A Virtual Think Tank (ViTTa®) Report

September 2019

The Character of Global Competition and Conflict, 2019-2029

Deeper Analyses
Clarifying Insights
Better Decisions

NSIteam.com

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

Author

Dr. Allison Astorino-Courtois

Editor

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: RAND Corporation (2019). https://wwwassets.rand.org/content/rand/blog/2019/02/the-need-to-think-more-clearly-about-great-power-competition/jcr:content/par/blogpost.aspectcrop.868x455.rt.jpg/x1551222588985.jpg.pagespeed.ic.Q3dXhQ6-0I.jpg

Table of Contents

Question of Focus

[Q1] How will the character of global competition and conflict change over the next decade, and which emerging global trends and conditions will drive this change? What are the implications of expected future global conditions for developing integrated US strategy and plans to defend US interests over both short- and long-term timeframes?

Subject Matter Expert Contributors

Dr. Gawdat Bahgat (National Defense 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), **Dr. Ryan Burke** (US Air Force Academy), **Dean Cheng** (Heritage Foundation), **Dr. Nicholas J. Cull** (University of Southern California), **Dr. Michael W. Fowler** (US Air Force Academy), **David C. Gompert** (US Naval Academy), **Dr. Barry B. Hughes** (University of Denver), **Dr. Dr. Molly M. Jahn** (University of Wisconsin-Madison), **Dr. Buddhika Jayamaha** (US Air Force Academy), **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), **Linda Robinson** (RAND Corporation), **Dr. Jacquelyn Schneider** (Hoover Institution), **Dr. Peter Schram** (Vanderbilt University), **Dr. Robert S. Spalding III** (US Air Force), **Nicolas Véron** (Bruegel and Peterson Institute for International Economics), **Valentin Weber** (University of Oxford), **Dr. William C. Wohlforth** (Dartmouth College), **Ali Wyne** (RAND Corporation), **Dr. Jen Ziemke** (John Carroll University)

Summary Overview

This summary overview reflects on the insightful responses of twenty-eight 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 how the character of global competition and conflict will change over the next decade, and the implications of those changes on United States policy and planning.

The Character of Global Competition and Conflict

Contributors generally argue that the changes in the character of global competition and conflict we see today will continue, and likely accelerate, over the next ten years. The changes contributors mention most frequently fall into three categories:

- the *domains* in which they expect serious competition and conflict to occur,
- the types of *actors* they expect to be involved, and
- the *tactics and techniques* that adversaries are most likely to use.

Overall, the contributors suggest that, over the next decade, decision makers and planners should expect an operational environment characterized by increased use of asymmetric, non-kinetic, and non-physical tactics in the cyber and cyber-cognitive domains by a widening set of potential adversaries that includes cyber warriors, private corporations, mercenaries, and political organizations.

Key Domains: Cyber-Cognitive, Political, Economic, and Warfare

A majority of the contributors suggest that technologies such as unmanned and autonomous weapons, robotics, artificial intelligence (AI), and ubiquitous communication will change the global environment. Competition and conflict will shift away from reliance on kinetic weapons and physical destruction, toward greater dependence on virtual and information domains in which non-kinetic, but equally destructive operations, will take place. That is, conflict will occur less frequently in the "traditional" physical domains (e.g., land, sea, air) and more frequently in a non-conventional space at the confluence of the cyber and human cognitive domains. In this space, effective information operations are the most relevant competences. "Political warfare" (i.e., using what are commonly viewed as political or diplomatic levers of power) and the use of economic measures are also identified by contributors as increasingly prevalent means of achieving states' desired international outcomes in this non-conventional space.[1]

Challengers: New Types Added to the Old

Contributors also discuss the types of actors they expect to pose security challenges over the next ten years, many of which are updated versions of the *usual suspects*. Dr. Peter Layton of Griffith University, for example, expects that non-state actors' increasing ability to acquire new, more advanced capabilities, such as precision-guided weapon systems and integrated battle networks, which are today typically thought of as restricted to state actors, will increase their potency as global threats. Similarly, Dr. Patricia Blocksome of the US Naval War College suggests that increasingly inexpensive cyber, space, and robotic technologies will work to the advantage of "weak" states (i.e., those currently discounted as unimportant security challengers), which she believes will also become more potent threats as their ability to conduct devastating attacks without the need of conventional military operations increases.

Other contributors identify *less-usual suspects* (i.e., those currently unlikely to be considered as posing any type of security threat) as potential challengers. For example, Linda Robinson of the RAND Corporation believes non-governmental organizations and civil society groups, such as social clubs and cultural foundations, may be weaponized through Chinese and Russian infiltration. Funding and manipulation of these groups would create

[1] See contributions from Blocksome, Burbach, Robinson, and Spalding III.

deniable means to accomplish aggressive objectives by using local nationals. Dr. Sean McFate of the National Defense University suggests that, in the near future, 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." Finally, Dr. Robert Spalding III of the US Air Force argues that cyber warriors—avatars of live soldiers—might use "their own weapons and networks to create the intended effects."

Tactics and Techniques

The tactics and techniques used by global competitors are also likely to evolve over the next decade. Increasing use of state and non-state proxies by powerful states to conduct conflict with stealth and ambiguous attribution is a tactic commonly highlighted by the contributors. In fact, the team of Dr. Buddhika Jayamaha of the US Air Force Academy, Dr. Jen Ziemke of John Carroll University, and Dr. Molly Jahn of the University of Wisconsin-Madison observe that we have seen the beginning of this trend in Russian (and Chinese) use of proxies to confuse Western abilities to respond to serious challenges. Lieutenant Colonel Jeffrey Biller of the US Naval War College agrees, noting that using proxies to conduct plausibly deniable cyber operations is a good bet for major states, 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."

In addition to an increasing use of proxies by state actors, contributors project that global competition and conflict will include:

- widening use of cyber and information operations,
- use of "blackmail or public discrediting of Western elites" to influence adversary behavior,[2]
- use of economic and political pressure, and
- use of other non-conventional tactics that intentionally circumvent international legal norms and standards.

Layton adds one more to this list: a broad preference among technically advanced states for defensive over offensive strategies. Layton argues that because deployment of AI, robotics, and other technologies upon which modern militaries depend is more easily done from friendly than from hostile areas, defense of friendly territories will become increasingly critical and will constitute a "dominant form of future war."

Drivers of Change

As mentioned, the majority of the contributors reference technological advances as a key driver of the transformation of the current operational environment. Biller offers an additional driver: the failure of the US and its allies to take active leadership in developing international law and standards of behavior around new technologies and capabilities—particularly governance of cyber activities. Unless corrected, Biller argues, today's permissive legal environment will continue to engender an operational space in which democratic states are at a continual disadvantage to centrally-controlled and authoritarian regimes.

Others put much of the blame for the current state of global competition and conflict—particularly regarding US-

[2] See contribution from Burbach.

China-Russia relations—on permissive US policy more generally, stemming from two sources. First, by focusing elsewhere for too long, the US itself has allowed China and Russia to gain advantage, notably in the cyber and cyber-cognitive domains and in information operations. Second, by failing to predict, recognize, and adapt to changes in the operational environment, the US defense establishment has remained focused on the kind of kinetic, conventional warfare that China and Russia will not fight—as Blocksome notes, "only an unintelligent adversary would fight the US in a conventional battle."

Implications for United States Policy and Planning

Dr. Ryan Burke of the US Air Force Academy cautions that "superior technology alone does not win wars." In this vein, interestingly, very few of the contributors' suggestions for managing global competition and conflict include capabilities or weapons systems. Rather, the primary concern contributors discuss relates to how US strategists and decision makers *perceive* the environment. Specifically, the contributors recommend a revision of the assumptions about both US "adversaries" and the nature of warfare that remain embedded in US strategy and operations.

Regarding US "adversaries," there is little room for doubt among the contributors that China's rise is "inevitable"—even if the pace of that rise is not. Several contributors argue, therefore, that US planners and policy makers should adopt a worldview, and develop strategies, that can accommodate the possibility that China is a peer-competitor, or an outright threat, on some issues and in some circumstances, but not on all.[3] The US view of Russia must be similarly discerning; allowing for the possibility that Russia is a weakening state and, although a "rogue" and troublesome threat in the short-term, the challenges it poses to the international system over the long-term will not be as significant as those posed by China.

Regarding ourselves, more broadly, McFate observes that today "our systems, our bureaucracies, our force structure," and even our force acquisition and postures are still determined by a set of (explicit or implicit) assumptions that reflect a traditional, Westphalian view of conflict and warfare.[4] McFate recommends, therefore, a thorough review and update of the US "strategic way of thinking" that is relevant to, and aligned with, the (decidedly non-Westphalian) threat environment and the technologies, actors, and actions that are driving its evolution. Finally, Ali Wyne of the RAND Corporation highlights a key point for those charged with developing US tactics, techniques, and strategies for navigating expected future global conditions: remember that competition (and conflict) are means, but not strategic ends.

[3] See contributions from Bahgat, Cull, Gompert, Hughes, and Véron.
[4] See also the contribution from Wyne.

Subject Matter Expert Contributions

Dr. Gawdat Bahgat

Professor, National Security Affairs, Near East South Asia Center for Strategic Studies
(National Defense University)
17 February 2019

Competitions and conflicts between nations are likely to move away from traditional wars and instead, take the form of asymmetric warfare, where different techniques will be utilized. These include proxies, cyberattacks, terrorism and economic pressure.

US-Sino relations are complicated. China is NOT our enemy, we have a huge trade volume with Beijing and China sends a large number of students to the United States. China is a competitor, we agree and disagree on certain issues, but stable and growing China is in US best interest.

For different reasons, Russia and President Putin enjoy more creditability in the Middle East than the United States.

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[5]

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.

[5] 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 Johson, 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, the more that any attack on that system could lead to catastrophic failures within that 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.

Dr. Ryan Burke

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

Geography Matters: Key Interests in Future Global Competition and Conflict

If we ask defense hawks this question, some answers will no doubt emphasize the so-called Revolution in Military Affairs (RMA) concept. RMA implies that evolving technology will change the nature and character of war, and that those military powers possessing the most advanced technology will prevail in future military conflicts of the 21st century. While possession of superior technology almost certainly provides advanced military capability, superior technology alone does not win wars. The American efforts in Vietnam, Iraq, and Afghanistan to date are examples of such efforts where superior military force enabled by superior technology was insufficient to combat irregular factions of "freedom fighters" intent on resisting American occupation and western influence. This is not to say that technology is irrelevant or that it won't aid in military victory. It is to say, rather, that reliance on superior technology alone – and the resulting perception of competitive military advantage stemming from such superior technology – is ill-founded and frankly ignorant. The "tech trend" that so many defense advocates stand behind is not the only trend that will drive future change in global competition and conflict. Those lacking superior technology tend to be more adaptable and creative; even the most technologically advanced militaries in the world find themselves – at times – vulnerable to relatively primitive – yet successful – attacks. To utilize modern technology, militaries require – at the very least – bases and infrastructure from which to employ it. The nature and character of future conflict will be influenced just as much by geography as it will be technology. In this way, military powers with the greatest global influence, regardless of their technology, will be most likely to shape global competition and resulting conflict far into the 21st century.

To support this claim, look no further than the Chinese effort to expand their territorial claims in the South and East China Seas. Though historically contested for centuries, the South China Sea has seen a sharp rise in tensions since 2010. Since their renewed territorial claims in 2013, the Chinese have annexed existing land masses and reefs in the SCS and ECS while simultaneously constructing approximately 3200 acres of artificial islands in the same areas.[6] Why? Depending on one's source, over 30% of global maritime trade flows through this highly-trafficked economic trade zone; and over 60% of regional Asia-Pacific trade traverses these contested waters.[7] With control – or at least geographic influence – of such critical waters to the global economy, Chinese land and power grab efforts in this area should come as no surprise to those familiar with the international security landscape. But regional and economic influence in the SCS and ECS alone are wholly insufficient for a nation in China that – arguably – seeks to supplant the United States as the global hegemon. Given this, it should also come as no surprise that the Chinese are actively seeking to expand their prepositioned military presence beyond the Asia-Pacific.

The Chinese government has been engaged in diplomatic efforts with Nicaragua and Venezuela in recent years. Reports suggest Chinese influence and private funding of the now halted Nicaraguan Canal project, as the Chinese are reported to be militarily interested in controlling this potential maritime throughway.[8] More recently, the Chinese government has refused – unlike most global leaders – to denounce Nicolas Maduro's contested reelection as President of Venezuela and even blocked a United Nations Security Council resolution to institute new elections.[9] Venezuela's massive oil reserves and prime location at the extreme northern portion of the South American continent combined with its failing economy make it a target of opportunity and exploitation for a Chinese government seeking to expand its influence into the Americas. With a booming Chinese economy and a failing Venezuelan economy, President Xi and China can serve as Maduro's and Venezuela's savior – in exchange – potentially – for future basing and infrastructure rights of operation. With the Chinese Navy's ongoing efforts to both modernize and expand their naval capabilities and compete with the United States for regional influence, the northern coast of Venezuela seems like a pr location for China's newest strategic prepositioning effort.

---

[6] Specia, Megan and Takkunen, Mikko, "South China Sea Photos Suggest a Military Building Spree by Beijing." February 8, 2018. https://www.nytimes.com/2018/02/08/world/asia/south-china-seas-photos.html

[7] Team, China Power. "How much trade transits the South China Sea?" Center for Strategic and International Studies, Washington DC (2017). https://chinapower.csis.org/much-trade-transits-south-china-sea/

[8] Shaer, Matthew. "A new canal through Central America could have devastating consequences." Smithsonian. com, December (2014). https://www.smithsonianmag.com/science-nature/new-canal-through-central-america-could-have-devastating-consequences-180953394/

[9] Wainer, David, "Russia, China Veto UN Resolution Seeking Venezuela Elections," February (2019). https://www.bloomberg.com/news/articles/2019-02-28/russia-china-veto-un-resolution-seeking-venezuela-elections

But China isn't the only big power adversary seeking to expand its geographic influence. Russia – like China – refuses to condemn, denounce, or delegitimize Nicolas Maduro's retention of his office, despite mounting pressure from major international powers like the United States.[10] Russia is also interested in south and Central American basing infrastructure. Reports suggest Russian interest and suspected military activity also in Nicaragua.[11] The list of nations with expansionist interests goes on, but suffice to say that China and Russia present the greatest current threat to United States' interest internationally.

Beyond central and South America, nations like China and Russia seem interested in establishing greater presence and influence in the Polar Regions. Climatic variations have objectively changed the polar landscape in the 21st century making these regions – arguably – some of the most strategically imperative areas on the planet for both influence and control. In particular, the Arctic Circle provides a direct avenue of approach for military powers with the capability to exploit dwindling land mass obstructions and to traverse what was once considered an impassable region of the world. The direct approach benefit is one of many such motivations for Arctic expansion. What's more, controlling territory in the Artic may yield tremendous economic benefits via oil and liquid natural gas extraction as the Arctic Circle is thought to be an area rich with such energy sources.[12] We know that the Chinese, as of 2018, have expressed interest in the poles via a "white paper policy" document released by their State Council Information Office.[13] As well, we know Russia's interest in the Arctic Circle is multifaceted given the country's northern border is immediately adjacent to the circle. With Russia's apparent interest in reunifying territories of the old Soviet Union, a northern flanking approach via the Arctic Circle may enable surrounding regional influence on the Scandinavian nations first and the Baltic States by extension. Russia could even use a play from the Chinese playbook and seek to expand territorial claims in the Arctic Circle. Such claims may seem sensational to some but are well within the realm of possibility for a nation-state motivated by global power. Complicating matters is the lack of law governing international water ways. Currently, the United Nations Convention on the Law of the Seas (UNCLOS) is the only document governing maritime conduct in international waters. The problem is that UNCLOS doesn't actually govern and there few real deterrents built into the system to dissuade Russia or China from complying with UNCLOS parameters. In other words, the Arctic is ripe for military expansion. With the United States' lack of emphasis on the Polar Regions and the Americas relative to other areas of the world, these are growing problems requiring reorientation.[14]

Currently, the United States' prepositioned global military presence far exceeds that of any other nation. However, despite the U.S. force postures influencing diplomatic, military, and economic efforts in myriad global hotspots, the U.S. sorely lacks geographic influence in both the Poles and the Americas. United States Southern Command headquarters is in Doral, Florida and not even in the true Southern Command area of responsibility. The United States military has a small forward expeditionary base in Honduras acting as the lead element in the U.S. military's efforts to counter transnational crime among other efforts.[15] Soto Cano Air Base is the home of Joint Task Force-Bravo, a small forward military presence that, despite documented Central American expansion efforts by both China and Russia, sees little emphasis from DoD relative to other geographic combatant command priorities. This and small operating elements of Army and Marine Corps special operations units in Colombia and other countries make up the entirety of the U.S. SOUTHCOM defense posture. With Venezuela soon to be a failed-state ripe for Chinese and Russian exploitation, coupled with Chinese and Russian expansion in Central America, this is insufficient.

As well, U.S force posture is nearly non-existent in the Polar Regions. Marine Forces Pacific maintains the Marine Rotational Force Darwin program that deploys about 1,500 Marines on six-month continuous rotations to Darwin, Australia.[16] While firmly entrenched in the Southern Hemisphere, this rotational force presence is situated on the extreme north-central coast of Australia, still thousands of miles north of the Antarctic continent. It is difficult to influence operations from this distance. Smaller numbers of Marines have in recent years participated in European theater training exercises in Poland, Norway, and the Baltic States as part of BALTOPS and Saber Strike.[17] While

[10] Ibid.
[11] Sanchez, Alejandro, "Forget Venezuela, Russia is Looking to Nicaragua." September (2017). https://nationalinterest.org/feature/forget-venezuela-russia-looking-nicaragua-22464
[12] King, Hobart, "Oil and Natural Gas Resources of the Arctic," n.d., https://geology.com/articles/arctic-oil-and-gas/
[13] English Translation by Lu Hui from *Xinhua*: "China's Arctic Policy: The State Council Information Office of the People's Republic of China," January 2018, http://www.xinhuanet.com/english/2018-01/26/c_136926498.htm
[14] For a more detailed discussion of the proposed military reorientation to the Polar Regions, see Burke and Matisek's (forthcoming 2019) article "The American Polar Pivot: Gaining a Comparative Advantage in Great Power Competition," *Marine Corps University Journal.* 10(1).
[15] United States Southern Command: Joint Task Force-Bravo. https://www.jtfb.southcom.mil/
[16] Marine Forces Pacific: Marine Rotational Force-Darwin. https://www.marforpac.marines.mil/MRFDarwin/
[17] "Exercise BALTOPS 2018 Enhancing Interoperability Among NATO Allies and Partners in Baltic Region.'

Marine rotational forces actively deploy to Australia and or northern Europe as part of training and readiness efforts, Marine Expeditionary Units (MEU) deploy rotationally around the world as well and are far more expeditionary than their Darwinian counterparts. East and West Coast MEUs deploy simultaneously and at any given time can project power in numerous areas of U.S. interests. Deploying more maritime assets in and around the Polar Regions—provided sufficient capability and seasonal conditions to enter or approach arctic waters – is in order as an indication of U.S. interest and commitment to securing the Polar Regions. The U.S. should also consider – in this vein – reorienting carrier strike group and other surface ship package deployments beyond amphibious ready groups (ARG) and MEUs to the Polar Regions in an effort to maximize U.S. presence and military power projection in these regions.[18] Such commitments of visible military force postures to strategically vital regions of the world would speak volumes to Russian and Chinese expansion. There is some discussion on this front as of late 2018 under then-Secretary Mattis' 'dynamic force employment' concept. Such discussions about avoiding unpredictability while integrating newly determined strategic locations is vital to continued global competition.

The U.S. needs a strategic rebalancing effort that extends beyond the INDO-PACOM area of responsibility. As large and sustained combat operations wind down in the CENTCOM AOR, the U.S. must consider its geographic presence in other soon-to-be contested regions, namely the Polar Regions and the Americas. The U.S. no longer enjoys geographic isolation and protection from its 21st century adversaries as it once did. The threats from the Arctic and Central and South America now present legitimate concerns for homeland defense. The U.S. needs to meet these challenges before they arrive at our doorstep. Re-orienting rotational force efforts to expand operations in the Poles and the Americas is a necessary first step that may deter continued Russian and Chinese military expansion in these geographically critical regions of the world that, until now, few people have truly emphasized as areas of global interest in the future of great power completion and conflict.

Dean Cheng

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

Global competition will increasingly involve multiple different areas, beyond the traditional economic, political/diplomatic, and military. It will incorporate advances in technology (reflected in the increasing importance of information and communications technologies), but also in the ever-increasing availability of information and concomitant decline in privacy.

Ideally, the United States should be trying to develop a coherent approach to these various changes, but that is unlikely. However, the more flexible American economy and society may evolve more rapidly, and accommodate these changes more effectively, than the top-down approach preferred by authoritarian systems.

Dr. Nicholas J. Cull

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

My expertise is in the role of 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

https://navylive.dodlive.mil/2018/06/11/exercise-baltops-2018-enhancing-interoperability-among-nato-allies-and-partners-in-baltic-region/; https://www.eur.army.mil/SaberStrike/

[18] Eckstein, Megan, "Navy May Deploy Surface Ships to Arctic This Summer as Shipping Lanes Open Up," January (2019). https://news.usni.org/2019/01/08/navy-may-deploy-surface-ships-arctic-summer-shipping-lanes-open

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 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 they 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 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.

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 focused on producing psychological effects: a combination of exhaustion, denial, and subversion.[19]

The annihilation method of 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 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 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.[20] 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

[19] Michael Fowler, "Ways of War: Constructing a Compellence Strategy," Burke, Fowler, and McCaskey, *Military Strategy, Joint Operations, and Airpower* (DC: Georgetown University Press, 2018).
[20] J. Boone Bartholomees, "The Issue of Attrition," *Parameters* (Spring 2010), 9.

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. 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.[21] 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%.[22] 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.[23] Yet, cooperation via security assistance is now a common element in the strategist's toolbox across a multitude of countries.[24] Security cooperation is increasingly 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

---

[21] 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.

[22] Dyfed Loesche, "The World's Arms Exports," *Statista* (Feb 20, 2017), at: https://www.statista.com/chart/8163/the-worlds-arms-exports/.

[23] Gordon Adams and Shoon Murray, eds., *Mission Creep: The Militarization of US Foreign Policy?* (Washington, DC: Georgetown University Press, 2014).

[24] 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).

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.[25]

David C. Gompert

Distinguished Visiting Professor (US Naval Academy)
Adjunct Professor (Virginia Union University)
Senior Fellow (RAND Corporation)
15 February 2019

Projecting the future ten years out is hazardous duty. But from what we know now about economics, demography and geo-politics, it is not unreasonable to forecast that great power dynamics during the 2020s will boil down to the relationships among the United States, China and Russia. What might throw this forecast off are technology (e.g., AI), health breakthroughs, or climate shocks that could cause rapid and unforeseeable changes. In that vein, India, Japan and EU (sans UK) could play larger roles and affect great-power relations. However, because none of them is likely to become a U.S. adversary, let's stick with China and Russia.

As Jim Dobbins and his RAND colleagues recently explained, China is a peer competitor but not a rogue, whereas Russia is a rogue but not a peer competitor. The difference between them, and between the challenges they pose, is basic: China's leaders, from Deng until now, have taken care to invest wisely in developing a strong, balanced economy, modern infrastructure, vast manufacturing capabilities, and improved living conditions *before* pursuing external ambitions. In contrast, Putin and Co. have pursued Russian external ambitions in the interest of shoring up their domestic power despite a severely imbalanced economy and degraded living conditions in the country at large.[26] This is evident in the way Russia has become increasingly aggressive in the five years since revenue from fossil-fuel production collapsed.[27]

Thus, while China has the wherewithal to achieve its strategic goals, Russian aspirations to great power status and post-Soviet supremacy cannot be supported indefinitely. Moreover, China's external strategy could help fuel further development, whereas Russia's external strategy is a drain. Taking account of not just conduct but also resources, China is a growing power and Russia is, in relative terms, a declining one.

This does not make China more threatening than Russia is to U.S. interests. History shows that declining powers can be dangerous.[28] Indeed, so long as Russian external misbehavior is not constrained by economic weakness but rather is prompted by economic weakness, its current menacing conduct could persist. In contrast, China will likely continue to modulate its external conduct so as not to outpace its internal strength. As a result, Russia is the more dangerous of the two *in the short term.* For now, the challenges China poses to U.S. interests are the more predictable and manageable of the two, but this could change as China gathers more strength. In a nutshell, Russia is today's biggest great-power problem; China is tomorrow's.

Trends in technology, energy and economics are likely to perpetuate this condition. As a major player in technological competition, with growing productivity, and with stable energy costs, China's economy should continue to grow at least 5%/year; and its military capabilities will be increasingly sophisticated and threatening to U.S. forces. In contrast, Russia's extreme dependence on revenue from fossil-fuel production leaves it vulnerable to continuing expansion of world supplies (and stable demand), mainly due to U.S. on-shore

[25] Jahara Matisek, "The crisis of American military assistance: strategic dithering and Fabergé Egg armies," *Defense & Security Analysis* 34, no. 3 (2018): 267-290.
[26] Russia's GDP ranks #12 in the world (after South Korea); the life expectancy of Russians ranks #148 in the world. (Economist). China ranks #2 in GDP, but is tied with the U.S. on a PPP basis. The life expectancy of Chinese (~76) is greater than that of Russians (~70). Russia is tied with Belarus in per capita alcohol consumption.
[27] Russia is, on average, a high-cost producer of petroleum and natural gas; therefore, declining prices mean even greater declines in margins and thus state revenues.
[28] Post-Napoleonic France was considered the greatest threat to Europe and British interests for half a century.

production and OPEC responses to that production. As a secondary player in global technological competition (especially IT) and a non-player in value-added production and trade, Russia must continue to count heavily on (dwindling) state revenues to compete.

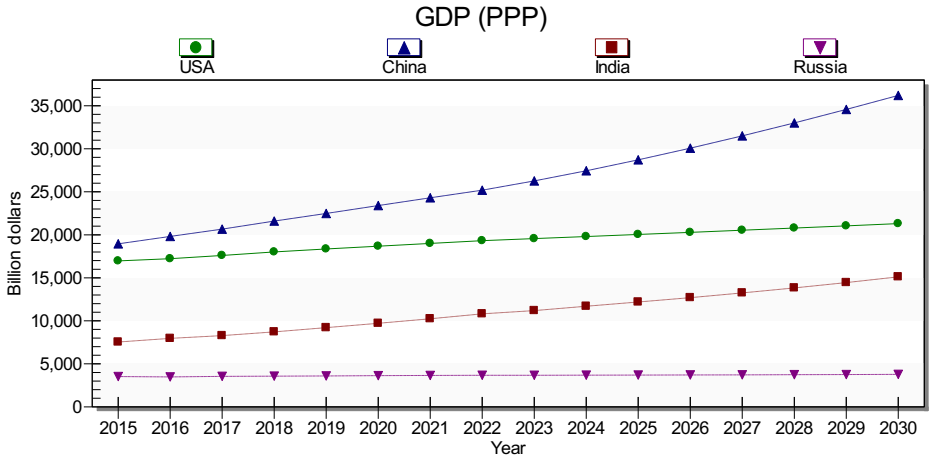
In sum, Russia presents greater dangers to U.S. interests in the short term but, with a fundamentally poor economy, will find it difficult to support a belligerent external strategy, especially if and as the U.S. compels it to pay a high price for that strategy. China has a sustainable external strategy, which is focused mainly on recovering its losses and its preeminence in East Asia. Though its global aspirations are not necessarily problematic, the importance of the region make China the biggest great-power challenge over the next decade.

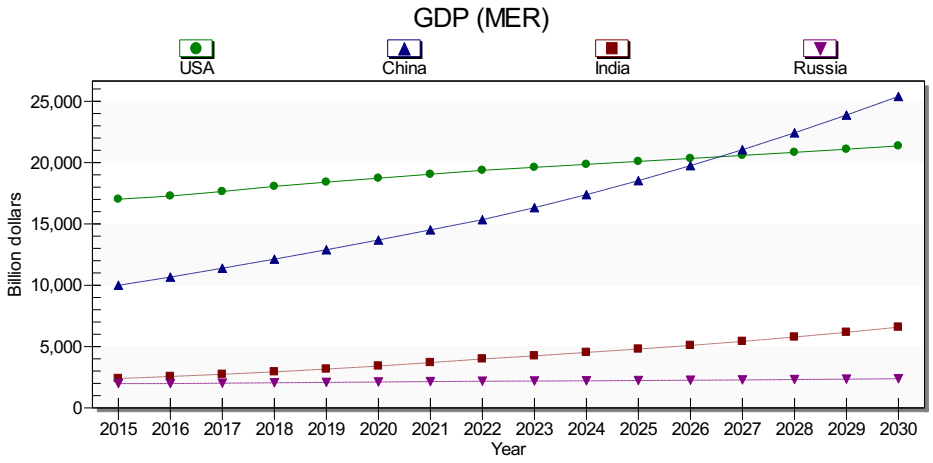
Dr. Barry B. Hughes

John Evans Professor, Josef Korbel School of International Studies (University of Denver)
5 March 2019

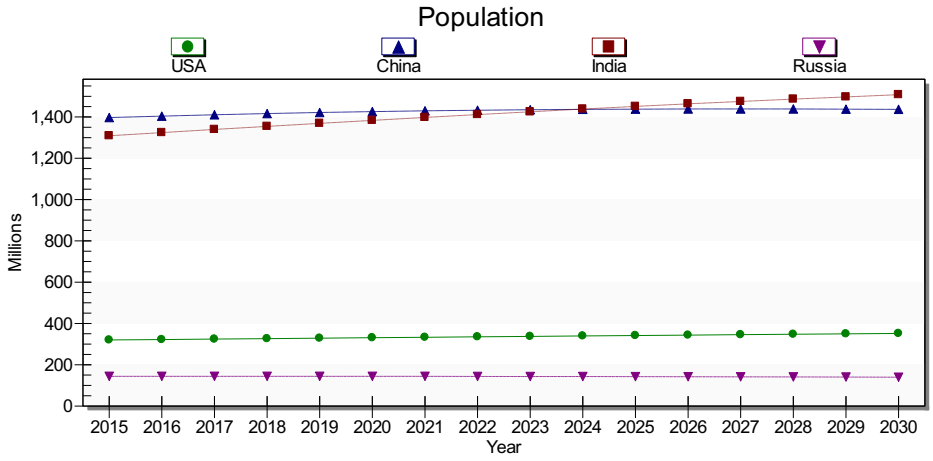
As a basis for strategic thinking, it is useful to bring to bear some numbers concerning the current and prospective operating environment. The following come from the Base Case scenario of the International Futures (IFs) model system at the Frederick S. Pardee Center for International Futures. I look here only at the US, China, India, and Russia, ignoring other highly important contextual elements including the rise of power in countries near China and therefore also the larger ongoing global shift of focus to Asia. One increasingly critical element of that more regional environment, especially just beyond the 2029 horizon, is the ongoing rise of India; hence its inclusion here.

The first two graphics show the movement of China into a prominent global leadership role economically. I agree with the increasing consensus that China has difficult navigation ahead with respect to the continued shift internally away from a heavily state-directed economy (in fact the movement back toward more of that under President/Chairman Xi) and with respect to broad global pushback against an export-oriented and significantly mercantilist country. Nonetheless, even slowing growth will reinforce the lead China already has in GDP measured at Purchasing Power Parity and put it ahead of the US at market exchange rates. The two graphics also show the increasingly diminished role in store for Russia, as its GDP falls to less than half of even India at MER and less than one third at PPP.

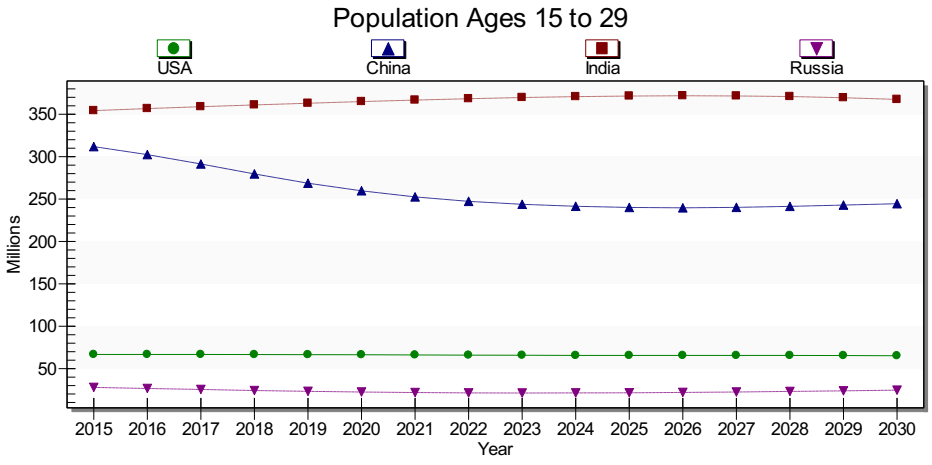




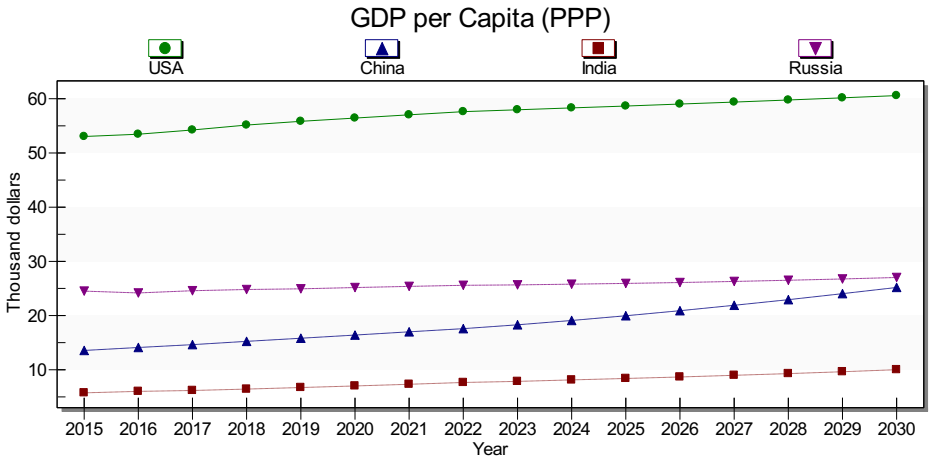
Demographically, we all know the story of India and China relative to any other significant global power.



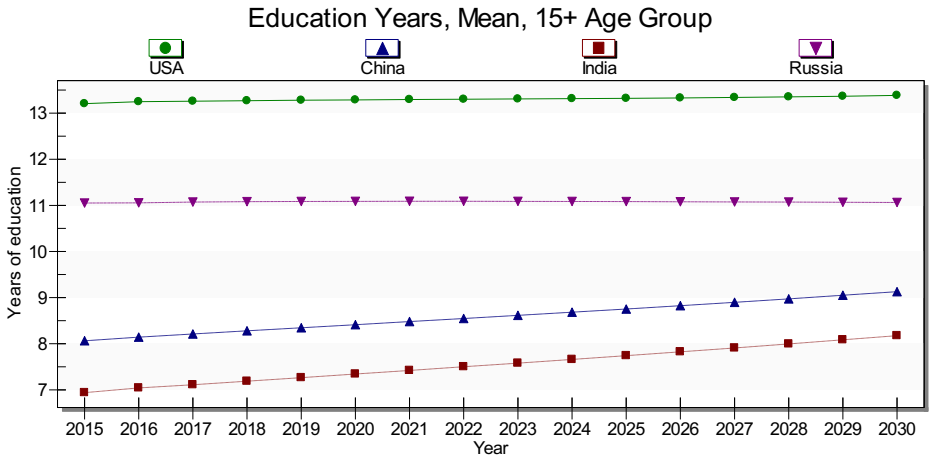
But the graphic below touches also on the important role of demographic structure. The number of military- recruit-aged men is now falling quite rapidly in China (as the numbers of elderly and their need for care by the state given the 4-2-1 cross generational family structure rises quickly), in contrast to other major global powers. Reluctance to send only sons (or daughters) into danger makes the coming years very different from those preceding World Wars I and II in all of these countries, especially China. That alone helps shift the field of competition of other forms of confrontation.

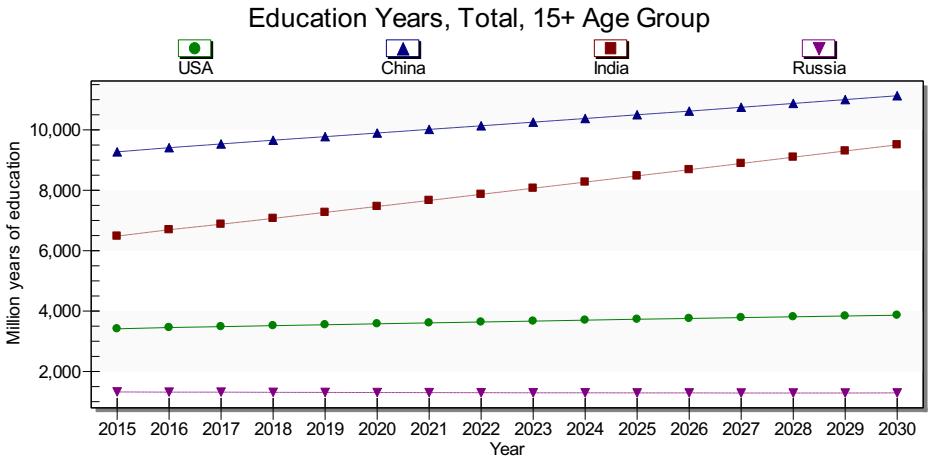


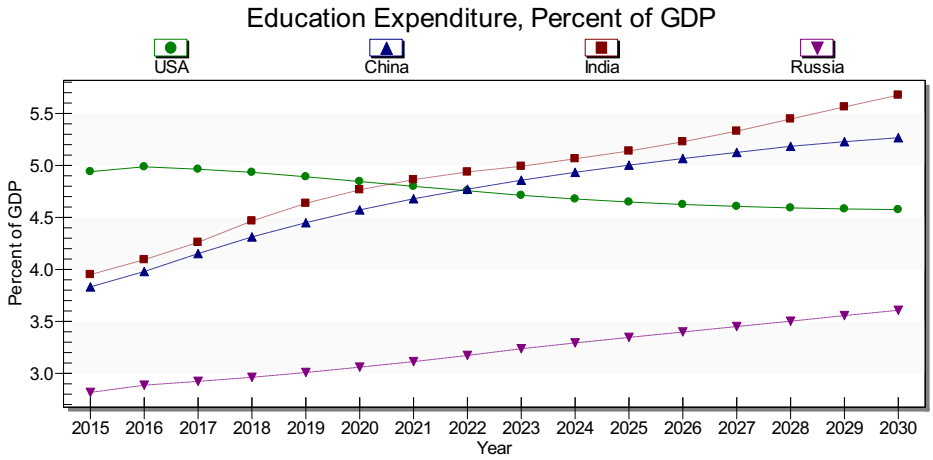
Putting these demographic and economic trends together shows the continued dominance the US will have in GDP per capita (at least at PPP), reinforcing its potential also for technological dominance.



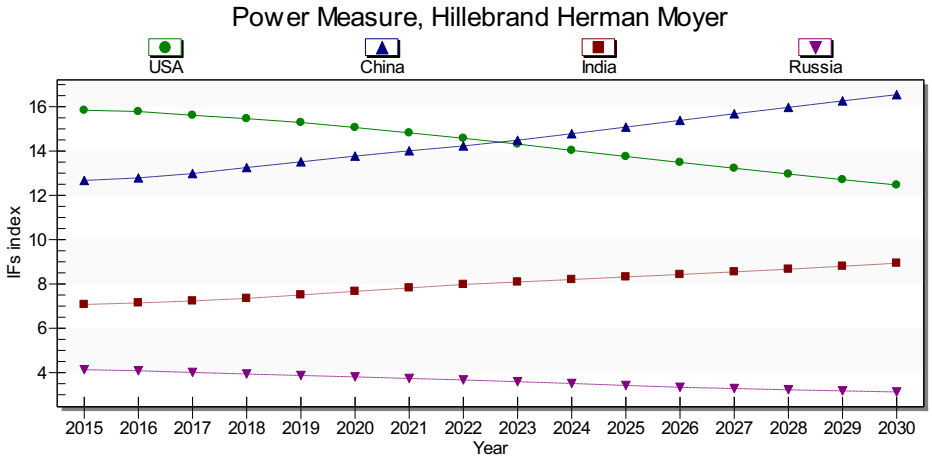
However, patterns around education suggest some of the challenges to that US potential. Immediately below, the graphic shows the *average* years of educational attainment that citizens 15 and older have, and are likely to have, across the country set. China is already nearly at the level of the U.S. as recently as 1960, with all the technological achievements of the country by that decade. Below that is a figure showing the *total* education years accumulated by all adults—not only is the Chinese total already twice that of the US, but the rise of China and India appears unstoppable. Reinforcing that pronounced and rapid shift of intellectual capacity predominance to Asia, the third graphic below shows the portion of GDP each country is directing to education and pattern of change that appears underway. To the degree that quality differences might now exist, those will be evaporating.







All of the above patterns suggest the unstoppable movement of China on the path of its Made in China 2025 drive for technological leadership in a significant range of fields. Putting the population, education, and GDP elements together, the final graphic shows an admittedly somewhat subjective measure of aggregate "power" (but one quite different from the older and outdated, equally weighted summations of economic, demographic and military capabilities). The graphic suggests the magnitude of the underlying shift that may take place in just this historically brief 15-year period. Do not fail to notice not only the crossing of China above the US, but the growing convergence of India toward the US and the already small and shrinking place of Russia in the system.



I leave to others with greater expertise the task of drawing conclusions concerning likely and desirable strategy of the great powers. But a generation ago I taught a university course in China to then early career and now presumably quite well-placed professionals in international politics. I took away two less data-based, more subjective and qualitative perceptions of Chinese thought patterns deeply rooted in history. The first is the pervasive sense of historical injustice at the hands of Western powers, and the second is the equally widespread belief that global politics is fundamentally a matter of power-based realism rather than institution-building liberal internationalism. Unfortunately, the US does not consistently act in a manner that contradicts the contemporary applicability of those understandings and conveys our own recognition that we either need to actively involve China in a full range of cooperative global governance-building activities or it will disrupt and ultimately restructure the current system. While it seems unlikely that China will be able to, or interested in, militarily challenging the US outside of the region across this horizon, more economically and technologically based challenges will inevitably grow. And the desires to dominate regional seas and to reunify with Taiwan seem highly unlikely to diminish with growing regional capacity to act. Finding a path that combines preparedness with constant efforts to increase cooperation across economic, social, and military domains seems an essential strategic foundation.

Dr. Buddhika Jayamaha, Dr. Jen Ziemke, and Dr. Molly M. Jahn

Dr. Buddhika Jayamaha
Assistant Professor, Military and Strategic Studies Department (US Air Force Academy)

Dr. Jen Ziemke
Associate Professor (John Carroll University)

Dr. Molly M. Jahn
Professor (University of Wisconsin-Madison)

5 March 2019

Defending the Realm in an Age of Interstitial Warfare[29]

America continues to reign supreme in the traditional domains of conflict: land, sea and air. As ever, nuclear deterrence holds. Revisionist and regional powers with the hopes of altering the existing order, as well as state-backed or autonomous violent non-state actors, do not directly confront the U.S. and its allies along the traditional, clearly discernible, spectrum of conflict. Instead, they strike at the interstices of traditional domains of power projection and in the interstices of emergent domains.

Power is most formidable at the core areas where the traditional domains of defense – land, sea and air - overlap. Conversely, power is weakest at the seams - where the boundaries of traditional domains of power projection do not perfectly overlap. It is that interstitial space where defenses are stretched and the political will to resist is weakest.

The domain of cyber and the domain of civil society offer two examples of interstitial spaces with an enormous and vulnerable attack surface with inadequate defenses. Cyber is a highly dynamic, evolving domain, where the frontier keeps moving at a relentless clip. Civil society in liberal democracies was always a domain relevant to adversarial information operations but is of increased import in recent years.

Interstitial Attrition

America and its allies small and large are ready to crush the Visigoths if they dare to crash the gates. And rightly so. Maintaining formidable traditional defenses is necessary, and its desirability is reflected in why the smaller states, such as the Baltic nations, and soon Macedonia, wish to join NATO.

[29] This paper consolidates the insights of a longer work forthcoming by Major Jahara Franky Matisek, PhD., Lt Colonel Travis Robinson, PhD., Dr. Buddhika Jayamaha & Dr. Molly M. Jahn.

The danger is that by focusing exclusively on a potential herd of Visigoths, we have missed out on the termites eating away at the gates. These are the slow and steady acts of attrition taking place in the interstitial space. The steady accumulation of small outcomes of interstitial attrition overtime can generate an absolute advantage to our adversaries and strategic competitors. Interstitial attrition provides an intuitive frame to better understand the actions of our adversaries and strategic competitors. A few examples illustrate the nature of the interstitial challenge.

We begin with the Russian annexation of Crimea, and the creation of a secessionist conflict in Ukraine. The implications of their behavior go beyond Russia reasserting itself as a regional power in its slowly decreasing sphere of influence. Rather, Russia's acts in Crimea fundamentally undermine an international consensus that has contributed to post WWII international stability: that deploying the force of arms is not an acceptable way to alter state borders. To make matters worse, as the U.S. turned up the heat in Venezuela, Russia sent Kremlin-backed mercenaries to protect Maduro. Because the soldiers were disguised as mercenaries doing the Kremlin's bidding, the U.S. is uncertain and unable to respond because it is engaging an emergent interstitial space that undermines the traditional understandings of military interventions and the legal annals that define foreign interventions.

Interstitial attrition has also undermined the U.S. position in the Middle East. Russia today is a powerhouse in the Middle East as well as an arbiter of their regional politics. It constantly probes American will - in air and on land - as it did when Russian mercenaries attacked American soldiers in Syria. It compels U.S. allies to cooperate with their potential adversary, Iran, an avowed American adversary (whose Supreme leader ritually chants "Death to America" on most Fridays). All of this sends the message that the U.S. no longer has primacy in the Middle East.

New realities in the South China Sea constitute another case of successful interstitial warfare. This area has long been an interstitial space by design. The Chinese knew the American position: that some U.S. Marines grabbing "a bunch of Chinese fishermen on an abandoned atoll" would not have gone over well. Little by little, China defeated the U.S. in this space. China today is in actual *de facto* control of the South China Sea, relegating the notion that the area is somehow contested to a mere figment of international juridical imagination.

Russia constantly probes along the border lands of NATO, and NATO airspace, and even in the western hemisphere by sending Kremlin-allied mercenaries (the Wagner Group), to protect Maduro in Venezuela. This was the same group that openly challenged US special operators in Syria in direct-fire engagements. Iran constantly probes American lines of control in the Middle East both overtly and covertly. China has incrementally proven that American primacy of command over the global open waters is subject to challenge. The point is that, in each of these cases, it was the steady accumulation of small outcomes that reversed the previous reality on the ground. Death by a thousand cuts - this is warfare in the interstitial space.

As interstitial spaces, both cyber and civil society also inhabit a legal space that defines a core element of western liberal democracies: the balance between negative and positive freedoms, between individual and collective rights and a state's ability to limit them. The challenge is how one secures the realm of domestic rights and upholds principles and builds defenses while generating a coherent offensive strategy of deterrence – ideally, with the buy-in from U.S European and Pacific allies. This is a daunting conceptual and strategic challenge.

Dr. Peter Layton

Visiting Fellow, Griffith Asia Institute (Griffith University)
22 February 2019

Can Machines Fight Wars?

Technological development is both accelerating and diffusing across the world. Future wars between great and perhaps also middle powers may involve both sides using large numbers of remotely controlled or semi-autonomous platforms and weapons. Given this, wars may become primarily a case of machines being violent to other machines. While such robot battles would test the opposing states' materiel resources as the process of violent machine attrition runs its course, whether it would be consequential is uncertain.

Geoffrey Blainey considers that wars are undertaken when the states concerned do not have an accurate assessment of their relative

strengths.[30] Robot wars may be a means to gain such an assessment albeit one more of materiel strengths than of moral ones. If states feel they have a greater stake in a conflict after the wars between the machines conclude, they may move on to wars between the people.

There is a seductive notion inherent here that low stakes conflicts might be able to be decided by robot wars even if high stakes ones cannot. Such robot wars would then be similar to current grey zone confrontations but destructive, a new step in the continuum between war and peace. Such an argument overturns a Russian notion that, if all involved have intelligent robots and none has a decisive advantage, that there will be peace through a balancing of military power. Instead, such widespread proliferation may lead to a greater temptation for states to unleash robot forces upon each other, hopeful that, while avoiding human casualties, the robots can decide the issue.

Today that perspective would probably mainly involve intelligent machine cyber forces battling in the virtual domain. In the medium-term it may expand to intelligent-machine swarms fighting each other at sea, in the air or in remote land areas (where discrimination between combatants and non-combatants is much easier). Crisis management approaches need to be reconceived, with priority given initially to approaches to manage intelligent machine-powered cyber-attacks.

An Emerging Defence Dominance?

The near-medium term future is seen as featuring potentially hostile state and non-state actors that can both employ precision-guided weapon systems and integrated battle networks[31] of various forms across the full conflict spectrum. New technology may allow new operational ways and capabilities to address this problem. Technological developments are providing the option of acquiring affordable remotely controlled/ semi-autonomous/ autonomous platforms and weapons that can be directed from distant command centres. Moreover, the capabilities of these command centres can be greatly enhanced through using artificial intelligence (AI) powered command support systems.

A distributed intelligent-machine approach can potentially transform extant battle networks from being simply movers of information into active fighting networks. Such intelligent machines would do more than enhance processing and improve contextualising as currently. They would now become actors themselves. This is a vision of robotic warfare conducted by unmanned and increasingly autonomous intelligent machine weapon systems, operating across multiple domains (air, sea, land, space, and cyber) and across all types of military operations.[32]

While this intelligent machine warfare approach still involves human-machine teaming, the place of machines is much greater. Earlier "do things better" concepts emphasised improved man-machine teaming. This "do better things" distributed intelligent machine approach reverses this. Machines now loom large as meaningful participants, not simply trusted advisers: humans command, machines do. In some respects, it is now not the battle network that is key to victory but the edge devices. Battle networks become conceptually inverted.

This machine-waged way of war brings three changes. First, it could allow affordable mass based around a force structure of many unmanned systems and limited numbers of crewed platforms. Second, it would sharply lower risks to personnel, thus lowering casualty rates of hard-to-replace, highly skilled people. Moreover, it would also ease the stresses and strains of war on people while reducing human workload, fatigue and cognition demands. Third, it could lower the present battle network's vulnerabilities to electronic jamming and cyber-attacks by sharply reducing the communication demands across the four grids. Intelligent machines may be able to wage war semi-independently, only needing human guidance from afar occasionally.

The distributed intelligent machine approach raises a fundamental issue when considering future warfare. The approach alters the shape of the present offence-defence balance although the direction is unsure. Is the offence or the defence dominant in this brave new robotic

[30] Geoffrey Blainey, *The Causes of War*, 3rd Edn, The Free Press, New York, 1988.
[31] Battle networks comprise interlinked digital computer systems conceptualised as four virtual grids (information, sensing, effect and command) that overlay the operational theatre. The sensing grid observes, the information grid orients (through disseminating information), the command grid decides, and the effects grid acts by targeting adversary forces.
[32] In this article, I am not considering the rather futuristic general AI robots envisaged in fiction. Instead I am focused on the capabilities narrow AI can potentially provide.

age? The worry is that, if offence dominates, the incentives to strike first in a crisis might grow. This would be strategically destabilising as all participants would then prefer to land the first blow given this may be a knockout one.

Being somewhat contrarian, I think defence will be the dominant form of future war. The complicated mix of AI, robotics, low cost sensors, big data, cloud computing and more will be easier to deploy and use in friendly territory than hostile.

In friendly territory a large number of internet-of-things (IoT) sensors can be emplaced in optimum locations based on a deep knowledge of both the terrain and the environment gained across decades. These IoT sensors can be robustly connected through a cloud-computing network to feed data back into remote command support systems that use AI to rapidly filter out the important from the background clutter. Changes will be able to be quickly responded to using well-positioned artillery, missiles or attack drones. Importantly, such engagement weapon systems are relatively short range; all have distinct limits because of energy constraints whether from propellant design on restricted onboard fuel.

In contrast invading forces will lack many of the home-ground advantages. They will need to be able to under fire quickly deploy large sensor fields cross distant battlefields, almost instantaneously very accurately map these battlefields, rapidly move short range robots forward, set up forward logistic and maintenance support areas and swiftly train the AI command support systems to detect changes.

The last may be particularly problematic in that the attacker compared to the defender will not have the depth or breadth of 'big data' necessary for optimum AI support or the best employment of robotic forces. Given they will have had years to prepare, the defender will potentially always have much better information about battlefield conditions than an attacker. The old computer-programming adage of 'garbage in, garbage out' then favours the defender.

In addition, the robotic battlefield requires a cloud-computing network that links all involved. In friendly territory clouds can be set up, tested, optimized and hardened against interference. By comparison, an invading force would need to push forward a combat cloud in the face of emplaced hostile electromagnetic countermeasures. This would be technically hard.

The result of all this is that a country's border zones will be able to be developed into no-man's lands. Hostile forces moving into them will be able to be quickly detected, identified, tracked and targeted using precision kinetic and non-kinetic fires. There will be nowhere to hide. In some respects, the Donbas battlefield's trench warfare may be a harbinger of this emerging age of robotic static frontlines. Small, wealthy Estonia seems already headed down the path of progressively building a robotic-barrier border zone.[33]

Defence looks likely to become dominant. However, this does not mean that offence will disappear. Instead new ways to mount an offensive will be developed. If a nation's borders cannot be penetrated and its critical centres of gravity attacked using kinetic means perhaps non-kinetic means are the offensive style of the future. Russia's recent information warfare against the US political system may hint at such new offensive warfighting techniques. Instead of destroying another's capabilities and national infrastructures, they might be exploited and used as bearers to spread confusion and dissent.

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

[33] Kelsey Atherton, 'Estonian war robots could have big implications for future NATO plans', *C4ISRNET*, 3 August 2018, https://www.c4isrnet.com/unmanned/2018/08/03/estonian-war-robots-could-have-big-implications-for-future-nato-plans/. [Accessed 21 February 2019].

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 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 functions 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

Infrastructure as a Key Point of American Weakness: Ripe for Attack?[34]

One of the most universal truths of military strategy, from Sun Tzu's *Art of War*, to Kautilya's *Arthaśāstra* (War and Diplomacy), and Clausewitz's *On War*, is that: You never attack an opponent at their strongest point. Instead, you focus your force where your opponent is weak and vulnerable. While this may *sound like common sense*, the United States (U.S.) military seems overly focused on fighting a style and form of war that adversarial near-peer states, such as Russia and China will not fight.[35] Instead, Russia and China will pursue indirect ways of waging war against the U.S., which weakens America's position and resolve, without provoking a direct military confrontation.

There is a famous (although misattributed) quote from Japanese Admiral Isoroku Yamamoto: "You cannot invade mainland United States. There would be a rifle behind each blade of grass."[36] While this quote lacks veracity, the sentiment seems to hold true. The Pew Research Center noted in 2013 that there are between 270 and 310 million guns in the United States.[37] The U.S. Census Bureau estimates that the U.S. population is around 315 million.[38] Any adversary would know that a direct assault on the mainland U.S. would be a bloody fight not worth the treasure. However, any military leader who has read Clausewitz also knows that leveraging your own strength against your enemy's weakness is a key to success. China has already established itself in the cyber domain, by developing artificial intelligence (AI) and quantum computing, and China and Russia are striving towards parity with American cyber capabilities.[39] It would make sense, then, that these rising revisionist powers would want to leverage these capabilities to create the greatest effects – as cheaply as possible. The easiest way for Russia and China (and to a lesser extent Iran and North Korea) to maximize their destructive power would be through cyber-attacks that cripple American infrastructure. Such actions would halt the U.S. economy, and would make an American military response difficult to mobilize and support.

The U.S. power grid has long been understood to be vulnerable to an attack.[40] Over the years, the growth of the power grid has left the grid more and more vulnerable.[41] Multiple digital points of entry allow for a wider spectrum of places that an enemy could target in hopes of compromising the system. This problem is compounded by the additions and patchwork integration of new systems into the ones already existing, leaving holes that have already been exploited (and continue to be).[42] Across America, 3,300 utilities work together to deliver power through 200,000 miles of high-voltage transmission lines and across 55,000 substations. This vast networked array has been cobbled together over several decades, with industry practices that vary in terms of technology used, as well as techniques for

---

[34] This article was made possible by contributions from Cadet Ethan D. Adams, my Research Assistant in the Department of Military and Strategic Studies, U.S. Air Force Academy, Colorado.
[35] Jahara Matisek and Ian Bertram, "The Death of American Conventional Warfare: It's the Political Willpower, Stupid," *The Strategy Bridge*, November 5, 2017, https://thestrategybridge.org/the-bridge/2017/11/5/the-death-of-american-conventional-warfare-its-the-political-willpower-stupid
[36] For the story of how this misattributed quote came to be, refer to: https://www.factcheck.org/2009/05/misquoting-yamamoto/
[37] Drew Desilver, "A minority of Americans own guns, but just how many is unclear," *Pew Research Center*, June 4, 2013, http://www.pewresearch.org/fact-tank/2013/06/04/a-minority-of-americans-own-guns-but-just-how-many-is-unclear/
[38] "Census Bureau Projects U.S. Population of 315.1 Million on New Year's Day," *United States Census Bureau*, December 27, 2012, https://www.census.gov/newsroom/releases/archives/population/cb12-255.html
[39] "Analysis on China's emerging governance regime around technology and cyberspace," *Center for Strategic & International Studies*, 2019, https://www.csis.org/programs/technology-policy-program/technology-and-innovation/cybersecurity-and-governance/china
[40] Jonathan Stidham, "Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack," *SANS Institute*, 2019, https://www.sans.org/reading-room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack-606
[41] "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," *Mission Support Center: Idaho National Laboratory*, August 2016, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf
[42] "Significant Cyber Incidents," *Center for Strategic & International Studies*, 2019, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

protecting the system from attack.[43] Increased connectivity between these industrial systems and the Internet-of-Things, alongside poor cyber security practices have given adversaries the ability to cause more physical and financial damage than the terrorist attacks of 9/11.

A coordinated, effective attack on the U.S. power grid could be catastrophic. According to the Department of Homeland Security (DHS), America has 16 sectors of infrastructure that are critical to a functioning society and economy.[44] They are headlined by the energy services sector, because the 15 other sectors – dams, financial services, nuclear reactors (to include material and waste), food and agriculture, water and wastewater systems, healthcare and public health, emergency services, transportation systems, chemical, communications, information technology, defense industrial base, critical manufacturing, government facilities, and commercial facilities – are all dependent on the power grid to keep them functioning. Unfortunately, there is little redundancy in this system, with a miniscule capability for a few to operate temporarily in a degraded fashion under diesel generator power. With only a few properly placed attacks, an adversary could cheaply cripple the U.S. – all without firing a shot and with little risk for retribution due to the attribution problem (i.e. it is extremely difficult to determine where an attack truly originated from).

America could not function as a modern state without these sectors working smoothly. Even if a power grid attack only degraded a handful of these sectors, the lost economic potential could be massive. If emergency services, healthcare, and transportation sectors were all decommissioned for even just a few days – while power was being restored – millions of Americans would be unable to work. The economy would suffer, public safety and security would be endangered, and thousands would likely die from a lack of medical care. This vulnerability is dependent on a single node, of which, any malicious actor – foreign or domestic – could exploit, plunging the U.S. into chaos. Those that wish to cause such harm to the U.S. could have discovered this for themselves through probing attacks, but a short visit to the DHS website showcases numerous American vulnerabilities with little investigation needed.[45]

While cyber-attacks pose a tremendous threat, the U.S. power infrastructure is equally vulnerable to kinetic attacks as well.[46] A small extremist group that lacks the funding and expertise of a well-trained army could inflict substantial damage through a physical attack on a power plant or loaded substation.[47] Such a domestic attack could even occur at the direction of foreign powers, by covertly funding and training one of America's many militia groups to follow through on their anti-government views and beliefs. The right attack at the right moment could produce blackouts stretching across multiple states, affecting millions of Americans.[48] Since many of the safety systems in place to prevent such a cascading failure of substations are designed simply to revert to manual system operations, they were designed to protect against natural disasters, which offer some warning and preparation. A cyber-attack would offer no such warning, and most likely no indication whatsoever of the breach until it was far too late. A conventional attack would run into the same difficulties, but even if the system was switched over to manual and isolated from the grid in time, the attackers could just take physical control of the plant or substation, and achieve the same results.

The American power grid lacks resilience, and is unprepared for an attack from malicious actors, relying on cyber power or kinetic attack. Equally unprepared, are agency emergency preparedness plans and systems, which are highly dependent on access to power and communications. In light of this, and coupled with the low cost, low risk, and far-reaching effects, the American power grid is a clear target for all adversaries, large or small. The future looks even bleaker as drones (especially ones equipped with AI) become mission capable in adversarial near-peer states that seek to weaken the U.S. and her allies. Such AI-drones could easily assault several critical nodes in the power grid, essentially taking the U.S. offline, and making the government and military too blind to know how to respond and coordinate a response.

Finally, with reports of China, Iran, North Korea, and Russia, developing electromagnetic pulse (EMP) weapons, this will create another avenue of capability in which any one of these hostile states could cheaply kill thousands of Americans, while inflicting billions of dollars'

---

[43] Anthony H. Cordesman and Justin G. Cordesman. *Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland* (Westport, CT: Greenwood Publishing Group, 2002).
[44] "Infrastructure Security," *Department of Homeland Security*, March 1, 2019, https://www.dhs.gov/topic/critical-infrastructure-security
[45] The topics tab on the DHS website illustrates the numerous vulnerabilities that DHS has identified. For more see: https://www.dhs.gov/
[46] "Electric Grid Security and Resilience Establishing a Baseline for Adversarial Threats," *ICF International*, June 2016, https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf
[47] "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector."
[48] Ryan Kinney, Paolo Crucitti, Reka Albert, and Vito Latora, "Modeling cascading failures in the North American power grid," *The European Physical Journal B-Condensed Matter and Complex Systems* 46, no. 1 (2005): 101-107.

worth of damage.[49] EMP bombs paired with miniaturization technology could make the dismantling of the American power grid as easy as delivering the mail to several power plants. Such developments mean that the U.S. military and allies must develop similar capabilities as a form of deterrence.[50] Without proper backups and redundancies, the U.S. may be on the precipice of an infrastructural 'Pearl Harbor' that may not be recoverable. Steps, such as modernization and proactive maintenance, must be taken to harden critical power nodes – physically and digitally – to ensure that any sort of attack does not plunge the U.S. back into the Stone Age.

Dr. Sean McFate[51]

Professor (National Defense University)
7 March 2019

How will the character of global competition and conflict change over the next decade? And which emerging global trends and conditions will drive this change?

Dr. McFate: I talk about the idea of durable disorder in my book (*The New Rules of War: Victory in the Age of Durable Disorder*). Durable disorder is what is left after the Westphalian system of nation states retreat, which we have been seeing consistently since at least the end of the Cold War. What this looks like is not, "The sky is falling. Invest in more sky." Rather, it is the overlapping authorities, sovereignties, etc. of other types of systems of governance. If you look at Somalia or Afghanistan or the Middle East or Iraq or Africa, for example, you do not have lawlessness—what you have is formal and informal authorities that overlap. And the central characteristic of this is persistent conflict (i.e., low-level intensity conflict that does not resolve). This is going to be the new environment for warfare. And this is not new, it is old. If you think back to the Middle Ages, this is the world that Machiavelli and others were lamenting. I think we are just actually returning to the status quo ante, and the Westphalian system of global governance is rather anomalous in world history.

How does US strategy and planning need to adjust to account for this new or reemerging age of durable disorder that you mention?

Dr. McFate: If I had a lot of time, I would write another book about grand strategy for durable disorder. Just like how after the Cold War the global environment shifted, it has shifted again. Yet, there is a lot of, in my opinion, confirmation bias by certain think tankers and experts about a need to reestablish the liberal world order. In my opinion, that horse has left the barn. I think what we need to do now is instead look at who, how, and why people will fight in the future—and the Westphalian way of warfare or conventional war is not the answer to these questions. The problem, however, is that our systems, our bureaucracies, our force structure, and the weapons that we buy and how we deploy them are essentially still conventional warfare-based, despite having dealt with unconventional war for several years now. Ultimately, warfare is changing, and we need to think more closely about how it is doing so.

It sounds like you are saying that the US and its systems might not be currently best suited or fully prepared to deal with this new age of durable disorder?

Dr. McFate: That is right. We are very deficient at this way of warfare. Our adversaries have grasped durable disorder, but we have not, and that is probably why we struggle.

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

[49] Laura Widener, "Russia, China, Iran, and North Korea working on EMP weapons for devastating attack on US," *American Military News*, October 23, 2018, https://americanmilitarynews.com/2018/10/russia-china-iran-and-north-korea-working-on-emp-weapons-for-devastating-attack-on-us/
[50] Kenneth Geers, "The challenge of cyber attack deterrence," *Computer Law & Security Review* 26, no. 3 (2010): 298-303.
[51] 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).

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.

Are there any final points about the future of global competition and conflict that you would like to highlight or emphasize?

Dr. McFate: Yes, a big one is: Why does everybody assume that a fight with Russia and China will be conventional? Why is that the case? I do not believe that is the case at all. In fact, I think we are already at competition. I do not know what word is appropriate for the competition, but we are already dealing with that right now with Russia and China and we need to get to beyond our current paradigm. We are a paradigm prisoner right now. We need to shift the paradigm and move on. Because war has moved on and we have not. Some of the best weapons today do not fire bullets. So, what do we need to do to get there? I do not think we need more F-35s or more forward carrier groups. I think we need other things. And we need to abandon this idea that great power competition will be conventional.

Additionally, I think we have been operating under several tropes that are strategic assumptions of both political science and strategy thinkers, such as command-driven economies will always fail, that internet will liberate everybody, etc. All of this stuff is, in retrospect, kind of childishly naive. War is getting sneakier, and we have to get sneaky with it. The challenge for us as a democracy is how do we do this without losing our soul? And this is an old problem going back to Thucydides—as Athens prolonged the war it became more autocratic. So, this is a central challenge we face.

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

Changes in the character of war, conflict, and competition are fundamentally driven by human agency, which is by definition open to and understandable by analysis.[52] Yet having the information, concepts, and frame of mind to anticipate or understand change appropriately is a completely different question. Further, there are two broad types of human-driven change: those it is possible to anticipate in some specific detail, and those which can be anticipated only generically because their precise implementation and performance depend on particulars from the theater of engagement.

The first category of change tends to be technology-based, taking substantial periods of time to develop the requisite capabilities to any level of competence and utility. Cyber operations have become an increasingly prominent feature of both global competition and conflict, with increased risk of damage proliferation, as cyber power does not discriminate. Worms such as Not-Petya can cause millions in damages not just to their main targets (Ukrainian firms and ministries) but also to wholly unrelated commercial organizations (Maersk, FedEx). It should be noted that the exact extent and victims of such collateral damage cannot be predicted.[53] Whenever conflict and competition develop a cyber element, the chances of collateral damage will skyrocket. Remotely piloted vehicles in the air, in and on the sea, and on land are also proliferating. These will affect the specific conduct of military operations, despite currently experiencing teething troubles, particularly on land (terrain generally and especially urban areas in Syria, interfering with Russian control of remotely piloted vehicles). The increasing development of missiles by US competitors is a noteworthy trend creating asymmetric capabilities with which to counter the traditionally dominant US military. The common element for all these developments is that humans are increasingly distanced from the battlefield or engagement points and so from physical harm, which may limit both political liability and commitment to a conflict.

The second category of change is based on specific human agency and innovation on the spot to adapt to the immediate environment and the challenges being faced, everywhere from the highest-level of political decision-making to armed individuals in the theater of conflict. It is impossible to anticipate such changes in detail, but it should be possible to anticipate generic phenomena as a response to one's own actions. Failure to anticipate solutions is often due to an inappropriate perspective on existing information (rather than pure lack of information) combined with a sudden shift in adversary intentions. Russian "hybrid warfare" in Crimea took the West by surprise because, first, it manifested a sudden apparent change in Russian policy towards aggression, completely bucking Western expectations; and, second, the West failed to think how competitors might exploit the weaknesses of its decision making, news agencies, etc. In retrospect, the notion of Russian "hybrid warfare" is completely logical as a way of competing with the West, but the West did not develop the necessary perspective until after it had occurred. However, now that it has been recognized, it is plausible to anticipate and identify this sort of ambiguity being employed elsewhere, such as by Russia in the Donbas and Syria (employing the Wagner Group).

Planning over the short and long term for strategic and other purposes will continue to focus on both categories of change, the more specific for technologies and the more general for the human dimension. Long-term planning for the unknowable future remains a gamble, but still needs to be done for decisions whose implementation has to be sustained over time and whose effects will be felt still longer-term, such as procurement. Given the uncertainty, it seems prudent to focus short-term planning on those capabilities and methods which are definitely coming—remotely piloted vehicles, various kinds of missile, cyber, as well as anticipatable non-kinetic means of evading or countering US military superiority—and longer-term on those capabilities which will always be needed, such as inter-regional if not global logistics and mobility.

If the history of US wars teaches anything, it is the imprudence of assuming that we will no longer fight certain kinds of wars. Politics may demand that the military undertake some strategic venture to protect national interests regardless of what form the anticipated resultant conflict may take. Moreover, the enemy contributes substantially to the character of any war, conflict, or competition, almost always to our disadvantage. Probable future demands require maintaining the capability to engage certain sets of adversarial tactics and strategies which the modern US military has traditionally sought to avoid when possible, such as counterinsurgency.

---

[52] See for example Lukas Milevski. "The Nature of Strategy Versus the Character of War", *Comparative Strategy* 35/5 (December 2016), 438-446.
[53] Andy Greenberg. "The Untold Story of Not-Petya, the Most Devastating Cyber Attack in History", *Wired.com*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, accessed 25 February 2019.

The United States and its allies also shape the character of a war, conflict, or competition. Good strategic, tactical, and planning performance minimizes the meaningful input the adversary can make to determine the character of the mutual interaction. This requires honest and thorough planning, rather than foregoing planning for political misassumptions about the results of intervention. Planning that turns out to have been unnecessary is still more prudent that not planning and losing the potential to offer a coherent response.

Contingency planning may need to incorporate more organizations even beyond the public sector as certain challenges increasingly involve non-military and even non-state dimensions, such as the Not-Petya worm's collateral damage. Not-Petya damage was partially incidental, but the future may bring coordinated cyber attacks which aim to strike at key corporate nodes, including perhaps logistical corporations such as Maersk alongside military targets to inflict not just an initial crippling but also to inhibit subsequent recovery efforts.

There is one final apparent trend which is significant for future great power competition and conflict, although its impact on planning is difficult to assess. This is the growing chasm between open liberal societies, which in the past have been wealthier and more technologically advanced, and authoritarian closed societies, which no longer are impoverished, but now challenge the West through their wealth, which can undermine through corruption, and technological know-how, often honed by foreign students in western universities. These players infiltrate western institutions even as their countries close themselves off, as China behind its firewall and Russia limiting and controlling its military, and now even civilian, access to the worldwide web. As democracies strive to represent majority political thought by regularly changing governments and their directions, authoritarian governments persist in political continuity potentially for decades, but when pressed can change policy virtually on a dime. This apparently unsolvable asymmetric disadvantage of democratic countries influences every level of decision-making and action, including even the viability of some long-term planning, especially that long-term planning which is most directly affected by politics and political activity.

Robert Morgus

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

Changing Character of Global Competition

As Valery Gerasimov, chief of the Russian armed forces, observed in 2013, "the use of political, diplomatic, economic and other non-military measures in combination with the use of military forces" will normalize globally as part of new, non-linear warfare.[54] Gerasimov's writing was not a threat from Russia to utilize all aspects of national power in competition with the United States, but instead an observation about the activities of what Russia sees as its peer-competitors in the U.S., Europe, and China. The warfare that Gerasimov described then is the same "great power competition" that recent United States defense and security strategies and national intelligence estimates have likewise observed.

This competition will play out in areas of traditional geopolitical competition, including over natural resources like rare earth minerals, water and waterways, and fossil fuels. However, for the purposes of this note, I will focus on an emerging area of strategic competition between powers: the struggle for control and dominance over the internet.

The battle over technology—particularly the internet, which produces data and fuels innovation—is both a medium of and a proxy for broader great power competition. Democracy versus authoritarianism is a part of it, but so too is the future of the global economy and global order or disorder. The way a country constructs (and spreads) its model for the internet impacts everything from sharing information on cybersecurity incidents to commerce and businesses, human rights and democracy, geopolitics and competition, and—critically—how data is generated, collected, and stored. A century ago, as the world industrialized, oil became the critical resource and—in many ways—drove competition between powers, great and small. Today, as technology evolves and the world digitizes, data becomes ever more crucial. This means that any great power competition may be over before militaries even enter the fray.

[54] https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf

Specifically, two crucial aspects of global competition over the internet are worthy of increased scrutiny:

1. The competition for information supremacy;
2. The competition for data supremacy.

The first battle over the internet implicates the global battle for ideas. While the internet has eschewed certain of its early stereotypes (free, open, secure), it has lived up to its billing as the "information superhighway."[55] For the better part of two decades, this increased information flow enabled by the global internet was held up as a potential great force for democratization around the world and as a means through which the U.S. and our allies could exercise soft power. However, to the surprise of many in the democratic world, undemocratic governments are immensely resilient, even in the face of forced transparency and greater information. The internet has not exactly carried through on the initial idealizations of democratic policymakers.

In recent years, authoritarian competitors have developed and leveraged methods to exploit the openness of the internet in the west to destabilize democracies, while consolidating control over information in their own countries. As more of the world digitizes, governments have figured out how to control and shape the internet in their character, consolidating greater and greater control over information in their borders. Rather than being a thorn in the side of authoritarianism in these places, the internet has become a vehicle through which governments can consolidate power and control, to varying extents, public discourse online.

The more codified undemocratic models for the internet, its governance, and its architecture become, the easier these models become to emulate around the world. Control over the internet, and mastery of its inherent vulnerabilities, equates to control over crucial information and narratives. Governments doing more to assert their control over the internet through social norms and laws that govern human behavior on it. But they are also taking steps to codify material changes to the internet's architecture that enable greater government control and visibility of data flows and online content. China and Russia are leaders in building out these viable alternative models for the internet and labor to spread them throughout the world using diplomatic, economic, and informational means.

The second point of competition over the internet takes is squarely economic. The metaphor "data as the new oil" isn't without its shortcomings, but it nonetheless captures the tenor of current and future competition over this resource. The massive amount of information exchanged on the internet—one estimate suggests that the internet facilitates over 3 billion gigabits of traffic per minute[56]—has created massive amounts of data. A great deal of attention has been paid to how applications of artificial intelligence (AI) and quantum computing could change the nature of military competition. However, this data will, in many cases, be the resource that drives forward crucial technological breakthroughs that drive economies and society into the future. How countries move to govern data and data flows will further impact digital economic competition.

Leninist and Maoist doctrine, from which modern-day Russia and China draw inspiration, emphasize the importance of the control of information, and particularly the role of information dominance in subduing technologically and materially superior opponents. In today's world, the internet is the key medium through which information is controlled. International forums like the United Nations are increasingly engaged in internet governance. As a result, the ultimate trajectory of the internet, its architecture, its governance, and its use are just as likely, if not more, to be driven by domestic developments around the world.

In the global contest over the internet, three primary clusters of countries have emerged.

- On one end of the spectrum sit a number of countries—spearheaded by the likes of Russia and China—that advocate for greater sovereign control over as series of interconnected but nationally distinct internets. On the other end of the spectrum sits a cluster of states that advocate for an open, global internet. Traditionally, both sides have argued for a global norm that fits their own national interest and that which they view to be in the interest of the rest of the world. The third cluster of states [are] the *Digital Deciders*—a group of states undecided or unconcerned about the best trajectory for the internet.[57]

Developments in Russia—like the creation of new technologies and laws to consolidate control over the internet with the

[55] https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/
[56] https://web-assets.domo.com/blog/wp-content/uploads/2018/06/18_domo_data-never-sleeps-6verticals.pdf
[57] https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/introduction/

government[58]—and China—like new data protection regulations[59] or cybersecurity laws[60]—impact the global push and pull over the internet. However, they are less interesting for what they do in Russia and China and far more interesting for what they do to prove their efficacy for others, particularly the *digital deciders*, to emulate.

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 non-kinetic 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 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*[61], 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 non-lethal 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 non-kinetic 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:[62]

- 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)

[58] https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/russias-plans-for-a-national-internet/
[59] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/china-data-governance-regime-timeline/
[60] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/
[61] RAND (2018). https://www.rand.org/pubs/research_reports/RR1772.html
[62] 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

- 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 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."[63]

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 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.

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

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

There is much that can be said about the character of global competition and conflict that I will not mention here. Instead, I will highlight one important piece of it: victories in global competition, if improperly managed, can come with significant costs. Specifically, while the US should remain competitive, the US must also consider the tradeoff between weakening global competitors and maintaining some level of state capacity.

This tradeoff was maybe most salient at the collapse of the Soviet Union. On one hand, decades of competition between the East and West ended with a major victory for the West. On the other hand, the collapse of the Soviet Union's state capacity left nuclear, chemical, and biological weapons unsecured. This is not to say that the US made a mistake and should have propped up the Soviet Union in some way. However, during the collapse, it was more possible for (a) rouge actors within the Soviet Union to launch attacks, (b) transnational terrorist or rogue states to obtain fissile material or biological weapons, or (c) nuclear weapons technology to proliferate more than we know it did (for example, potentially creating a nuclear Middle-East). In a counterfactual world where (a), (b), or (c) occurred, presumably the US would have absorbed significant costs to prevent any of these actions from happening.

There are many points to be raised on this issue. First, successes smaller than the outright collapse of a great power competitor can lead to problematic instances of diminished state capacity. The Soviet Union's retreat from Afghanistan created a vacuum where international terrorism flourished. Second, fractionalized state capacity is also a serious problem. Some share of Pakistan's government supports violent jihadi militants; as an oversimplification, the less control the elected government of Pakistan has over the government and military elements supporting these violent groups, the more the region will be destabilized and international terrorism will be a threat. Third, the concerns from limited state capacity is not limited to problems of terrorism. In the 1960s, to conduct a catastrophic attack, state or non-state actors would need to steal, hijack, be gifted, or develop a nuclear weapon. This is hard. Today, biological sciences and genetic editing has advanced to make developing a catastrophic biological weapon relatively cheap and possible under conditions that may be insecure. Ensuring that states, whether competitors or allies, have the capacity to keep some elements of the state from developing these weapons is critical to international security. Last, without maintaining state capacity, losses by one rival great power can become gains for another rival great power. As a success of this, after World War II, the US implemented the Marshall Plan to stave off initial losses in a new great power struggle.

Managing this tradeoff is hard. In some cases, it could be that maintaining a great power competitor or expanding their capacity is better in the long run. In other cases, letting great powers fail, despite the problems this failure can create, may be optimal. Regardless, when pursuing successes against global competitors, the US can better serve its own interests by considering the details of how to handle the aftermath of these successes at the onset.

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 outsized 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

The major trend is the continued rise of China, in both absolute and relative terms and across a growing array of metrics. This trend compels the United States to think less in terms of absolute dominance and more in terms of how it can rely on attraction and alliances to ensure desired global outcomes. While the pace of China's further rise in the next decade is uncertain, there is no plausible policy that would allow the United States to stop or reverse that trend.

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 most commonly does 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's 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.

Dr. William C. Wohlforth

Daniel Webster Professor (Dartmouth College)
4 March 2019

Managing the Emerging Great-Power Rivalry

The dominant assessment among governments and experts in Russia, China, and the United States is that great power rivalry will likely continue and even increase in the policy relevant future. This assessment is consistent with standard academic models for explaining and predicting great power politics. A major challenge in this setting is managing rivalry to reduce the threat of unwanted escalation. Rivalry management of this type hinges on the existence of mutually obvious thresholds that define what constitutes escalation. The main problem today is that the strategies of all three great powers work against the establishment of these thresholds.

1. Rivalry Management

Rivalry management is cooperation among rival great power leaders to control unnecessary escalation. The US Russian and Chinese leaderships have each concluded that its country's core interest requires military postures—force deployments, war plans, alliances, etc.—to shape the others' choices via deterrence or coercion. Each is ready to escalate to war if a rival truly threatens its core interest. Yet none believes war is inevitable. Each has a theory according to which sustaining a credible military posture will enable it to secure its objectives in the near and medium term until, over some unknown longer term, the rivalry is superseded by some now unforeseen development, or perhaps shifts in relative power and/or interest allow some now unattainable bargain to be achieved.

The phrase "unnecessary escalation" is needed because each side's theory presupposes a willingness to escalate to war under certain conditions. We have a rivalry because each side has rationally concluded that escalation of the rivalry (increasing risk of war) may be necessary according to its understanding of its interests. Each thinks the other might take action damaging to its core interests were it not deterred from doing so by the credible military forces it faces. Making that military posture credible requires plans and willingness to escalate if need be. Each, moreover, has an estimate of the other's basic disposition (its "type")—how strongly it supports or opposes the status quo—but that estimate is always uncertain, and, in any case, tomorrow the other side's type may change. Each therefore maintains security postures as a hedge against some shift in the other's interests. And each, finally, is maneuvering for advantage using tools of statecraft at its disposal, including, of course, implied or explicit promises to use force. So their military postures don't only deter and hedge but also cast the shadow in which day-to-day competitive bargaining occurs.

For all of these reasons, escalation may result from each side's rational pursuit of its interests. But all can agree that what each wants to avoid is any escalation inconsistent with its understanding of those interests. And achieving that may call for tacit or explicit cooperation with the leadership of the rival power.

2. Unnecessary Escalation

Escalation is an increase in the scale, intensity or scope of the rivalry that crosses a threshold the rivals regard as important. Unnecessary

escalation is any escalation inconsistent with the rational theories the sides hold about their rivalry. It may emerge endogenously from strategic interaction between rivals or it might appear to the leaders in part or entirely as some exogenous pressure.

The main endogenous cause is misunderstanding. One side may misinterpret the other's action as an escalation when it was not intended as such and escalate in response, setting off an unwanted "tit-for-tat" spiral. Scholarship from many disciplines has long established that leaders tend to see their own intentions as far less aggressive and threatening than others see them, and vice versa. It is easy to see how this bias could lead one side to interpret the other's move as more escalatory than it was intended to be.

Massive bodies of research have identified ways in which leaders may also feel pressure for unnecessary escalation that is partly or wholly exogenous: the imperatives of domestic governance (staying in power, retaining authority domestically); organizational "use it or lose it" pressures a crisis; status, "loss of face" fears that may impel leaders to escalate in response to minor or symbolic disputes in ways inconsistent with the underlying theory of the rivalry, and reputational pressures in which some peripheral commitment to which they have no major interest somehow comes to be defined by relevant audiences as a do-or-die test of their overall credibility.

3. Challenges to rivalry management.

These different escalatory mechanisms call for different forms of rivalry management.

Explicit cooperation can include "strategic dialogue" to try to explain each side's theory of the rivalry to the other; efforts to communicate limits, thresholds and red lines; holding summits and other prestige rituals to ward off status threats; holding regular summits as in the Cold War detente era to facilitate multiple avenues of rivalry management; arms control and confidence building measures to limit military postures that create organizational pressures to escalate early in a crisis. Tacit cooperation may entail mutual restraint to ward off status spirals; tacit agreement to keep actions secret that might incite escalation pressure from domestic or foreign audiences; and unstated mutual acceptance of certain thresholds.

Much IR scholarship that deals explicitly with these issues suggests that such cooperation is extremely hard and is likely to require a risky learning process. Aside from the ubiquitous complexity and difficulty of telling signal from noise in international politics, the key problem is that escalation is not just some problem to be managed; it is a strategic tool to be wielded to gain competitive advantage. This complicates any effort to cooperate to insulate the rivalry from unwanted escalation.

The chief antidote to unnecessary escalation arising from misunderstanding is cooperation to establish mutually unambiguous thresholds. The chief challenge to that cooperation is that leaders will face incentives to misrepresent their true thresholds. A line of research running from Schelling through Jervis to today's formal game theory sums to the expectation that communication through verbal pronouncements will be difficult because leaders will want to convince others that they are more willing to challenge or defend a given status quo than they really are. Each rival may thus discount the other's representations about thresholds. Each will try to work around, undermine, or render ambiguous the other's declared thresholds. Figuring out true thresholds may require bearing costs and risks.

The chief challenge to cooperation to limit more exogenous pressures to escalate is that the rivals will try to use those pressures strategically to gain advantage. A leadership team may well want its rival to believe that it is being constrained or pushed by domestic politics or allies when in fact it's seeking to move a piece on the chessboard to a more advantageous position. Schelling famously discussed how organizational processes might be strategically manipulated to gain advantage.

4. Mutually Obvious Thresholds

The main theme that runs through all the potential sources of unnecessary escalation pressure is uncertainty—the difficulty of knowing whether some action represents a true escalation that puts core interests at risk. Given that each rival faces incentives to try to make advances that do not elicit an escalatory retaliation from the other side, each will seek to use salami tactics against the other. If one is revisionist and the other stands for the status quo, then the latter faces the incentive to establish the most favorable possible thresholds for escalation and the former will seek to slice away at these or devise clever strategies to render them ambiguous. The strength of the rivals' incentive to cooperate on limits to these strategic games will be a function of their joint estimate of the point at which unnecessary escalation risks outweigh the expected strategic gains in play.

The escalation literature suggests that cooperation to establish clarity about these things is easier if there are mutually obvious, inarguable thresholds in the strategic environment. All such thresholds are subjective social constructions, but some may be well settled and predate the rivalry itself. Today these would include such thresholds as nuclear use, the use of other WMD, the use of force against sovereign territory, or otherwise directly against the rival's military forces, assassination of the rival leader, seizing of hostages, etc. We can call these "exogenous" in the sense that they do not require additional strategic interaction or negotiation to clarify.

These should be easiest to anticipate and least subject to strategic manipulation. The more such salient thresholds there are that are important to the rivalry but do not need to be clarified, the easier rivalry management should be. But the longer your time horizon, the more things can be "endogenized." That is, thresholds that seem well set, such as sovereignty or first use of force or prohibited weapons, can become blurry as a result of conscious strategy or as the unanticipated outcome of other behaviors.

Other thresholds emerge in the context of the rivalry, such as use of force against allies, or against a rival's forces deployed overseas as tripwires, or various levels of activity in the rival's spheres of influence. These may be tacit or explicitly recognized in agreements, with the former sometimes leading to the latter, as in the case of the Helsinki Accords. As the Helsinki example suggests, these can also become very settled and clear. To the degree that leaders anticipate that settled thresholds will end up structuring the rivalry, they face incentives to try to establish them early. Leaders may be tempted to push hard early in a rivalry to set the most advantageous thresholds, but setting them can itself cause a crisis. This reinforces the worry that some initial crises in a rivalry may necessary for later cooperation.

5. Implications for US Strategy

If settled, salient thresholds are as important as theory says they are, we may be in for some trouble, for two reasons. First, much current commentary suggests that management might be harder now than in the Cold War:

- So called "hybrid war" or "raiding" blurs the key first-use-of-force-across-sovereign-borders threshold;
- The ambiguous new domain of cyber may also be resistant to mutual understanding on the meaning of escalation and thresholds as well as the interference-in-sovereign-affairs threshold;
- The rise of human rights norms muddies the sovereignty threshold opening up avenues for misunderstanding, or perhaps the strategic use of these norms to intervene in adversaries' domestic affairs.
- The geography of the US-PRC rivalry may just be less amenable to salient thresholds: scattered islands and reefs and contending maritime claims may just be harder to clarify than the Cold War's land border-based central front;
- Emerging multipolarity may complicate signaling of thresholds compared to the comparatively pristine bipolarity of the Cold War.

Second, these challenges are in part just an outgrowth of strategic assessments and associated strategies in the relevant capitals. Analyses of strategic thinking in Washington Beijing and Moscow suggest that in each capital the belief is that time is on its side over the long term. In particular, Americans think China's rise is going to slow or stall and that Russia is a declining state with few options, while both China and Russia think US decline, dissension within and among US allies, US strategic retreat, and the emergence of multipolarity are all likely in the medium-term. Hence each faces lower incentives to manage the rivalry by establishing thresholds that reflect the status quo. Research I have conducted with Stephen Brooks shows that the status quo remains favorable to US interests.[64] If that is so, then, as I have argued with Jennifer Lind, the United States stands to gain the most by a move toward a more unambiguously conservative strategy. [65]

[64] https://www.amazon.com/America-Abroad-Superpower-Should-World/dp/0190464259
[65] https://www.foreignaffairs.com/articles/2019-02-12/future-liberal-order-conservative?cid=otr-author-march_april_2019-021219

Ali Wyne[66]

Policy Analyst (RAND Corporation)
8 March 2019

The Imperative of Articulating Long-Term Strategic Objectives

Close to two decades after the publication of his seminal text *Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy* (1982), the historian John Lewis Gaddis considered how, if at all, he would have written it differently. He concluded that "there were greater sources of strength on the Western side of the [Cold War]—and elements of continuity in American grand strategy—than had been apparent at the time I wrote my book."[67] The most critical, in Gaddis's judgment, was "an implicit agreement, within the American foreign policy establishment, on the fundamental purposes of containment: on *its projected end point*" (emphasis mine). "This single, simple, and continuous priority," he explained, supplied "a center of gravity for American Cold War strategy: whatever the oscillations between parties or between approaches, this fundamental objective always remained."

The United States has lacked a comparable ballast since the Soviet Union's dissolution. At least as presently conceptualized, the construct of "great-power competition" seems unlikely to furnish one, not only because its two central foci—China and Russia—have markedly different capacities, strategies, and ambitions, but also because it does not articulate a steady state. Recall the old quip, often attributed to Yogi Berra: "If you do not know where you are going, any path will get you there." The two potential objectives that do come to mind, unfortunately, offer little policymaking guidance. First, suppose that the United States were to endeavor to remain the world's foremost power. Even if it were henceforth to commit no self-inflicted strategic errors, the "rise of the rest" would virtually assure that it would be unable to maintain its present degree of centrality in world affairs. While there is good reason to believe that it can, and will, remain primus inter pares indefinitely, it cannot preserve in amber the present global balance—a reality that raises important questions: what is the minimum threshold of preeminence that Washington would deem acceptable, and how would it assess whether it was staying above? Those questions, in turn, raise a more fundamental one: how should we measure power and influence?

Second, suppose that the United States were to endeavor to maintain the current postwar order. Attempting to lock it into place could further disillusion countries—vocal critics and sympathetic participants alike—who ask why they should indefinitely be beholden to a system that they had little to no role in constructing; an already fragile system could hurtle towards obsolescence. On the other hand, aiming to integrate China and Russia fully into the postwar order could risk diluting its normative essence, raising the possibility of its collapsing under the weight of internal contradictions: the Brookings Institution's Thomas Wright ventures that such a gambit would lead us back into "an era when a few people carved the world up into spheres of influence, rather than a system where rules, values, and votes play a leading role."[68] Implicit in the discussion of both possibilities, however, is the presumption that the chief threats to the postwar order are external; unfortunately, though, and perhaps more importantly, that architecture is also under duress from within: the U.S. adoption of an "America First" foreign policy—with its emphasis on transactional diplomacy and its skepticism of multilateral accords and institutions—and the ascent of disintegrationist elements within the European Union have collectively weakened the transatlantic project that has buttressed it for nearly three quarters of a century.

The point of the preceding is less to suggest a particular steady state than to stress the importance of articulating one; competition, after all, is a means, not an end. The more that the United States treats competition as an imperative unto itself, the more that it risks conflating action with accomplishment (consider a seesaw, which continues to move but ultimately stays in place) and losing the ability and/or willingness to distinguish between unfavorable outcomes in world affairs that significantly undermine its national interests and those that undercut them only marginally. It would be imprudent to hope that the accumulation of notionally "competitive" measures will reveal a coherent strategy in due course; it would be more sensible, instead, for Washington to envision alternative futures in which it is able to advance its vital national interests and shape an order that is consonant with their continued pursuit, and to formulate strategies that might help those scenarios to materialize.

[66] 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.
[67] https://www.hoover.org/research/strategies-containment-past-and-future
[68] https://www.theatlantic.com/international/archive/2018/09/liberal-international-order-free-world-trump-authoritarianism/569881/

Even if Washington did not have to worry about the financial challenges inherent in undergirding a global order, it would eventually confront strategic exhaustion were it to assume uncircumscribed competition as an indefinite mandate. Despite its singular capacity, though, it does not have that luxury: fiscal imperatives will increasingly require it to pursue a foreign policy that prioritizes the defense of what *Foreign Affairs* Editor-in-Chief Gideon Rose calls the "core" of the postwar order over its "periphery." The Congressional Budget Office projects that the United States "will spend more on interest [payments on federal debt] than it spends on Medicaid in 2020; more in 2023 than it spends on national defense; and more in 2025 than it spends on all nondefense discretionary programs combined."[69] This trajectory will increasingly curtail America's agency.

In addition, a foreign policy that avows the necessity of tradeoffs but admits none in practice runs counter to the basic precepts of strategy: the United States cannot credibly assess, on the one hand, that the nerve center of world affairs is, and increasingly will be, the Asia-Pacific, and insist, on the other hand, that it will commit to that region as significantly as it will to other regions. Foreign policy entails the continual reallocation of finite equities abroad; it does not permit the indefinite creation of new ones. While Washington would be remiss to neglect Russian revanchism and turbulence in the Middle East, it should manage them within an eastward-looking framework that appreciates the Asia-Pacific's growing importance to global growth: PricewaterhouseCoopers forecasts that four of the world's ten largest economies in 2050 will belong to Asian countries, with China ranking first, India ranking second, Indonesia ranking fourth, and Japan ranking eighth.[70]

The Mistaken Pretension to Omnipotence

One might contend that the world's lone superpower need not be overly concerned with the purported necessity for choice, given the unrivaled freedom of maneuver it enjoys—perhaps the greatest of any power in history. One might posit, alternatively, that the United States does not have the luxury to prioritize certain regions over others, lest it convey the impression that it is disinterested in maintaining the whole of the order that it has constructed—and, in so doing, embolden revisionist elements. Though they arise from different sentiments—complacence and concern—both contentions exaggerate U.S. agency. Few judgments have proven as essential in the shaping, and as damaging to the conduct, of postwar—and especially post-Cold War—U.S. foreign policy as the belief that the United States can strengthen its position abroad through sheer dint of unilateral exertion; then-Secretary of State John Foster Dulles articulated its folly in an October 1957 essay for *Foreign Affairs*:[71]

> There still remains a nostalgia for the "good old days." This is reinforced by recurrent demonstrations that, great as is our strength, we are not omnipotent. We cannot, by fiat, produce the kind of a world we want. Even nations which depend greatly upon us do not always follow what we believe to be the right course. For they are independent nations, and not our satellites. Our power and policy are but one significant factor in the world in which we live. In combination with other factors we are able to influence importantly the course of events. But we cannot deal in absolutes.[72]

The resilience of the aforementioned presumption has tracked with the endurance of declinism: if one believes that the United States should essentially be able to dictate the course of world affairs, one will understandably adduce any outcome that runs counter to its national interests as evidence of its impotence. In reality, while Washington has endured many setbacks in the postwar era, ranging from the "loss" of China to wide-ranging Soviet inroads across Africa and Asia, it has become the world's preeminent power.[73] Declinist thinking, of course, can be strategically useful even if it is analytically misguided: the political scientist Samuel Huntington argued near the end of the Cold War that "the United States is unlikely to decline so long as its public is periodically convinced that it is about to decline."[74] His optimism, though, requires a prudent harnessing of that fear. If Washington responds to its present anxiety about China's resurgence by strengthening its own economic vibrancy and working to forge a more inclusive order, that sentiment could be an asset; if it responds by further overextending itself and undertaking to suppress the eastward shift in geopolitical gravity, that same sentiment could be a liability.[75]

---

[69] https://www.wsj.com/articles/u-s-on-a-course-to-spend-more-on-debt-than-defense-1541937600
[70] https://www.pwc.com/gx/en/world-2050/assets/pwc-the-world-in-2050-full-report-feb-2017.pdf
[71] https://www.foreignaffairs.com/articles/united-states/1957-10-01/challenge-and-response-united-states-policy
[72] See also D. W. Brogan, "The Illusion of American Omnipotence," *Harper's Magazine*, No. 205 (December 1952): pp. 21-28.
[73] I discuss some of those setbacks—and the attendant declinist prognostications—in "Myth of decline," *American Review* (August 2014): pp. 38-46.
[74] https://www.foreignaffairs.com/articles/united-states/1988-12-01/us-decline-or-renewal
[75] Huntington offered valuable advice on leveraging declinism, as I note in "How the US should frame its approach to China," *Financial Times*'s beyondbrics forum (July 24, 2019).

The supposition of, or hope for, something approaching omnipotence militates against the imperative of prioritization; paradoxically, explains the political scientist Robert Jervis, the preponderance of America's power breeds anxiety: "The very fact that the United States has interests throughout the world leads to the fear that undesired changes in one area could undermine its interests elsewhere….Disturbances that would be dismissed in a multipolar or bipolar world loom much larger for the hegemon because it is present in all corners of the globe and everything seems interconnected."[76] Thus, rather than husbanding its power, Washington tends to err on the side of omnipresence and overcommitment.[77]

[76] Arthur Schlesinger, Jr. made a similar point nearly three decades before Jervis, albeit in a different geopolitical context (and with considerable snark): "A recurrent experience of the American people is to discover that some exotic locality of which they had not previously heard is vital to the national security of the United States. An unknown place that had never before disturbed our dreams suddenly becomes…the key to some momentous global conflict." See "Russians and Cubans in Africa," *Wall Street Journal* (May 2, 1978).

[77] I elaborate on this point in "A Preliminary Critique of the 'Do Something Now' Doctrine," *War on the Rocks* (April 2, 2014).

Subject Matter Expert Biographies

Dr. Gawdat Bahgat

Professor, National Security Affairs, Near East South Asia Center for Strategic Studies (National Defense University)

Dr. Gawdat Bahgat is professor of National Security Affairs at the National Defense University's Near East South Asia Center for Strategic Study. He is an Egyptian-born specialist in Middle Eastern policy, particularly Egypt, Iran, and the Gulf region. His areas of expertise include energy security, proliferation of weapons of mass destruction, counter-terrorism, Arab-Israeli conflict, North Africa, and American foreign policy in the Middle East. Bahgat's career blends scholarship with national security practicing. Before joining NESA in December 2009, he taught at different universities. Bahgat published ten books including Alternative Energy in the Middle East (2013), Energy Security (2011), International Political Economy (2010), Proliferation of Nuclear Weapons in the Middle East (2007), Israel and the Persian Gulf (2006), and American Oil Diplomacy (2003). Bahgat's articles have appeared in International Affairs, Middle East Journal, Middle East Policy, Oil and Gas Journal, and OPEC Review, among others. His work has been translated to several foreign languages. Bahgat served as an advisor to several governments and oil companies. He has more than 25 years of academic, policy and government experience working on Middle Eastern issues. Bahgat has contributed to CNN, BBC, Washington Post and Al-Jazeera. He has spoken at Tufts University, Columbia University, London School of Economics, Swiss Federal Institute of Technology in Zurich, Swiss Foreign Ministry, Yildiz Technical University in Istanbul, Qatar University, Kuwait University, Oman Diplomatic Institute, Griffith University (Australia), and India School of Business.

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.

Dr. Ryan Burke

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

Dr. Ryan Burke is an Associate Professor and Curriculum Director in the Department of Military & Strategic Studies at the U.S. Air Force Academy. As Curriculum Director, Dr. Burke designs and implements the academic curriculum of instruction for 22 Military & Strategic Studies courses taught to over 1,500 students per year. Ryan received his USAFA appointment after completing a Department of Defense-funded post-doctoral research fellowship in the University of Delaware's Joseph R. Biden School of Public Policy and Administration. He also earned his Ph.D. from the Biden School where – in addition to teaching undergraduate public policy courses – he was awarded the prestigious University Dissertation Fellowship during his final year of study. Ryan's research emphasizes military and defense policy across the spectrum of conflict. He has authored multiple monographs focused on defense policy; peer-reviewed journal articles; book chapters; conference papers, and winning essays in national competitions. He is also the chief editor of Military Strategy, Joint Operations, and Airpower: An Introduction (Georgetown University Press, 2018) and is an opinion contributor to The Hill on defense and military policy matters. Ryan's research has been featured on TV and in print with Fox News, NBC, ABC, Business Insider, USA Today, The Hill, the Modern War Institute, and more. He has been an invited consultant in educational steering groups nationwide, serves as a peer-reviewer for multiple journals, and regularly presents at national conferences. Prior to his academic pursuits, Ryan was a U.S. Marine Corps officer where he served as a platoon commander, operations officer, and company commander during his fleet tour. He then served as the Deputy Marine Officer Instructor at the University of Pennsylvania's Naval ROTC unit. After leaving the Marines, he worked as a Senior Consultant and Logistics Analyst for Booz Allen Hamilton supporting Department of Defense projects in the Pentagon and with the Marine Corps Combat Development Command. He earned his bachelor's from Penn State University – where he attended on a Marine-Option Naval ROTC scholarship – and his master's from Saint Joseph's University in Philadelphia prior to earning his doctorate at the University of Delaware.

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. He and his wife reside in Vienna, Va.

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. Orignally 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 Cooporation 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.

Dr. Michael W. Fowler

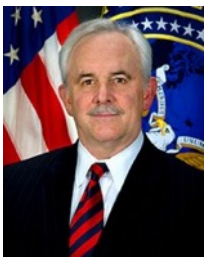
Associate Professor, Department of Military and Strategic Studies (US Air Force Academy)

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. Mike and his wife, Krissie, have three kids: Josh, Katie, and Sarah.

David C. Gompert

Distinguished Visiting Professor (US Naval Academy)
Adjunct Professor (Virginia Union University)
Senior Fellow (RAND Corporation)



The Honorable David C. Gompert is currently Distinguished Visiting Professor at the U.S. Naval Academy, Adjunct Professor at Virginia Union University, and Senior Fellow at RAND. Mr. Gompert was Principal Deputy Director of National Intelligence from 2009 to 2010. During 2010, he served as Acting Director of National Intelligence, in which capacity he oversaw the U.S. Intelligence Community and acted as the President's chief intelligence advisor. Prior to his most recent government service, Mr. Gompert was a Senior Fellow at the RAND Corporation, from 2004 to 2009. Before that he was Distinguished Research Professor at the Center for Technology and National Security Policy, National Defense University. From 2003 to 2004, Mr. Gompert served as the Senior Advisor for National Security and Defense, Coalition Provisional Authority, Iraq. He has taught at RAND Graduate School, U.S. Naval Academy, the National Defense University, Virginia Commonwealth University, and Virginia Union University. Mr. Gompert served as President of RAND Europe from 2000 to 2003, during which period he was on the RAND Europe Executive Board and Chairman of RAND Europe-UK. He was Vice President of RAND and Director of the National Defense Research Institute from 1993 to 2000. From 1990 to 1993, Mr. Gompert was Special Assistant to President George H. W. Bush and Senior Director for Europe on the National Security Council staff. He has held numerous positions at the State Department, including Deputy to the Under Secretary for Political Affairs (1982-83), Deputy Assistant Secretary for Europe (1981-82), Deputy Director of the Bureau of Political-Military Affairs (1977-81), and Special Assistant to Secretary of State Henry Kissinger (1973-75). Mr. Gompert worked in the private sector from 1983-1990. At Unisys (1989-90), he was President of the Systems Management Group. At AT&T (1983-89), he was Vice President, Civil Sales and Programs, and Director of International Market Planning. Mr. Gompert has published on international affairs, national security and information technology. His books (authored or co-authored) include *War with China: Thinking through the Unthinkable, Blinders, Blunders, and Wars: What America and China Can Learn; Sea Power and American Interests in the Western Pacific; The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability; Underkill: Capabilities for Military Operations amid Populations; War by Other Means: Building Capabilities for Counterinsurgency; BattleWise: Achieving Time-Information Superiority in Networked Warfare; Nuclear Weapons and World Politics (ed.); America and Europe: A Partnership for a new Era (ed.); Right Makes Might: Freedom and Power in the Information Age; Mind the Gap: A Transatlantic Revolution in Military Affairs*. Mr. Gompert is a member of the Council on Foreign Relations and the Advisory Board of the Naval Academy Center for Cyber Security Studies and chairman of the board of Bobcats Sports League. He has served on numerous for-profit and not-for-profit boards. Mr. Gompert holds a Bachelor of Science degree in Engineering from the U. S. Naval Academy and a Master of Public Affairs degree from the Woodrow Wilson School, Princeton University. He and his wife Cynthia live in Virginia and New Hampshire.

Dr. Barry B. Hughes

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

Dr. Barry B. Hughes is John Evans Professor at the Josef Korbel School of International Studies, University of Denver. Dr. Hughes earned a B.S. in Mathematics from Stanford and his Ph.D. in Political Science from the University of Minnesota. He served the University of Denver as Vice Provost for Graduate Studies in the 1990s. He established and led the Pardee Center in 2007-15. His principal interests are in (1) global change, (2) computer simulation models for economic, energy, food, population, environmental, and socio-political forecasting, and (3) policy analysis. The fundamental concerns that synthesize these interests are (1) developing effective response to long-term global

change and (2) improving the long-term human condition. He developed *International Futures (IFs),* the widely-used computer simulation for study of long-term national, regional, and global issues (see http://Pardee.du.edu). Dr. Hughes has supported the U.S. National Intelligence Council's reports to the President on *Mapping the Global Futures 2020, Global Trends 2025,* and *Global Trends 2030.* He provided long-term global forecasting for the United Nations Environment Programme's *Global Environment Outlook 4*. He provided background research papers and forecasting content used in the *United Nations Human Development Reports* (2011 and 2013). He was a principal researcher in European Commission projects on the New Economy and on Information and Communications Technology. He has contributed research to projects of RAND, the Central Intelligence Agency, United States Institute of Peace, Peru's National Center for Strategic Planning (CEPLAN) and many other organizations. Dr. Hughes has written or co-authored *The Domestic Context of American Foreign Policy* (Freeman 1978), *World Modeling* (Lexington 1980), *World Futures* (Johns Hopkins 1985), *Disarmament and Development* (Prentice-Hall 1990), *Continuity and Change in World Politics* (Prentice-Hall 1991, 1994, 1997, 2000), *International Futures* (Westview 1993, 1996, 1999), *Exploring and Shaping International Futures* (Paradigm 2006), *Reducing Global Poverty* (Paradigm and Oxford University Press, 2009), *Advancing Global Education* (Paradigm and Oxford University Press, 2010), *Improving Global Health* (Paradigm and Oxford University Press, 2011), *Building Global Infrastructure* (Paradigm and Oxford University Press, 2013), *Strengthening Governance Globally* (Paradigm and Oxford University Press, 2014), *International Futures: Building and Using Global Models* (Elsevier 2019) as well as articles in publications including *World Politics, International Organization*, *International Studies Quarterly*, *Futures*, *L'Express, Energy Policy, Policy Studies Review, International Political Science Review, Simulation and Gaming, Economic Development and Cultural Change, Bulletin of the World Health Organization, Sustainability, Climatic Change, Technological Forecasting and Social Change,* and *World Development.*

Dr. Molly M. Jahn

Professor (University of Wisconsin-Madison)

Molly M. Jahn served as Deputy and Acting Under Secretary of Agriculture and is a Professor at the University of Wisconsin-Madison where she holds appointments in the Department of Agronomy, the Nelson Institute, and the Global Health Institute. She was Joint Faculty at the U.S. Department of Energy Oak Ridge National Laboratory (ORNL) where she chaired the Scientific Advisory Committee of the Energy and Environmental Sciences Directorate. She is a Senior Research Scientist at Columbia University and Guest Scientist at Los Alamos National Laboratory.

Dr. Buddhika Jayamaha

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

Buddhika Jayamaha is a former U.S. Army Airborne Infantryman and Veteran of the 82nd Airborne Division with numerous deployments to Iraq. He holds a Ph.D. in Political Science from Northwestern University and is currently an Associate Research Scientist at the University of Wisconsin-Madison, Department of Agronomy.

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.

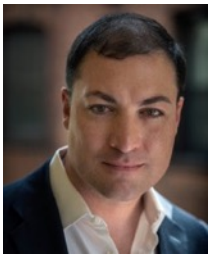
Dr. Jahara Matisek

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). He lives in Washington, DC.

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.

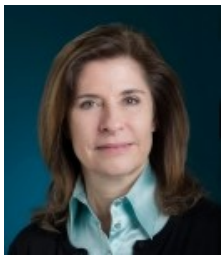
Robert Morgus

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.

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. 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. 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.

Dr. William C. Wohlforth

Daniel Webster Professor (Dartmouth College)

A member of the Government Department's faculty since 2000, I teach and conduct research on international relations, with an emphasis on international security and foreign policy. Before coming to Hanover, I taught at Princeton and Georgetown. I am the author or editor of nine books and some 60 articles and chapters on topics ranging from the Cold War to contemporary U.S. grand strategy. I teach courses in international politics, Russian foreign policy, leadership and grand strategy, violence & security and decision-making. My curriculum vitae has all the details. At Dartmouth, I've served as chair of the Government Department, on the Committee Advisory to the President, the Committee on Instruction, and on many College level search committees. Beyond Dartmouth, I've held fellowships at the Institute of Strategic Studies at Yale, the Center for International Security and Cooperation at Stanford, and the Hoover Institution. For six years I served as associate editor and then editor-in-chief of the journal Security Studies. A lot of my work is relevant to policy. I participate in a working group sponsored by the National Intelligence Council that is studying strategic responses to U.S. unipolarity. Our work has figured in several NIC reports, including most recently *Global Trends 2030*. I have served as a consultant to the Strategic Assessment Group and the National Bureau of Asian Research. I routinely lecture and conduct seminars with policy-makers, including, in recent years, the National Defense University, Naval War College, Army War College, George C. Marshall Center for Security Studies, and defense and foreign policy institutes in Germany, Canada, Portugal, Norway, Russia, and the United Kingdom.

Ali Wyne

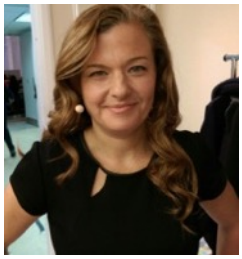
Policy Analyst (RAND Corporation)

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.

Dr. Jen Ziemke

Associate Professor (John Carroll University)



Jen Ziemke holds a Ph.D. in Political Science from the University of Wisconsin-Madison. She co-founded the Crisis Mappers Network, co-curated its conference series, and serves as a director for the Open Geospatial Consortium. She is currently Associate Professor at John Carroll University focusing her teaching and research at the intersection of data perceptualization, conflict, and security studies.

Author Biography

Dr. Allison Astorino-Courtois

Chief Analytics Officer and Executive Vice President (NSI, Inc.)

Dr. Astorino-Courtois is NSI's Chief Analytics Officer (CAO) and Executive Vice President. She has served as co-chair of a National Academy of Science's study on Strategic Deterrence and served as the deterrence lead on the National Research Council's recent Space Deterrence and Protection study for the Director of National Intelligence and Secretary of Defense. For the past 10 years Dr. Astorino-Courtois also has served as technical lead and provided the conceptual models and analytic frameworks for rapid turn-around projects sponsored by the Office of the Secretary of Defense. These efforts include design of a "Rich Contextual Understanding" analytic approach for for the Intelligence Chief and Commander of Allied forces in Afghanistan (Com ISAF); development of NSI's Stability Model (StaM) as a methodology for conducting provincial assessments for the ISAF Joint Command; assessments of national and sub-national drivers of political, economic, and social instability for USCENTCOM, USPACOM, USAFRICOM, and the intelligence community; and projects on deterrence and decision assessment models for USSTRATCOM. Previously, Dr. Astorino-Courtois was a tenured Associate Professor of International Relations at Texas A&M University where her research focus was cognitive aspects of foreign policy decision making. She has also taught at Creighton University and as a visiting instructor at the U.S. Military Academy at West Point. Dr. Astorino-Courtois earned her Ph.D. in International Relations/Research Methodologies from NYU. Her BA is in political science from Boston College.