry brings the man back. The exploration of history also shows that range on its own is seldom enough to create a revolution and that there is a strong relationship between increases in firepower and lethality with increases in range (and subsequent incentives for first strike). Further, advancements in maneuver cannot create revolutionary changes in warfare unless they significantly affect maneuver at the operational or strategic level. Increases in tactical maneuver (for instance, the increased amount of Gs from an unmanned airframe) have only short-term effects on tit for tat weapons development.

This suggests a potential theory of unmanned warfare that pivots away from range or maneuver (two of the dominant characteristics of current discussions about unmanned advantages) and focuses instead on political risk in competition and mass and economic cost in conflict. Mitigating economic cost helps create mass and increase firepower (thus also increasing range) and mitigating political cost allows states to use weapon systems without disenfranchising domestic populations (important for post levee en masse conflicts) or in escalating conflicts with adversaries willing to sustain costs over time. Therefore, in low stakes warfare or great power competition in which the U.S. is concerned about escalation, unmanned systems should privilege political risk above all other characteristics. This means investment in unmanned strike technologies that are potentially expensive and exquisite with costly sensors and remote operations by human controllers. In contrast, in conflict these systems that mitigate political cost have little utility. Because of the lack of quantity, these systems become high demand low density assets that require protection by other assets. Therefore, unmanned systems in great power conflict must be designed to decrease economic cost, serving as missile soakers, adversary cost imposition capabilities, and resiliency/redundancy creators.

Both competition and conflict see an advantage for unmanned intelligence, surveillance, and reconnaissance missions—especially for sensors that can be deployed in mass and for low cost. As competition moves to conflict, these sensors need to become more and more replaceable with quick turnover times to replace destroyed sensors as well as resilient networks that are able to adapt to constant sensor replacements. Additionally, unmanned sensors that will succeed in conflict must be able to operate autonomously and have multiple modes of transmission to central repositories of information. Unmanned platforms that are high capability but also in low numbers (for example the Global Hawk) will be increasingly suboptimal as conflict intensifies. These platforms will have to be protected in a similar manner as manned alternatives and therefore will lose any revolutionary capability in conflict.

Finally, the geography of warfare plays an important role in the future role of unmanned technology in warfare. Warfare over open seas or in the air—where the vast majority of great power competition and conflict is envisaged—will necessarily privilege economic cost in building unmanned systems. Urban warfare, in which civilian deaths are a high risk and terrain is cluttered, will necessarily increase the economic cost of unmanned warfare because of the need to build sensors that can function in these environments.

However, the increased economic cost of unmanned systems in urban warfare may be mitigated by the high cost of combatting unmanned systems in those environments (where barrage fire isn't utilized). Finally, if a core tenet of urban warfare is winning civilian opinion, then unmanned systems that privilege political or human risk will contribute to long term victory.

Dr. Peter Schram

Assistant Professor, Department of Political Science (Vanderbilt University)
3 March 2019

I will answer this question in the context of Russia's political tampering (broadly speaking). To date, Russia has been undertaking a series of political manipulations. Russia is undertaking kinetic and nonkinetic operations that undermine Western states' national unity, that undermine traditionally anti-Russia international organizations, and that support pro-Russian policies or activities. Together, these activities appear to be conducted with the intent of shaping the political landscape of US and Europe in ways that would make the West less able to counter Russian interests.

In undermining Western states' national unity, Russia is seeking to create a more fractionalized world. Russia has conducted propaganda operations supporting California breaking off from the rest of the United States and Catalonia splitting from Spain. In the 2008 Russian Georgian War, Russia empowered the break-away republics of South Ossetia and Abkhazia to pursue autonomy from Georgia. Several arguments could be made as to why creating more states, even if these states are not natural allies of Russia (like California), advances Moscow's interests. As one explanation, the international institutions that currently challenge Russian interests rely on overcoming collective-action-type problems. Mechanically, more states means more opinions, which can strain international cooperation. Second, through Coase Theorem type arguments, consolidated entities may function better than multiple distinct entities. The efficiency losses from one state becoming two could be significant and could (through relative gains) strengthen Russia.

Russia is also attempting to weaken traditionally anti-Russian international organizations. Russia has supported various right-wing Nationalist movements in Europe, including the Brexit campaign, as a means to undermine European support for international institutions. Additionally, Russia has undertaken kinetic operations that either attack potential NATO allies -- like Russia's annexation of Crimea and support for rebels in the Donbass – or has undertaken small, ambiguous operations against NATO's recently inaugurated smaller members – like the cyberattacks in Estonia. In all cases, these behaviors constrain or strain the international cooperation that has historically balanced Russian ambitions. Undermining international institutions seems to be of particular interest to Russia, as evidenced by Russia's support of right-wing nationalist groups. Traditionally, right wing parties in Europe and the United States have been hawkish on Russia; this means that even if some far-right parties are persuaded by to be more pro-Russia through Moscow's influence, any functioning political coalition that these far-right parties form will contain more moderate-right members that will likely be more hawkish on Russia. In some cases, it is telling that Russia is willing to empower political coalitions that could be more hawkish on Russia so long that these coalitions are against international political participation.

Russia is also supporting pro-Russian candidates and undertaking activities to minimize anti-Russian sentiment. A small Russian bank was the first to offer Marine Le Pen a loan for her presidential campaign. In several European countries, Russian dissidents are being assassinated; while the assassinations do create anti-Russian sentiment, in the long-run they may deter future individuals from speaking out.

In all likelihood, Russia will continue conducting activities like those mentioned here. These types of political manipulations have been conducted for the past decade and throughout the Cold War, suggesting that Moscow believes they are effective. That being stated, it is difficult to predict the nuts-and-bolts of political manipulations over the next ten years. This is hard to predict because Russian operations will be in response to the steps that the US takes to prevent these political manipulations. For example, if under scrutiny Facebook changed its policies to prevent fake news stories from propagating, Russia could switch to Twitter or use various message boards.

Dr. Steve S. Sin

Director, Unconventional Weapons and Technology Division (University of Maryland START)
13 March 2019

In the coming decade, strategic competitors of the United States will continue their development of advanced weapon systems such as the sixth-generation fighters and autonomous weapons to maintain their competitiveness and close technological gaps with the United States. The advanced weapon systems developed and deployed by our strategic competitors will technologically be at least as advanced as those of the United States. Though our strategic competitors may not field as large of a number of units equipped with these advanced weapon systems as the United States, they will certainly aim to field a large enough force equipped with these systems so that they can attain and maintain domain superiority against their regional neighbors and rivals while simultaneously allowing them to attain and maintain limited-duration domain parity against the United States.

Non-kinetically, our strategic competitors will continue to develop their offensive cyber capabilities designed to disrupt and degrade combat effectiveness of the United States military. Additionally, they will continue to focus on further developing their capabilities to conduct offensive cyber-physical operations, targeting both civilian and military infrastructures. Additionally, they will continue to conduct domestic disinformation campaigns to discredit and sow discontent against the United States to their domestic audience. Simultaneously, they will increase the intensity of their influence operations against the United States audience with the primary goal of destabilizing our societal fabric and eroding our trust in our institutions.

Finally, also on the non-kinetic front, our strategic competitors will intensify their campaigns to diminish the United States' influence among the international community by offering it "alternatives" to the Bretton Woods system. A good example of this is the path China has been on for the entirety of the 21st Century. Throughout this century, China has been engaging with those countries who have been less successful or (perceived to be) marginalized in a globalized world founded on the Bretton Woods system by offering them "alternatives." Its efforts have proven to be quite beneficial for China's national interests, as they have successfully been eroding the influence of the United States throughout several regions of the world over the past 18 years – especially throughout Asia and Africa. Over the next decade, not only China, but other strategic competitor(s) of the United States will intensify this type of overt political and economic campaigns – along with all the usual behind-the-scene operations that accompany such overt campaigns – that will continue to erode the United States' influence throughout the world. The ultimate goal of these campaigns will be for our strategic competitors to establish regional hegemonic spheres of influence advantageous to them and further isolate the United States in their regions of interest.

Dr. Robert S. Spalding III

Brigadier General (ret) (US Air Force)
24 February 2019

The character of global competition has already begun to change. Today competition between nation states is waged primarily in the economic, diplomatic and informational domains. Military remains an effective regional tool employed against weaker states. In this global competition China is the most powerful just due to sheer economic heft. Russia continues to exert outsize power in the informational domain, because of its decades of experience left over from the Cold War. North Korea, Iran and others exert regional influence, and more importantly play the larger powers off one another.

Information domain – The Internet was built on a foundation of sand as it moved quickly from a military project to a commercial success. Today with the advent of smart devices it has become an essential feature of society and that gives the Internet enormous power as a tool of statecraft. The evolution of the airplane provides a good proxy for thinking about the use of the Internet as a weapon. It was not until the invention of GPS, stealth, space-based C4ISR that the airplane really demonstrated the potential of theorist's imaginations.

Like the initial application of flight to the battlefield, the Internet has mostly been used as an intelligence gathering platform. This

ability to gather intelligence provides nation-states with information on industrial base, financial institutions, diplomatic efforts and can be targeted to individual personalized data. The smart phone gathers metadata that allows for targeted intelligence gathering if required.

There is evidence, however, that the Internet is beginning to come into its own as a weapon system. While past experience has shown the Internet can be used to cause physical damage to industrial systems, we have not yet truly witnessed widespread use to create massed effects on the battlefield. But the lack of a true cyber war that creates effects on fielded military forces masks the true power of the Internet as a weapon. This also reduces discussion about the role of cyber on the battlefield to constant speculation on what could be done.

Instead military theorists and strategists need to mentally leave the battlefield of today and open up to the reality of everyday life. The first recognition of the battlefield of today-tomorrow is currently taking place in academia. The concept of Social Cyber Security is presenting an operating concept for future warfare as conflict migrates away from the kinetic to the cognitive. This is not some theoretical concept developed in war colleges. This is empirical analysis of ongoing campaigns. In other words, adversaries are gaining experience on the battlefield of today-tomorrow right now, while US practitioners fight on the "real" battlefields of today.

Combining personalized data with big data analytics and artificial intelligence today-tomorrow warriors are targeting and influencing individuals and groups. The effects caused are leading to large spontaneous protests and individualized targeted attacks. These warriors never need to learn to use weapons, their proxy soldiers use their own weapons and networks to create the intended effects. One recent example was the protest on the evening of the 2016 election in New York. Ostensibly organized by members of Black Lives Matter, subsequent investigation revealed it was Russian operatives.

These techniques are being refined on the today-tomorrow battlefield. As artificial intelligence becomes more sophisticated the ability to scale this type of warfare will grow. Additionally, as 5G networks become more prevalent the machines connected to these networks can be blended to increase the chaos.

Economic Domain – China has learned how to harness the power of globalization to enlist the private sector in its quest for power. The China market of 1.4 billion people is an enormous draw for corporate America, and no board of directors can effectively ignore it. This means that they are bound by duty to the corporation to do what it takes to enter the Chinese market and compete.

The price for market entry is often technology transfer, which results in a decrease in the long term viability of the firm. Since reporting requirements have a shortened time horizon, this long term risk is often discounted by the board with the chief defense invoked being that only old technology is introduced. Yet, China has demonstrated an ability to acquire and innovate faster than these companies can defend their intellectual property in the marketplace.

In addition to the large market, China uses large financial reserves to acquire stakes in leading technology companies. Many of these companies have technology developed using US government grants by the Department of Defense. Once acquired, the technology is moved into the Chinese eco-system for use by both the military and business sector. Chinese scientists refine the technology list as new discoveries come out, ensuring the entire apparatus is kept updated as to what China values.

When combined with the evolution of influence in the information domain, this economic warfare will ensure the tools of the battlefield are developed and produced by China. This affords them enormous power as they seek to synchronize the economic and information campaigns towards ever more targeted and nuanced effects.

Diplomatic domain – The combination of the economic and informational allows for diplomatic success in multi-lateral institutions and other geopolitical forums. The ability to condition a population towards a certain policy coupled with targeting elites, business people and politicians through inducements or other financially beneficial relationships ensures political outcomes do not require force on force actions. This has already been democratized on the today-tomorrow battlefield, and will only become more opaque and nuanced as actions appear to be more self-inspired than conditioned from without.

In essence, the evolution of technology like the computer has surpassed the capacity of warfare as we know it to protect the socio-political independence of a nation-state in the globalized world. The solution to this problem may require a technological design

baseline which inculcates relevant documents like the constitution into the fabric of technological development. Already large tech companies are surpassing the power of a nation-state to influence. As government employees, elites, business people and politicians become incentivized to disregard or in some cases suppress democratic principles because they believe it is the right and proper thing to do the irrelevance of military power may become a fait accompli.

Nicolas Véron

Senior Fellow (Bruegel and Peterson Institute for International Economics)
11 March 2019

Aggressive interference behavior from Russia has been observed in recent years in electoral and other democratic processes throughout the advanced Western economies and particularly in the United States, United Kingdom, France and other EU countries. This behavior is likely to continue if not met with robust counteraction.

By contrast, China has mostly relied on attraction and positive incentives to build up its bilateral relationships with individual countries around the world, a stance reflected in the Belt and Road Initiative pursued since 2013. While the Chinese government has adopted repressive policies vis-à-vis its own citizens and Chinese diasporas abroad, its behavior with foreign countries has generally not be openly confrontational in the last decade, in contrast to Russia during the same period.

Valentin Weber

DPhil Candidate (University of Oxford)
Research Affiliate, Centre for Technology and Global Affairs (University of Oxford)
4 March 2019

During the last decade, the predominant effect of cyberattacks between major cyber powers has been non-kinetic. Recent advanced nation-state cyberattacks on the US included the 2016 Democratic National Committee email leak, the Office of Personnel Management data breach, Chinese theft of the F-35 fighter jet plans and the transformation of it into its very own J-31 fighter jet. Those attacks will likely continue as spying is difficult to deter and does most commonly not lead to immediate escalation.

In the next decade kinetic cyber-attacks are likely to become more common. On the one hand, this is due to the fast merging of data and objects and the rapid proliferation of the Internet of Things (IoTs). A 2017 IHS Markit analysis estimates that by 2030 there will be 125 billion IoT devices. On the other hand, I expect kinetic attacks to become more widespread because of the poor security of IoT devices.

Largely non-kinetic threats to the confidentiality, integrity, and availability of data already led to the addition of *election infrastructure* as a national critical infrastructure. It is likely that in the future kinetic threats will repeatedly lead to a redefinition or to a blurring of what national critical infrastructure is and what it is not. At the moment, when one thinks about transport as a national critical infrastructure one might enumerate public transport systems, such as planes or trains. One does not think about the average commuter that is stuck in a traffic jam every morning. However, in a future where most cars will be autonomous and linked to the internet in one way or another: What will be the difference of an American Airlines plane being grounded by an attack on the one hand, and a hundred autonomous vehicles being crashed at the same time on the street by a cyberattack? Is it more critical to protect the former than the latter?

While cyberattacks probably will most likely not lead to a Cyber Pearl Harbor, as illustrated above, it is expected for major countries to push boundaries in this respect and see whether and to what extent this “extended national critical infrastructure” can be manipulated. This will open new attack surfaces not only in in the United States but also in Russia and China. Nevertheless, China and Russia have worked diligently towards closing their countries off the global internet, which may arguably reduce their vulnerability. China has been very active refining its Great Firewall. Russia too, has shown that it is serious in reducing domestic vulnerability. It has

eyed disconnecting its internet from the world since at least 2014.

Implications for an integrated US strategy

More IoT devices translate into an increased vulnerability in the short term, especially because of the United States' strongly interconnected and open internet. IoT devices are notorious for their insecurity. It may be possible to build in proper security into the IoT parts of what has traditionally been considered national infrastructure, such as the energy sector or government facilities sector. But the attack space is much larger. It includes privately owned devices by individuals and companies. In these spaces there has been and continues to be a cyber security market failure that prevents proper cyber security design and practices to develop.

In the long-term this vulnerability may prevent the US from exercising an integrated strategy. Despite its large military spending and capabilities to project power abroad the US remains vulnerable at home. And because it is vulnerable at home its actions abroad may be endangered.

Ali Wyne[92]

Policy Analyst (RAND Corporation)
8 March 2019

America's Psyche

While America's adversaries and competitors will likely continue to invest in asymmetric capabilities that aim to limit its capacity to project force, they recognize that they would incur enormous losses were they to confront it directly. As such, they may instead try to exploit potential psychological vulnerabilities—vulnerabilities that will grow in proportion to America's uncertainty about its strategic course:

- Goading the United States to Overreact: Osama bin Laden gloated in late 2004 that he could easily "provoke and bait" Washington.[93] While it cost al-Qa'ida at most $500,000 to execute the attacks of September 11, 2001,[94] the United States has spent at least $2.8 trillion on counterterrorism-related efforts,[95] and, in the judgment of the Brookings Institution's Michael O'Hanlon, "stopped looking for an exit from the Middle East."[96]
- Compelling the United States to Adopt a Reactive Foreign Policy: Despite confronting formidable challenges at home and abroad, Xi Jinping's China has proven masterful at conveying an aura of inexorability around its resurgence—and, it appears, at unnerving the United States. Unfortunately, though, the more Washington tries to match Beijing's flurry of activity—whether the Belt and Road Initiative (BRI) or "Made in China 2025"—the more it will compete on the latter's terms, potentially discounting its unique strategic assets in the process and adopting a zero-sum approach to bilateral relations.
- Inflaming Divisions Between Americans: Russia's interference in the 2016 presidential election demonstrates its desire and ability to amplify America's existing societal tensions. Its conduct follows the guidance of General Valery Gerasimov, who concluded in early 2013 that "nonmilitary means of achieving political and strategic goals" had increasingly "exceeded the power of force of weapons in their effectiveness."[97] If Americans determine that their country is under siege from within and become preoccupied with internecine ideological strife, they will find it hard to meet the challenges of an increasingly chaotic and contested external environment.

[92] The views expressed in this submission are solely those of Mr. Wyne; they do not reflect those of the RAND Corporation or any of its other employees.
[93] http://www.washingtonpost.com/wp-dyn/articles/A16971-2004Nov1.html
[94] https://www.9-11commission.gov/report/911Report.pdf
[95] https://www.stimson.org/content/counterterrorism-spending-protecting-america-while-promoting-efficiencies-and-accountability
[96] https://www.wsj.com/articles/resigned-to-endless-war-1532706551
[97] https://warontherocks.com/2018/05/warfare-as-violent-politics-an-integrated-framework-for-analyzing-armed-threats/

Subject Matter Expert Biographies

Bogdan Belei

Research Associate, Belfer Center for Science and International Affairs (Harvard University)
17 March 2019

Bogdan Belei is a Research Associate at Harvard Kennedy School's Belfer Center for Science and International Affairs, where he works with Belfer Center Director and former Secretary of Defense Ash Carter. His work focuses on U.S. foreign policy, international security, technology and innovation. Prior to joining the Belfer Center, Bogdan was a James C. Gaither Junior Fellow at the Carnegie Endowment for International Peace. He has previously worked at the Center for New American Security and the Council on Foreign Relations. Bogdan graduated with high honors from the University of Michigan, with a double major Bachelor's Degree in Political Science and History.

Lieutenant Colonel Jeffrey Biller

Military Professor, Stockton Center for International Law (US Naval War College)

Lieutenant Colonel Jeffrey Biller is an active duty Air Force Judge Advocate assigned as a Military Professor at the United States Naval War College in the Stockton Center for International Law. The Stockton Center is the world's premier research institute for the study of international law and military operations throughout the domains of the land, sea, aerospace and cyberspace. His previous Air Force positions include assignment as the Staff Judge Advocate for the Air Force's two operational cyberspace wings and the Deputy Staff Judge Advocate for the Air Force Intelligence, Surveillance and Reconnaissance Agency. Prior to service as a Judge Advocate, Lieutenant Colonel Biller was an Air Force intelligence officer. He received his J.D. from the University of Kansas and has a LL.M. in National Security Law from the George Washington University

Dr. Patricia J. Blocksome

Assistant Professor, National Security Affairs (US Naval War College)

Patricia J. Blocksome is assistant professor in the National Security Affairs department at the Naval War College – Monterey. Her research focuses on special operations, unconventional warfare, rebel group operations and strategy, and hybrid warfare. Concurrently, Dr. Blocksome serves as an adjunct professor at Joint Special Operations University, where she teaches courses on countering violent extremism. She is the vice president for research at the Special Operations Research Association, managing editor of the *Special Operations Journal*, and associate editor of *the Journal of Interdisciplinary Conflict Science*. Prior to joining the Naval War College faculty, she served as assistant professor at the School of Advanced Military Studies in Ft. Leavenworth, Kansas. She is the editor, along with Christopher Marsh and James Kiras, of the forthcoming book *Special Operations: Out of the Shadows*. She has also been published in the *Journal of Human Rights*, *International Political Science Review*, *Special Operations Journal*, *Small Wars Journal*, *CTX Journal*, *Air Commando Journal*, and *Interagency Study*. She received her PhD in Security Studies from Kansas State University.

Dr. David T. Burbach

Associate Professor, National Security Affairs (US Naval War College)

Dr. David T. Burbach is an Associate Professor of National Security Affairs at the U.S. Naval War College in Newport, Rhode Island. Dr. Burbach earned a doctorate in political science from the Massachusetts Institute of Technology, and is a graduate of Pomona College. He has a background in international security and U.S. foreign policy. At the Naval War College, Dr. Burbach has focused on the teaching of national strategy and force planning, regional security in Africa and Europe, and issues with significant technical aspects such as space and cyber. He has published on the future of conflict in Africa as well as the domestic politics of U.S. foreign policy and civil-military relations. Prior to coming to the Naval War College, Dr. Burbach taught at the U.S. Army's School of Advanced Military Studies, and has also worked for the RAND Corporation and several technology start-ups.

Dean Cheng

Senior Research Fellow, Asian Studies Center, Davis Institute for National Security and Foreign Policy (Heritage Foundation)

Dean Cheng brings detailed knowledge of China's military and space capabilities to bear as The Heritage Foundation's research fellow on Chinese political and security affairs. He specializes in China's military and foreign policy, in particular its relationship with the rest of Asia and with the United States. Cheng has written extensively on China's military doctrine, technological implications of its space program and "dual use" issues associated with the communist nation's industrial and scientific infrastructure. He previously worked for 13 years as a senior analyst, first with Science Applications International Corp. (SAIC), the Fortune 500 specialist in defense and homeland security, and then with the China Studies division of the Center for Naval Analyses, the federally funded research institute. Before entering the private sector, Cheng studied China's defense-industrial complex for a congressional agency, the Office of Technology Assessment, as an analyst in the International Security and Space Program. Cheng has appeared on public affairs shows such as *John McLaughlin's One on One* and programs on National Public Radio, CNN International, BBC World Service and International Television News (ITN). He has been interviewed by or provided commentary for publications such as *Time* magazine, *The Washington Post*, *Financial Times*, *Bloomberg News*, *Jane's Defense Weekly*, South Korea's *Chosun Ilbo* and Hong Kong's *South China Morning Post*. Cheng has spoken at the National Space Symposium, National Defense University, the Air Force Academy, Massachusetts Institute of Technology (MIT) and Eisenhower Center for Space and Defense Studies. Cheng earned a bachelor's degree in politics from Princeton University in 1986 and studied for a doctorate at MIT.

Dr. Nicholas J. Cull

Professor, Annenberg School for Communication (University of Southern California)

Nicholas J. Cull is professor of Public Diplomacy at the University of Southern California's Annenberg School for Communication, where he established the prioneering Master's Program in Public Diplomacy. Originally from Britain, he has published widely as a historian of the role of the media in international affairs, including two volumes on the history on the United States Information Agency. His latest book is 'Public Diplomacy: Foundations for Global Engagement in the Digital Age' (Polity, 2019). He is a regular speaker at foreign ministries and diplomatic academies around the world and has acted as a consultant for the UK's Foreign and Commonwealth Office, the Royal Netherlands Foreign Ministry and the Internet Corporation for Assigned Names and Numbers among others. He is currently visiting fellow at the Reuter's Institute for the Study of Journalism at the University of Oxford.

Michael Fabey

Americas Naval Reporter (Jane's Fighting Ships)
US Editor (Jane's Fighting Ships)

Michael Fabey is an award-winning journalist who has more than three decades of experience writing for newspapers, magazines and online news sites. As author of *Crashback*, he gained unparalleled access to the Chinese naval command after 15 years covering the Pentagon. The result is the much-anticipated book about the U.S. and China power clash in the Pacific slated for publication by Scribner (a division of Simon & Schuster) in October 2017. Now the Americas Naval Reporter for *Jane's* and the US Editor for *Jane's Fighting Ships*, Fabey has reported on military matters throughout his career, writing for such publications as *Aviation Week*, *Defense News* and *Janes*. As a foreign correspondent, he worked in newsrooms around the globe for *The Economist Group*, *O. Estado de S. Paulo* and a variety of other publications.

Dr. Michael W. Fowler

Associate Professor, Department of Military and Strategic Studies (US Air Force Academy)

Michael W. Fowler is an Associate Professor, Department of Military & Strategic Studies (MSS), United States Air Force Academy, Colorado. Mike retired from active duty Air Force in 2018. During his service, he was commissioned through the USAF Academy in 1993 and served in operations, intelligence, knowledge management, acquisition, command & control, and headquarters staff positions throughout the United States, Europe, and the Middle East. In 2011, he deployed to Combined Forces Air Component Command Unified Protector where he served as the deputy director for intelligence and the senior US intelligence officer. Mike holds a B.S. in History from the USAF Academy, an M.B.A. in Finance from Western International University, an M.S. in International Relations from Troy State University, and a Ph.D. in Security Studies from the Naval Postgraduate School. He lectures and publishes in the fields of security, strategy, logistics, intelligence studies, and political development. His current research projects involve strategic influence, unmanned aerial vehicles, and strategic planning.

Peter E. Harrell

Adjunct Senior Fellow (Center for a New American Security)

Peter Harrell is an adjunct senior fellow at the Center for a New American Security, where he focuses on the intersection of economics and national security. Research interests include economic statecraft, sanctions and energy. From 2012-2014, Mr. Harrell served as the Deputy Assistant Secretary for Counter Threat Finance and Sanctions in the State Department's Bureau of Economic and Business Affairs. In that role, Harrell was instrumental in developing the international sanctions against Iran, Russia, and Syria, and in the easing of sanctions on Myanmar. He also played a leading role in the U.S. government's efforts to counter terrorist financing, including work to combat the financing of the Islamic State (ISIL). Mr. Harrell served on the State Department's Policy Planning Staff from March 2009 to June 2012, where he played a leading role in developing Secretary of State Hillary Clinton's economic statecraft agenda. He also worked on a variety of other trade and economic issues, with a particular interest in Asia, and authored and edited sections of the State Department's first-ever Quadrennial Diplomacy and Development Review (QDDR). Before joining the State Department, Mr. Harrell served on President Barack Obama's 2008 campaign. He previously worked as a reporter for Congressional Quarterly in Washington, D.C., and is the author of one book, Rwanda's Gamble: Gacaca and a New Model of Transitional Justice. Mr. Harrell is a magna cum laude graduate of Princeton University and holds a J.D. from the Yale Law School. He is originally from Atlanta, Georgia.

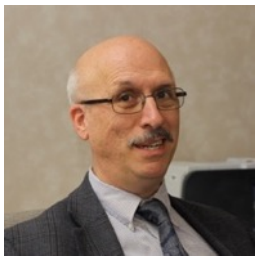
Dr. Peter Layton

Visiting Fellow, Griffith Asia Institute (Griffith University)

Peter Layton is a Visiting Fellow at the Griffith Asia Institute, Griffith University and a RAAF Reserve Group Captain. He has extensive aviation and defence experience and, for his work at the Pentagon on force structure matters, was awarded the US Secretary of Defense's Exceptional Public Service Medal. He has a doctorate from the University of New South Wales on grand strategy and has taught on the topic at the Eisenhower College, US National Defense University. For his academic studies, he was awarded a Fellowship to the European University Institute, Fiesole, Italy. His research interests include grand strategy, national security policies particularly relating to middle powers, defence force structure concepts and the impacts of emerging technology. He contributes regularly to the public policy debate on defence and foreign affairs issues and is the author of the book *Grand Strategy*.

Dr. Martin Libicki

Keyser Chair of Cybersecurity Studies (US Naval Academy)



Martin Libicki (Ph.D., U.C. Berkeley 1978) holds the Keyser Chair of cybersecurity studies at the U.S. Naval Academy. In addition to teaching, he carries out research in cyberwar and the general impact of information technology on domestic and national security. He is the author of a 2016 textbook on cyberwar, Cyberspace in Peace and War, as well as two others commercially published books, Conquest in Cyberspace: National Security and Information Warfare, and Information Technology Standards: Quest for the Common Byte). He is also the author of numerous RAND monographs, notably Defender's Dilemma, Brandishing Cyberattack Capabilities, Crisis and Escalation in Cyberspace, Global Demographic Change and its Implications for Military Power, Cyberdeterrence and Cyberwar, How Insurgencies End (with Ben Connable), and How Terrorist Groups End (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO. Dr. Libicki has numerous publications, his most recent book is "Cyberspace in Peace and War" and two papers being published on: 1) The Convergence of Information Warfare and 2) Second Acts in Cyberspace.

Dr. Julia Macdonald

Assistant Professor, Josef Korbel School of International Studies (University of Denver)

Dr. Julia Macdonald is an Assistant Professor at the Josef Korbel School of International Studies, University of Denver, where her research focuses on state threat assessments, use of force decisions, and U.S. military strategy and effectiveness. Her recent work has appeared, or is forthcoming, in Security Studies, the Journal of Conflict Resolution, Journal of Strategic Studies, Foreign Policy Analysis, Armed Forces and Society, and online at a range of policy outlets. She has held fellowships at the University of Pennsylvania's Perry World House, Harvard's Belfer Center for Science and International Affairs, and she was a Stanton Nuclear Security fellow in the Security Studies Program at MIT. Previously, she worked for the New Zealand Ministry of Defense and the RAND Corporation in Washington D.C. She holds a Ph.D. in Political Science from the George Washington University, an M.A. (Hons) in International Relations from the University of Chicago, and a B.A. (Hons) from the University of Canterbury, New Zealand.

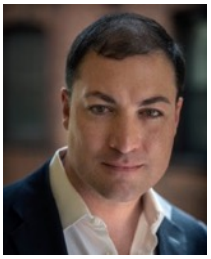
Dr. Jahara Matisek

Major (US Air Force)
Assistant Professor, Military and Strategic Studies Department (US Air Force Academy)
Non-Resident Fellow, Modern War Institute (US Military Academy)

Jahara "Franky" Matisek is an active duty officer in the US Air Force, currently serving as an Assistant Professor in the Department of Military and Strategic Studies at the US Air Force Academy and a Non-Resident Fellow with the Modern War Institute at West Point, US Military Academy. He is a former C-17 Pilot with over 2,000 hours of flight time, to include over 700 hours of combat time, and was a T-6 Instructor Pilot at the prestigious Euro-NATO Joint Jet Pilot program. Franky has a BS from the United States Air Force Academy, an MPA from the University of Oklahoma, an MS from Troy University, and a Graduate Certificate in African Studies and PhD in Political Science from Northwestern University. His current research projects explore the impact of technology on future warfare, security force assistance, hybrid warfare, and the way weak states create effective militaries. He is a contributing editor at *Over the Horizon: Multi-Domain Operations & Strategies* and has published in the *Joint Force Quarterly*, *Georgetown Journal of International Affairs*, *Journal of Strategic Studies*, *Defense & Security Analysis*, *Small Wars Journal*, *Civil Wars*, *The Strategy Bridge*, *The National Interest*, *African Security*, and many other outlets on the topic of military affairs.

Dr. Sean McFate

Professor (National Defense University)



Dr. Sean McFate is an author, novelist and foreign policy expert. He is a professor of strategy at the National Defense University and Georgetown University's School of Foreign Service in Washington, DC. Additionally, he is an Advisor to Oxford University's Centre for Technology and Global Affairs. A specialist in national security strategy, McFate was a think tank scholar at the RAND Corporation, Atlantic Council, Bipartisan Policy Center, and New America Foundation. Recently, he was a visiting Scholar at Oxford University's Changing Character of War Program, where he conducted research on future war. McFate's career began as a paratrooper and officer in the U.S. Army's storied 82nd Airborne Division. He served under Stan McChrystal and David Petraeus, and graduated from elite training programs, such as Jungle Warfare School in Panama. He was also a Jump Master. McFate then became a private military contractor. Among his many experiences, he dealt with warlords, raised armies for U.S. interest, rode with armed groups in the Sahara, conducted strategic reconnaissance for oil companies, transacted arms deals in Eastern Europe, and helped prevent an impending genocide in the Rwanda region. In the world of international business, McFate was a Vice President at TD International, a boutique political risk consulting firm with offices in Washington, Houston, Singapore and Zurich. Additionally, he was a manager at DynCorp International, a consultant at BearingPoint (now Deloitte Consulting) and an associate at Booz Allen Hamilton. McFate's newest book is *The New Rules of War: Victory in the Age of Durable Disorder* (William Morrow). Admiral Jim Stavridis (retired), the former NATO Supreme Allied Commander, said: "Stunning. Sean McFate is a new Sun Tzu." McFate also authored *The Modern Mercenary: Private Armies and What They Mean for World Order* (Oxford University Press) which explains how the privatization of war is changing warfare. The Economist called it a "fascinating and disturbing book." McFate also write fiction based on his military experiences. He co-authored the novels *Shadow War* and *Deep Black* (William Morrow), part of the Tom Locke series. *New York Times* #1 bestselling author Mark Greaney said: "I was blown away…. simply one of the most entertaining and intriguing books I've read in quite some time." A coveted speaker, McFate has appeared before the British House of Commons, top universities and popular audience venues. He has written for the *New York Times*, *Washington Post*, *The Atlantic*, *The New Republic*, *Foreign Policy*, *Politico*, *Daily Beast*, *CNBC*, *Vice Magazine*, *Aeon*, *War on the Rocks*, *Military Review* and *African Affairs*. He has appeared on CNN's *Amanpour*, MSNBC's *Morning Joe*, *Fox and Friends*, NPR, BBC, *Economist*, Vice/HBO, The Discovery Channel, and American Heroes Channel. As a scholar, he has authored eight book chapters in edited academic volumes and published a monograph for the U.S. Army War College on how to raise foreign armies. McFate holds a BA from Brown University, MPP from the Harvard Kennedy School of Government, and a Ph.D. in international relations from the London School of Economics and Political Science (LSE).

Dr. Lukas Milevski

Assistant Professor (Leiden University)

Lukas Milevski teaches strategy, grand strategy and war-related topics as a tenured Assistant Professor, Program in International Relations, Institute of History at Leiden University (Netherlands). His core competence is strategic theory, studied under Colin S. Gray, and his research interests include all aspects of military strategy in concept, history, and contemporary analysis, for education and policy support. Currently also a Foreign Policy Research Institute Baltic Sea Fellow, Milevski has partnered with Oxford University's Changing Character of War Programme for a Sasakawa Peace Foundation project on NATO intra-alliance diplomacy for deterrence, as a Smith Richardson Strategy and Policy Fellow on Baltic defense, and as a Visiting Research Fellow on Anglo-American grand strategy. Milevski has spoken at the US National Defense University, Naval War College, and Military Academy; UK Defence Academy; Military Academy of Lithuania; as well as many academic and professional venues. Major publications include *The Evolution of Modern Grand Strategic Thought* (OUP, 2016), *The West's East: Contemporary Baltic Defense in Strategic Perspective* (OUP, 2018), and *Grand Strategy is Attrition: The Logic of Integrating Various Forms of Power in Conflict* (US Army War College Press, 2019), plus over 40 journal articles in peer and non-peer reviewed sources. The national defence colleges or national universities of the US, UK, Canada, Australia, Singapore, and the Baltic, as well as private institutions such as King's College London/War Studies include his works in their syllabi. Besides his direct interest in his subject, Milevski aspires to leave the field of strategy in a stronger position than when he entered it.

Robert Morgus

Senior Policy Analyst, Cyber Security Initiative and International Security Program (New America)

Robert Morgus is a senior policy analyst with New America's Cybersecurity Initiative and International Security program and the deputy director of the FIU-New America C2B Partnership. His current research focuses on mechanisms to counter the spread of offensive cyber capability, cybersecurity and international governance, and Russian internet doctrine. In the past, he has authored reports on international cybersecurity norms, internet governance, cybersecurity insurance, amongst others. Morgus has spoken about cybersecurity at a number of international forums including NATO's CyCon, the Global Conference on Cyberspace at The Hague, and Cy Fy 2015 in New Delhi, India. His research has been published and recognized by the *New York Times*, *Slate*, the IEEE, peer-reviewed academic journals, and numerous other national and international media outlets. Morgus serves as a member of the Research Advisory Network for the Global Commission on Internet Governance, as well as the Global Forum on Cyber Expertise, and has served as an expert advisor for the World Economic Forum. Before joining New America, Morgus provided research and logistical assistance for a variety of organizations ranging from sustainable development firms to political action committees. Morgus received his BA with honors in diplomacy and world affairs from Occidental College in Los Angeles in 2013 where he focused on international security. While at Occidental, he was the recipient of the Young Fund Student Grant to conduct research on ethno-nationalism in Bosnia and Herzegovina, Croatia, and Serbia. His capstone thesis "Economic Shocks as a Catalyst for Instability: Conditions and Transmission Channels" was one of six honored by the college. He hails from Idaho.

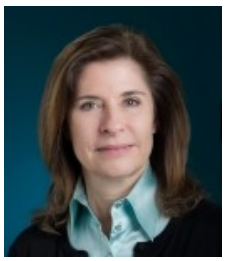
Dr. Christopher Paul

Senior Social Scientist (RAND Corporation)

Dr. Christopher Paul is a Senior Social Scientist at the RAND Corporation, where he is the principal investigator for a number of defense and security related research projects. He also teaches at Carnegie Mellon University and in the Pardee RAND Graduate School. Prior to joining RAND full-time in July of 2002, he worked at RAND as adjunct staff for six years. He spent academic year 2001-02 on the UCLA statistics faculty. During the course of his more than two decades in policy and defense research, Paul has developed methodological competencies in comparative historical and case study approaches, quantitative analysis, and evaluation research. His current and recent research efforts include analyses supporting operations in the information environment, security cooperation, counterinsurgency, irregular/unconventional warfare, and operations in cyberspace. Paul has authored or co-authored dozens of RAND reports and journal articles. Recent RAND reports include RR-1925/1-A, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*, RR-1166-1, *Dominating Duffer's Domain: Lessons for the U.S. Marine Corps Information Operations Practitioner*, RR-1742, *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*, PE-198, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, RR-809/1 *Assessing and Evaluating Department of Defense Efforts to Inform, Influence, and Persuade: Desk Reference*, and RR-1600-A, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*. Commercial books include *Strategic Communication: Origins, Concepts, and Current Debates*, and *Information Operations – Doctrine and Practice: A Reference Handbook*. Paul has spoken, presented, taught, testified, or lectured before the House Armed Services Committee, for NATO audiences, to defense audiences in Singapore, the United Kingdom, Australia, New Zealand, Poland, and the Netherlands, at the National Defense University, at the Naval Postgraduate School, at the Army War College, at the Naval War College, at the School of Advanced Military Studies – Army Command and General Staff College, at AETC Air Command and Staff College, at the Center for Army Analysis, at the USA/USMC COIN Center, at the Air Force Special Operations School, and at the State Department's Foreign Service Institute, and at the LeMay Center, among others. Paul holds a PhD, MA, and BA in sociology, all from the University of California at Los Angeles.

Linda Robinson

Senior Researcher (RAND Corporation)



Linda Robinson is a senior researcher at the RAND Corporation and award-winning book author. Her research spans whole-of-government strategy, low-intensity conflict and post-conflict stabilization. Recent studies address political warfare by and non-state actors, ISIS, and special operations forces. She has conducted extensive field work in the Middle East, South Asia, the Philippines and Latin America and testified before the U.S. Congress. She received a RAND Gold Medal for *Making Victory Count After Defeating ISIS: Stabilization Challenges in Mosul and Beyond,* and a Bronze Medal for *Lessons from 13 Years of War.* Other publications include a Council on Foreign Relations special report on the future of special operations forces (2013) and best-selling trade books including: *One Hundred Victories: Special Ops and the Future of American Warfare* (2013); *Tell Me How This Ends: General David Petraeus and the Search for a Way Out of Iraq* (2008), *Masters of Chaos: The Secret History of the Special Forces* (2004). Robinson graduated summa cum laude from Swarthmore College and was a Nieman Fellow at Harvard University. She received the Outstanding Civilian Service Medal for her tenure as chair of the U.S. Army War College Board of Visitors and numerous awards during her journalism career, including the Gerald R. Ford Prize for Reporting on National Defense and the Maria Moors Cabot Prize from Columbia University. She is a life member of the Council on Foreign Relations.

Dr. Jaganath Sankaran

Assistant Professor (University of Texas at Austin)

Dr. Sankaran works on problems that lie at the intersection of international security and science & technology. Sankaran spent the first four years of his career as a defense scientist with the Indian Missile R&D establishment. His work in weapons design and development led to his interests in matters such as the balance of military power, strategic stability, and arms control. Sankaran received his Ph.D. (in international security Policy) in 2012, writing his dissertation on the role of deterrence, dissuasion, denial and arms control in preserving peace and stability in outer space. The current focus of Sankaran's research is Asia-Pacific. Sankaran studies the growing military and nuclear weapons capabilities of China and the counter military balancing undertaken by the United States, Japan, India and other states. Sankaran has also worked on U.S.-Russia strategic stability and nuclear arms control. Sankaran has held fellowships at the Los Alamos National Laboratory, the Belfer Center for Science and International Affairs, Harvard University and at RAND Corporation. Sankaran has published in International Security, Contemporary Security Policy, Strategic Studies Quarterly, Arms Control Today, Bulletin of Atomic Scientists and other outlets. His research has also been published by the RAND Corporation and the Stimson Center.

Dr. Jacquelyn Schneider

Hoover Fellow (Hoover Institution)

Dr. Schneider is a Hoover Fellow at the Hoover Institution, a non-resident fellow at the Naval War College's Cyber and Innovation Policy Institute, and a Senior Policy Advisor to the Cyberspace Solarium Commission. She researches the intersection of technology, national security, and political psychology with a special interest in cyber, unmanned technologies, and wargaming. Her work has appeared in a variety of outlets including Security Studies, Journal of Conflict Resolution, Journal of Strategic Studies, Foreign Affairs, Lawfare, War on the Rocks, Washington Post, and Bulletin of the Atomic Scientists. She has a BA from Columbia University, a MA from Arizona State University, and a PhD from George Washington University.

Dr. Peter Schram

Assistant Professor, Department of Political Science (Vanderbilt University)

Peter Schram is am an Assistant Professor at Vanderbilt University's Department of Political Science. His research examines the organizational economics of insurgent groups and the political economy of external support for domestic militant groups. Before Vanderbilt, Peter worked for one year at UCSD's Minerva-sponsored Cross Domain Deterrence Project. He has a Ph.D. in Political Economics from Stanford University's Graduate School of Business, a Masters of Economics from Stanford University, and an AB in Politics from Princeton University.

Dr. Steve S. Sin

Director, Unconventional Weapons and Technology Division (University of Maryland START)

Dr. Steve S. Sin is the Director of the Unconventional Weapons and Technology Division (UWT) of START, where he manages large research projects, explores new avenues for research, and establishes collaborative research relationships. Dr. Sin specializes in a broad range of international security, terrorism, and homeland security challenges. His expertise includes radiological and nuclear (RN) terrorism; illicit trafficking of RN materials; terrorist use of cyber domain; emerging technology; emergency preparedness and management; intelligence/counterintelligence operations, analysis, and exploitation; Northeast Asia regional security; and counter-terrorism training, exercise, and curriculum development. His expertise in Northeast Asia regional security is focused on North Korea, including its nuclear program; cyber capabilities; intelligence apparatus; regime survival; and leadership. His additional regional expertise includes South Korean nuclear program and infrastructure; North South Korea relations; and Korea-Japan-China trilateral relations. Prior to joining START, Dr. Sin was the Senior Research Associate and Section Chief at the National Center for Security & Preparedness (NCSP), a strategic partner with the New York State Division of Homeland Security & Emergency Services (DHSES), headquartered at the State University of New York at Albany (University at Albany). At the NCSP, Dr. Sin directed the organization's Policy, Intelligence, Exercises, and Simulations section responsible for Homeland Security and Terrorism Research Program; led the development, coordination, and delivery of multiple counter-terrorism and emergency response training and exercise programs; and provided direct policy support to New York state homeland security leadership. Dr. Sin's extensive experience also includes a career as a U.S. Army Officer specializing in counterintelligence, counter-terrorism, and political-military affairs in the Asia-Pacific Theater of Operations.

Dr. Robert S. Spalding III

Brigadier General (ret) (US Air Force)

Dr. Rob Spalding is an accomplished innovator in government and a national security policy strategist. He has served in senior positions of strategy and diplomacy within the Defense and State Departments for more than 26 years. He was the chief architect of the framework for national competition in the Trump Administration's widely praised National Security Strategy (NSS), and the Senior Director for Strategy to the President. Dr. Spalding is globally recognized for his knowledge of Chinese economic competition, cyber warfare and political influence, as well as for his ability to forecast global trends and develop innovative solutions. Dr. Spalding's relationship with business leaders, fostered during his time as a Military Fellow at the Council on Foreign Relations, allowed him to recommend pragmatic solutions to complex foreign policy and national security issues, which are driving positive economic outcomes for the nation. Dr. Spalding's groundbreaking work on competition in Secure 5G has reset the global environment for the next phase of cyber security in the information age. Dr. Spalding is a skilled combat leader, promoter of technological advances to achieve improved unit performance, and a seasoned diplomat. Under Dr. Spalding's leadership, the 509th Operations Group—the nation's only B-2 Stealth Bomber unit—experienced unprecedented technological and operational advances. Dr. Spalding's demonstrated acumen for solving complex technological issues to achieve operational success, was demonstrated when he led a low-cost rapid-integration project for a secure global communications capability in the B-2, achieving tremendous results at almost no cost to the government. As commander, he led forces in the air and on the ground in Libya and Iraq. During the UUV Incident of 2016, Dr. Spalding averted a diplomatic crisis by negotiating with the Chinese PLA for the return of the UUV, without the aid of a translator. Dr. Spalding has written extensively on national security matters. He is currently working on a book concerning national competition in the 21st Century. His work has been published in *The Washington Post*, *The Washington Times, Foreign Affairs*, *The American Interest*, *War on the Rocks*, *FedTech Magazine*, *Defense One, The Diplomat,* and other edited volumes. His Air Power Journal article on *America's Two Air Forces* is frequently used in the West Point curriculum. Dr. Spalding is a Senior Fellow at the Hudson Institute and a Life Member of the Council on Foreign Relations. He has lectured globally, including engagements at the Naval War College, National Defense University, Air War College, Columbia University, S. Rajaratnam School of International Studies in Singapore, Johns Hopkins Applied

Physics Laboratory and other Professional Military Educational institutions. Dr. Spalding received his Bachelor of Science and Master of Science degrees in Agricultural Business from California State University, Fresno, and holds a doctorate in economics and mathematics from the University of Missouri, Kansas City. He was a distinguished graduate of the Defense Language Institute in Monterey, and is fluent in Chinese Mandarin.

Nicolas Véron

Senior Fellow (Bruegel and Peterson Institute for International Economics)

Nicolas Véron cofounded Bruegel in Brussels in 2002-05, joined the Peterson Institute for International Economics in Washington DC in 2009, and is currently employed on equal terms by both organizations as a Senior Fellow. His research is primarily about financial systems and financial services policies. He frequently briefs senior economic policy officials in Europe, the United States and Asia, and has testified at parliamentary hearings in the US Senate, European Parliament, and in several European member states. A graduate of France's Ecole Polytechnique and Ecole des Mines, his earlier experience includes senior positions in the French government and private sector in the 1990s and early 2000s. He is also an independent board member of the global derivatives trade repository arm of DTCC, a financial infrastructure company that operates on a non-profit basis. In September 2012, Bloomberg Markets included Véron in its yearly global "50 Most Influential" list with reference to his early advocacy of European banking union, a topic on which he has worked and published near-continuously since 2007.

Valentin Weber

DPhil Candidate (University of Oxford)
Research Affiliate, Centre for Technology and Global Affairs (University of Oxford)

Valentin Weber is a DPhil Candidate in Cyber Security at the Centre for Doctoral Training in Cyber Security and a Research Affiliate with the Centre for Technology and Global Affairs, University of Oxford. Previously, he was an Open Technology Fund Senior Fellow in Information Controls at the Berkman Klein Center for Internet & Society, Harvard University. He also worked for think tanks, embassies and international organizations in Paris, London, and Sarajevo.

Ali Wyne

Policy Analyst (RAND Corporation)

Ali Wyne is a Washington, DC-based policy analyst at the RAND Corporation, a nonresident senior fellow at the Atlantic Council, and a nonresident fellow at the Modern War Institute. He serves as rapporteur for a U.S. National Intelligence Council working group that analyzes trends in world order. Wyne served as a junior fellow at the Carnegie Endowment for International Peace from 2008 to 2009 and as a research assistant at the Belfer Center for Science and International Affairs from 2009 to 2012. From January to July 2013 he worked on a team that prepared Samantha Power for her confirmation hearing to be U.S. Ambassador to the United Nations. From 2014 to 2015 he served on RAND's adjunct staff, working with the late Richard Solomon on RAND's *Strategic Rethink* series. Wyne received dual degrees in management science and political science from MIT (2008) and earned his Masters in Public Policy from the Harvard Kennedy School (2017). While at the Kennedy School he served on a Hillary for America working group on U.S. policy toward Asia. Wyne is a coauthor of *Lee Kuan Yew: The Grand Master's Insights on China, the United States, and the World* (2013) and a contributing author to *Power Relations in the Twenty-First Century: Mapping a Multipolar*

World? (2017) and the *Routledge Handbook of Public Diplomacy* (2008). Wyne is a term member of the Council on Foreign Relations, a David Rockefeller fellow with the Trilateral Commission, and a security fellow with the Truman National Security Project.

Author Biography

George Popp

Senior Analyst (NSI, Inc.)

George Popp is a Senior Analyst at NSI, Inc. where he conducts research and analysis on a broad range of multidisciplinary analysis projects that focus on understanding the political, economic, and social dynamics of emerging conflict situations and environments throughout the world. The bulk of George's work has been in support of NSI's government initiatives, particularly leading and contributing to human behavior analytics efforts completed for the Strategic Multilayer Assessment (SMA) program on behalf of the Joint Chiefs of Staff and in support of direct requests from US Combatant Commanders to the Department of Defense. George has also supported NSI's commercial initiatives, conducting business intelligence analyses for clients in the video game industry. George's degree is in Economics from the University of Massachusetts, Amherst.