Strategic Studies Quarterly • Fall 2018

SSQ Strategic Studies Quarterly

Fall 2018 Volume 12, No. 3

Securing the Nation One Partnership at a Time
Gen Joseph L. Lengyel, USAF

Feature Article
Confidence Building Measures for the Cyber Domain
Erica D. Borghard
Shawn W. Lonergan

The Case for the US ICBM Force
Matthew Kroenig

Russian Information Warfare: Implications for Deterrence Theory
Media Ajir
Bethany Vailliant

The Strategic Promise of Offensive Cyber Operations
Max Smeets

Soft Power in China's Security Strategy
LTC Mikail Kalimuddin, SAF
David A. Anderson

AUP

SSQ Strategic Studies Quarterly

Strategic Studies Quarterly

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

FALL 2018 VOLUME 12, NO. 3

Policy Forum

Securing the Nation One Partnership at a Time 3
Gen Joseph L. Lengyel, USAF

Feature Article

Confidence Building Measures for the Cyber Domain 10
Erica D. Borghard
Shawn W. Lonergan

Perspectives

The Case for the US ICBM Force 50
Matthew Kroenig

Russian Information Warfare: Implications for Deterrence Theory 70
Media Ajir
Bethany Vailliant

The Strategic Promise of Offensive Cyber Operations 90
Max Smeets

Soft Power in China's Security Strategy 114
LTC Mikail Kalimuddin, SAF
David A. Anderson

Book Reviews

The China Questions: Critical Insights into a Rising Power 142
By: Jennifer Rudolph and Michael Szonyi
Reviewed by: Capt Sean E. Thompson, USAF

An Untaken Road: Strategy, Technology, and the Hidden History of America's Mobile ICBMs 143
By: Steven A. Pomeroy
Reviewed by: Daniel Schwabe

Understanding Cyber Conflict: 14 Analogies 145
By: George Perkovich and Ariel E. Levite
Reviewed by: Lt Col Mark Peters, USAF

Russia's Dead End: An Insider's Testimony 147
By: Andrei A. Kovalev
Reviewed by: Lt Col Mark Peters, USAF

Securing the Nation One Partnership at a Time

America's alliances and partnerships around the globe give the United States an unmatched advantage over our competitors. Maintaining and nurturing those relationships does not happen overnight but is a product of an enduring effort to build trust and confidence between nations. Twenty eighteen marks the 25th anniversary of the National Guard's State Partnership Program (SPP), and it is worth reflecting on the important contributions the SPP makes in enabling the US and its allies and partners to provide security and stability around the world.

The SPP is an innovative and cost-effective security cooperation program that connects the National Guard with the militaries of partner nations around the globe. Guard units conduct military-to-military engagements with partner nations in support of defense security goals and also leverage societal relationships to build personal bonds and enduring trust. The SPP is not designed to make other militaries self-sustaining. Rather, the goal of the SPP is developing and maintaining important security relationships between the United States and other nations sharing a long-term view of common interests.

As outlined in the National Defense Strategy (NDS), strengthening and evolving our alliances and partnerships is a secretary of defense priority as we look to meet shared challenges and potential threats. The National Guard is playing an integral role in this effort. At the request of US ambassadors in foreign countries, the National Guard forges its unique SPP relationships by integrating its activities with the strategic goals of combatant commands and chiefs of US missions. With the recent announcement of the partnership between Brazil and New York, the SPP currently partners with 81 nations and is a scalable and adaptable program preserving critical partnerships as well as developing new ones with nations that are ready to partner for a more secure future.

A Volatile Security Environment

Geopolitical changes in the last decade have brought greater concern over strategic competition. The United States is still the most capable military in the world, but our adversaries seek gaps and seams to exploit weaknesses, some through non-kinetic means, including the so-called

gray zones of warfare. We are seeing strategies that use all instruments of national power to compete within every aspect of the diplomatic, informational, military, and economic spheres. China is now a dominant player in the global economy, which has allowed it to increase spending for the People's Liberation Army and assert territorial claims in the South China Sea. Russia seeks to revise the international order and change longstanding universal norms through force and unconventional means that combine military action, coercive economic tools, diplomacy, and disinformation campaigns. Iran and its Revolutionary Guard Corps are attempting to dominate the Middle East through support of rogue organizations and their own military operations. Despite recent developments, security on the Korean Peninsula remains an international concern. Nonstate actors throughout the world with more sophisticated capabilities present new dangers abroad and in the homeland. All of these threats differ in geography and scale, making unilateral action a risky proposition that would stretch the capabilities of the US and its military. Without allies and partners, these threats become more difficult to deal with. In a competitive world with diverse threats, the US must attract and work with allies as a means of achieving a competitive advantage and decisive edge.

Standing Together: The Value of Alliances

Like-minded nations committed to collective defense provide a number of critical benefits—particularly strong economies so essential to security. When putting an economic value on our partnerships and alliances, the aggregate GDP for the US and our European and Pacific allies is $44.4 trillion, two and a half times the US GDP alone. Additionally, 13 of the top 20 militaries in the world are close US allies with a total of $1 trillion in defense spending and approximately four million personnel. Beyond direct military and economic power, allies offer additional perspectives on courses of action, provide diplomatic and political support in international forums, contribute essential logistical and transit hubs, and, as a collective group, add legitimacy to the use of military force. This level of political, economic, and military might is underwriting the ability of our alliances to share the burdens of promoting global peace and security.

Allies and partners are force multipliers in terms of manpower, capabilities, and resources. Ultimately, in any armed conflict, allies and

partners training together regularly substantially increase their combat capability. However, working with others is not always easy. While states may share common interests, they don't always have identical values or views. Nonetheless, the benefits of engaging allies and partners far outweigh the cost or occasional disagreement. Successful alliances share burdens and invest time and effort in creating enduring relationships. They are built on cultural understanding and a respect for each other's sovereignty. Alliances based on such characteristics are far more effective than those that are transactional, coercive, or intimidating. The SPP promotes healthy, enduring partnerships committed for the long term, beyond the completion of initial objectives. East-Central Europe after the fall of communism serves as a great example.

Founding of the State Partnership Program

With the fall of the Berlin Wall in 1989 and the collapse of the Soviet Union in 1991, a number of states chose a path toward democratization and integration when Eastern Europe broke free of authoritarian rule. The US sought to assist these states in reforming their militaries as a means to institutionalize democratic processes, promote respect for the rule of law, and reinforce healthy civil-military relations. The best way to create a Europe whole and free was to ensure new democracies built the institutions and capabilities that would support their individual reform efforts.

In 1992, US European Command initiated military-to-military engagements to assist in reforming the militaries of former Soviet-controlled republics and Warsaw Pact countries through an initiative called the Joint Contact Team Program (JCTP). The National Guard played a central role in these engagements. Each country desired to form reserve-based forces to promote democratization through civilian control of the military while also appearing less threatening to Russia. The National Guard had the additional advantage of being well suited to cooperate on issues such as disaster management, search and rescue, military education, and civil-military relations, areas of particular interest to the emerging democracies. The SPP, an outgrowth of the JCTP, signed its first partnerships in April 1993 with Estonia, Latvia, and Lithuania partnering with Maryland, Michigan, and Pennsylvania, respectively.

In forming these new relationships, economic, demographic, and military size were some of the factors considered so the partnerships would

be advantageous for both sides. Small states such as Maryland partnered with Estonia. Later, Illinois, with its large Polish-American community, matched up with Poland. Oil states such as Oklahoma and Azerbaijan were aligned together, while the state of Georgia teamed up with the country of Georgia. In the case of Iowa's partnership with Kosovo, increased ties spawned the opening of Kosovo's first foreign consulate in Iowa, which helps foster economic and business ties.

In each of these partnerships, the SPP went well beyond military aspects benefitting both partners in other sectors of society. The SPP currently has nine partnerships in the Indo-Pacific region that focus on broad and diverse engagements such as peacekeeping training, humanitarian assistance, disaster relief, search and rescue exchanges, noncommissioned officer development, and medical exchanges. State partnerships have also flourished in Latin America, with 24 nations participating in the program. Currently, the SPP has relationships throughout the world with nations such as Togo, Belize, Tonga, and Kyrgyzstan, creating opportunities for future engagement and mutual assistance.

The Broader DOD Strategy

The US National Defense Strategy provides three key elements in its efforts to strengthen alliances: uphold a foundation of mutual respect, responsibility, priorities, and accountability; expand regional consultative mechanisms and collaborative planning; and deepen interoperability. The Department of Defense has multiple tools to achieve these objectives, including security assistance; security cooperation; military-to-military leader and staff engagement; promotion of regional cooperation; participation in multinational exercises; and agreements on facilities, basing, and transit of forces. The operational National Guard is fully integrated with the National Defense Strategy through these activities as a part of the joint force and adds a unique contribution through the SPP. At a time when resources are being shifted and readiness is essential for strategic competition, the SPP provides DOD with a scalable and tailored approach to security cooperation and partner enhancement.

Regardless of geographic location, the National Guard consults and coordinates with combatant commanders, US country teams, and the host nations to understand the full range of issues affecting the partner nation. SPP events are led by the respective state adjutants general, who seek maximum impact of the SPP engagements by developing a

program that is in the interest of both countries. In addition, the majority of SPP partner nations have National Guard Bilateral Affairs Officers (BAO) living in the partner nation, participating in the development of an embassy's engagement plan, and ensuring SPP events that are conducted by combatant commands are consistent with the ambassador's intent.

One strategic benefit resulting from the SPP is many of our partners who began as security consumers evolved into global security providers. Seventy-nine times, our partners have co-deployed with the National Guard in Afghanistan and Iraq. For example, the Illinois and Poland partnership is one of the most robust and successful security cooperation partnerships in Europe. Poland and Illinois signed their partnership in 1993 with the goal of professionalizing Polish forces, bringing their forces up to NATO standards, and providing peacekeeping training. Poland was accepted as a member of NATO in 1999, and since the beginning days of the wars in Iraq and Afghanistan, Poland has co-deployed with the Illinois National Guard multiple times and contributed thousands of troops. Today Polish forces along with the Illinois National Guard are at the forefront of US deterrence and assurance activities in East-Central Europe.

Beyond the number of exercises, deployments, and military-to-military events, another striking feature of the SPP is how it cultivates personal relationships that enhance, influence, and promote access. Nowhere was this more evident than when Russia illegally annexed Crimea and fomented an armed conflict in eastern Ukraine. Chiefs of defense from Ukraine and other states bordering Russia were quick to engage with their partner adjutants general, providing invaluable information to the Joint Chiefs of Staff and informing the US response.

The Future State Partnership Program

The SPP is future focused and adaptive to geopolitical changes. As we celebrate the 25th anniversary of the SPP, we have seen the program evolve from assisting nations in developing more modern and professional militaries functioning under civilian control to partnerships that look to deepen interoperability with complementary capabilities and forces. Beyond the military benefits, we have witnessed the fruits of these relationships as they help the United States maintain and grow its alliances across the globe through enduring and personal relationships. What began as a program of 10 partnerships in Eastern Europe has

spread across five continents and currently encompasses approximately one-third of the nations in the world.

The National Defense Strategy's priorities include expanding Indo-Pacific alliances and partnerships, fortifying the trans-Atlantic NATO alliances, forming enduring coalitions in the Middle East, sustaining advantages in the Western Hemisphere, and supporting relationships to address significant terrorist threats in Africa. Our state partnerships are located in all of these strategic regions as a part of the "long game." For instance, the Indo-Pacific region will continue to play an important role in the global security environment. Encompassing three of the most populous nations in the world (China, India, and Indonesia), two of the three largest economies in the world (China and Japan), and home to several of the largest militaries in the world, this vast area and its partnerships and alliances will be paramount in ensuring a stable and peaceful region. The African continent with its vast population and resources is also a potential area for future partnership growth.

As the security environment continues to change, the State Partnership Program will adjust and develop accordingly. In a recent example from the evolving cyber domain, Estonia, Latvia, and Lithuania worked with their National Guard partners in Maryland, Michigan, and Pennsylvania respectively in a USEUCO-hosted cyber defense exercise preparing for a cyber incident that requires a multinational response. In working with partners that can assist in other regions of the world, Serbia and its partner, the Ohio National Guard, travelled to Angola to conduct a trilateral medical exchange. These are just a few compelling examples that show the SPP serves as a cost-effective strategy that enhances security capabilities while promoting essential pillars of a free and democratic society.

In its initial stages, the SPP forged relationships in Europe that still exist today and are stronger than ever. In our wars in Afghanistan and Iraq, our partner nations co-deployed with their partner states leveraging forces and capabilities where the sum was greater than its individual parts. The SPP will preserve the building blocks of its foundational partnerships while continuing to forge partnerships that are every bit as important as developing next-generation weapons. The importance of allies and partners that share common values and interests was succinctly described by Defense Secretary James Mattis when he stated, "nations with strong allies thrive, while those without stagnate and wither." The National

Guard has a unique role in this process through the SPP, one that provides a high return on investment. We work with our partners not only as one military to another but also as American citizens to partner citizens. When we establish partnerships this way, employing the full range of skills resident in the National Guard, we are preparing ourselves, our allies, and our partners to confront the full range of threats and in turn create a more secure future in the twenty-first century. SSQ

Gen Joseph L. Lengyel, USAF
Chief, National Guard Bureau

Confidence Building Measures for the Cyber Domain

Erica D. Borghard and Shawn W. Lonergan[1]

Abstract

There is a growing debate among scholars and practitioners in the cyber conflict field regarding the extent to which the cyber domain is likely to be characterized by inadvertent escalatory spirals and arms races between increasingly cyber-capable states. Historically, technological innovation or geopolitical dynamics have propelled states to form confidence building measures (CBM) or create arms control regimes to institutionalize constraints on offensive military technology and guard against inadvertent conflict and escalation. We argue that cyber CBMs could blunt some of the factors that contribute to crises and escalation. Given the absence of arms control regimes for the cyber domain, cyber CBMs could be used to mitigate the risks to stability between states and possibly change the incentives that could lead to crises. In assessing current cyber confidence building initiatives, this article creates a novel framework to better understand these efforts. It also identifies limits of cyber CBMs and provides prescriptions for new steps in cyber CBMs to enhance mutual security and guard against inadvertent conflict stemming from cyber operations.

❋ ❋ ❋ ❋

There is a growing debate among scholars and practitioners in the cyber conflict field regarding the extent to which the cyber domain is likely to be characterized by inadvertent escalatory spirals and arms races

Erica D. Borghard is assistant professor at the Army Cyber Institute at the United States Military Academy at West Point and a Council on Foreign Relations International Affairs Fellow. She holds a PhD in political science from Columbia University.

Shawn W. Lonergan is a research affiliate of the Army Cyber Institute at the United States Military Academy at West Point and a cyber officer in the US Army currently assigned to US Cyber Command. He holds a PhD in political science from Columbia University.

between increasingly cyber-capable states.[2] Furthermore, policy makers find themselves grappling with competing incentives. On the one hand, actions taken to limit the use of destructive cyber weapons or the targeting of civilian infrastructure could provide some assurances for digitally dependent societies. On the other hand, policy makers are loath to support self-imposed limits on capabilities in an environment where future technological trends are uncertain and adversary capability and motivations are difficult to discern and predict. Historically, technological innovation or geopolitical dynamics have propelled states to form confidence building measures or create arms control regimes to institutionalize constraints on offensive military technology and guard against inadvertent conflict and escalation. But to what extent can cyber CBMs be used to mitigate the risks to stability between cyber powers? Is it possible to change the incentives that could lead to crises? We argue that, while there are fundamental attributes of operating in the cyber domain that impede efforts to build effective and enforceable arms control regimes, CBMs, which are distinct from arms control, could blunt some of the factors that contribute to crises and escalation. In assessing current cyber confidence building initiatives, this article creates a novel framework to better understand these efforts and to identify areas that are not being addressed and remain as potential flashpoints that could exacerbate tensions and spark conflict.

First, we conduct a brief discussion of the role of CBMs in fostering stability and reducing the risk of inadvertent escalation and situate their development in a historical context. Next, we review the hurdles to establishing arms control regimes for the cyber domain and demonstrate how, despite these hurdles, states have demonstrated a willingness to enter into CBM agreements to clarify acceptable behavior in cyberspace, avoid inadvertent conflict, and stabilize potential disruptions to international security stemming from cyber operations. We use Cold War frameworks for evaluating CBMs as a benchmark for developing realistic CBMs for the cyber domain in light of the latter's distinct characteristics.[3] Specifically, cyber CMBs must take into account the multi-stakeholder nature of the cyber domain, as distinguished from other domains of warfare; the different types of information that should be shared for CBMs to be effective; the dual-pronged nature of the objectives of CBMs, which could be used not only to avoid cyber conflict, but also to bolster norm development efforts; and the administration and main-

tenance of cyber CBMs through unique mechanisms such the United Nations Group of Governmental Experts (GGE) and the Organization for Security and Co-operation in Europe (OSCE). The article concludes by identifying the limits of cyber CBMs and provides prescriptions for next steps in cyber CBM development. Importantly, there are additional measures that could be taken to enhance mutual security and guard against inadvertent conflict stemming from cyber operations.

Confidence Building Measures as Reassurance

When arms control is perceived to be a bridge too far between adversaries that hold many points of disagreement and mistrust, yet both acknowledge the potential for inadvertent conflict, decision makers have employed confidence building measures in lieu of establishing arms control regimes.[4] The post–Cold War literature on international law and institutions has reconsidered the value of soft law and information norms and institutions in terms of their contributions to fostering stability and reassurance between strategic rivals.[5] Like arms control, CBMs may constitute bi- or multilateral agreements or take the form of unilateral action. As trust is built between parties, CBMs may give way to more formalized arms control agreements due to the role the former have in reassuring a potential adversary—though this is by no means determinative. According to this logic, CBMs are a form of reassurance that seeks to demonstrate intent among rivals, therefore (ideally) conveying a desire to maintain the status quo and foster a sense of security between otherwise threatened states.[6] Indeed, they are designed to ensure crisis situations, routine tensions, or localized conflicts between states do not become inadvertent lighting rods that spark a general war.[7] As CBMs are only intended to signal the aim of military activities, they do not change the overall balance of power between adversaries. Rather, CBMs are simply designed to preserve a fragile stability in the context of potentially intense security competition between states.

Confidence building measures provide reassurance through four mechanisms. First, they seek to demonstrate nonaggressive postures by increasing the transparency of military actions. This could occur, for instance, through inviting designated observers or the public to witness events that otherwise could be construed as threatening.[8] Second, they place self-imposed limits on security activities, such as military exercises, that could cause another state to feel threatened. Third, CBMs often op-

erate in a time of crisis by enabling a vital communications link between adversaries. In other words, CBMs contribute to stability and détente by helping convey intent behind a state's unilateral security policies and actions that would otherwise be cloaked in uncertainty.[9] Finally, CBMs inject predictability into a potential adversary's actions and, therefore, serve as an early warning function. Specifically, CBMs make it easier for another state to detect a deviation from an established norm of behavior and thus enable it to take measures in advance to mitigate the damage stemming from a surprise attack.[10] Though CBMs do not replace the vital role of national technical means of intelligence in assessing another actor's capabilities and intent, they supplement it by enabling a fuller picture of the significance of a military policy or action than otherwise would have been available.[11]

During the Cold War, there were concerns among scholars and policy makers that CBMs could be used to mask a surprise attack, but these were overcome due to the mutually paramount interest of avoiding inadvertent conflict that could spiral into nuclear war.[12] Specifically, governments mitigated these apprehensions through voluntarily implementing more, rather than less, transparency to reassure rivals about the intent behind a military action or policy. Though CBMs can be unilaterally implemented, they often take the form of multi- or bilateral agreements so all parties can understand the level of transparency necessary to foster mutual and reciprocal confidence in the intent behind another actor's security policy or action. The Helsinki Final Act in 1975 is a case in point.

CBMs in Historical Context: The Helsinki Final Act

CBMs need not be formalized in international law or codified in a formal agreement to be effective. While they sometimes become institutionalized over time as they evolve from state practice, CBMs can have an independent effect on stability and cooperation through informal and norms-based mechanisms.[13] The exemplar for all subsequent CBM efforts was the Final Act of the Conference on Security and Co-operation in Europe that took place in Helsinki, Finland, in 1975.[14] We use the Helsinki Final Act, therefore, as our benchmark for assessing cyber CBMs. Broadly speaking, the 1975 conference had the goal of creating stability, noting "the need to contribute to reducing the dangers of armed conflict and of misunderstanding of military activities which could give rise to apprehension, particularly in a situation where the

participating States lack clear and timely information about the nature of such activities."[15] The Helsinki Final Act, initially signed by 35 states, sought to foster stability by addressing issues that strained East-West relations on topics ranging from sovereignty to freedom of the press and cultural exchanges.[16] Arguably, no part of the agreement has been as closely scrutinized as the establishment of CBMs between the signatories. The original act stipulated voluntary reporting with at least a 21-day prior notification of military maneuvers that would exceed over 25,000 troops and that would occur within 250 kilometers from a state's border.[17] The provision also enabled the exchange of observers for these maneuvers as well as the hosting of military delegations.[18]

The Helsinki Final Act noted that "the experience gained from the implementation of the provisions . . . together with further efforts, could lead to developing and enlarging measures aimed at strengthening confidence" and as such created a framework for follow on meetings. The first of these occurred in Belgrade in 1977, followed by Madrid in 1980, Stockholm in 1984, and Vienna in 1986.[19] Each of these conferences comprised multiyear efforts that endeavored to innovate new and creative means to demonstrate intent and promote transparency in response to changing security policies and technology. By the time the 2011 Vienna Document was finalized, CBMs had expanded to include the annual exchange of military information such as organizational charts, manning and equipment numbers, unit locations, defense budgets, and information relating to the employment of new weapon systems.[20] Furthermore, additional CBMs included the development of more robust communication regimes that could operate in a time of a crisis as well as for routine exchanges of officers and demonstrations of new major weapon systems. The original provisions for troop notifications were also refined to require at least a 42-day warning of exercises of at least 9,000 troops or 250 battle tanks. There were also controls addressing the number of major exercises that a state could perform per year and restrictions on the number of short-notice inspections of another signatory's military maneuvers and other troubling sites that a state could annually perform.[21]

The Helsinki Final Act illustrates how CBMs could offer a means to mitigate the risk of inadvertent conflict even under conditions when formalized arms control agreements that seek to change the incentives for military action are not feasible. CBMs do so through facilitating increased transparency and openness surrounding a state's security policies

and operations. However, changes in security requirements, polices, and technology suggest that, for CBMs to promote lasting stability, they must be reassessed and amended on an iterative basis, as was the case throughout the Cold War and in the ensuing years.

Initial Steps Toward Cyber Confidence Building Measures

CBMs were neither the sole nor most effective means of cultivating stability between nuclear-armed rivals during the Cold War. Mutual fear of miscalculation and escalation drove the United States and the Soviet Union to form arms control regimes.[22] Arms control can alter the incentives for the use of offensive military technologies, limit the damage to states in the event these technologies are used, and contribute to stable interstate relations, even between adversaries. However, there are reasons to be less sanguine about the feasibility of arms control for cyberspace.

First, several fundamental characteristics of operating in cyberspace confound the establishment of effective arms control agreements. Specifically, arms control in cyberspace is difficult due to the ambiguity surrounding the strategic balance of cyber weapons and the measurement of relative capabilities of cyber powers, the lack of transparency and issues with monitoring for compliance, the dynamic nature of the methods and means of cyber operations, uncertainty about the military implications of technological innovations, and problems of assigning and enforcing responsibility for cyber operations or capability development.[23] Put simply, this endemic uncertainty means governments do not want to find themselves at a strategic disadvantage if and when a future cyber war breaks out. Furthermore, the offensive parity that exists between many states (and even nonstate actors) in the cyber domain is likely to heighten these fears of being in a potential position of military disadvantage.[24] Indeed, while serving as chairman of the Joint Chiefs of Staff, Gen Martin Dempsey noted that the cyber domain is the only domain where the United States possesses peer competitors.[25] Second, cyber capabilities have been "weaponized" to deliver effects across two broad categories: to support traditional kinetic war fighting and for the purposes of punishment, subversion, or coercion. The more significant source of instability in cyberspace lies in the latter category rather than the former. Specifically, a key source of instability lies in exploiting national economies and critical infrastructure and manipulating the public's perception of the integrity of essential systems via cyber means to achieve

strategic objectives. Therefore, traditional concepts of arms control that limit the "quantity" or "quality" of cyber arms, for instance, are poorly suited to address the key contributors to strategic instability between cyber rivals.

Despite the significant hurdles to arms control for cyberspace, states have already taken steps to develop cyber CBMs through multi- or bilateral agreements to create mechanisms to share information about their intended uses of cyberspace and law enforcement information concerning nefarious actors, as well as to share information in a crisis. This is because governments have recognized that the secretive nature of cyber operations and the difficulties of signaling in cyberspace can be destabilizing to interstate relations, increasing tensions and the risk of inadvertent conflict. Therefore, though it is impossible to completely eliminate the incentives for actors to misrepresent or disguise their aggressive cyber actions, CBMs that facilitate a dialogue between states have become a first step toward mitigating the destabilizing effects posed by the cyber domain.[26] For example, in the past few years, several countries, such as the United States and Russia, entered into bilateral agreements establishing hotlines to guard against misunderstandings stemming from cyber operations in a crisis. During the fall of the 2016 US presidential election, President Obama used the hotline connection between the Nuclear Threat Reduction Centers, which was bilaterally designated to be used for cyber related events three years prior, to convey to President Putin that the laws of armed conflict applied to cyberspace.[27] The efficacy of President Obama's use of the hotline remains uncertain; Jeanette Manfra, the National Protection and Programs Directorate (NPPD) Assistant Secretary for the Office of Cybersecurity and Communications (CS&C) at the US Department of Homeland Security (DHS), disclosed in February 2018 that the Russians succeeded in penetrating a small number of state election systems, though it is not known if these breaches occurred prior or subsequent to President Obama's call.[28] Thus, in lieu of banning specific capabilities or seeking an agreement that depends on verification, states have sought to use informal, voluntary measures to grapple with the fundamental drivers of instability between cyber rivals by promoting clarity of the domain and enabling effective crisis management.

In the multilateral context, several international organizations have spearheaded attempts to develop cyber CBMs, with varying degrees of

success. Of particular note are the UN GGE and OSCE, which sponsored the original Helsinki Final Act. Additionally, beyond the OSCE, there have been other efforts to foster cyber information sharing and confidence building between states. Groundbreaking regional agreements such as the *African Union Convention on Cyber Security and Personal Data Protection*, the Organization of American States' *Inter-American Strategy to Combat Threats to Cybersecurity*, and the *ASEAN Regional Forum Work Plan on Security of and In the Use of Information and Communications Technologies* have all focused on addressing regional security needs stemming from cyber threats.[29] Similarly, there have been efforts by economic organizations, such as the Groups of 7 and 20 (G7 and G20, respectively), to promote norm creation that reflects the interests of the largest economies in the world.[30] Both the G7 and G20 declarations explicitly express support for the UN GGE and OSCE CBM development efforts but restrict their focus to the establishment of normative state behavior related to the use of cyber capabilities.

Despite representing the most advanced efforts by the international community to develop cyber CBMs, both the GGE and the OSCE have made only halting progress to arrive at mutually agreeable measures to promote stability and transparency between states in the cyber domain. Within the UN, the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security was convened in 2004 to discuss potential areas of cooperation.[31] A year later it failed to reach a consensus and no report was submitted. A second GGE was convened in 2009, and, after four meetings over the course of two years, it devised the first set of cyber CBMs that focused on information sharing, reducing risk to critical national infrastructure, and devising a set of commonly accepted terms; it also provided recommendations for continued dialogue.[32] The CBMs were expanded by a third and fourth round of GGE panels that concluded in 2013 and 2015, respectively, with notable agreements regarding the application of international law and the concept of sovereignty to cyberspace as well as state responsibility for attributed cyber acts.[33] However, the most recent GGE round in 2016–2017 failed to build on the success of previous iterations. For instance, while the 2013 GGE promulgated that international law, especially the UN Charter, is applicable to the cyber domain, members at the 2017 GGE summit were unable to arrive at a consensus regarding *how* international law should apply. Specifically, the

breakdown of the talks centered around questions of how concepts such as sovereignty, the right to self-defense, and appropriate countermeasures apply to cyberspace, with some members taking the position that it was premature to address these issues given the dynamic nature of the domain.[34] It is possible that the most recent GGE round was doomed to fail when assessed against unrealistically high expectations leading up to it. Ongoing processes of interpreting and applying international law are chronically difficult.[35] However, the 2017 GGE summit produced a regression from previous agreements that international law itself applied in the first place, not simply a failure to push forward the agenda. Relatedly, the Permanent Council of the OSCE directed efforts in 2012 to begin drafting CBMs specific for cyberspace, noting that CBMs were necessary to "enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs."[36] These efforts led to the drafting of additional CBMs in 2013 and a more comprehensive list in 2016.[37]

While governments have taken initial efforts to establish cyber CBMs, current academic work on the topic is at a nascent stage. Though multiple scholars have noted the need to avoid inadvertent conflict, few have postulated specific measures that states could implement to move in that direction.[38] Herbert Lin attributes this dearth of measures to the revolutionary nature of the domain. In Lin's words,

> Meaningful analogs to . . . [confidence building] measures in cyberspace are difficult to find. For example, there is no analog to large-scale troop movements—cyber forces can be deployed for attack with few visible indicators. Agreed conventions for behavior, such as "rules of the road," do not cover intent, and in cyberspace, intent may be the difference between a possibly prohibited act, such as certain kinds of cyberattack, and an allowed one such as cyber espionage.[39]

Tughral Yamin notes this dilemma but argues that, "A necessary precondition for developing cyberspace CBMs is to have good national cyber security policies and practices, particularly for the protection of critical infrastructure."[40] Yamin does not quantify the requisite level of policy creation necessary for the effective formation of CBMs. However, he does make an important contribution by noting that institutional development of cybersecurity organizations within a state are necessary, in part, because they play an important role in knowledge generation and information sharing in a domain that is difficult to conceptualize.

Absent institutions that assist in information sharing of vulnerabilities, known threats, remediation strategies, and national policies and attitudes for approaching the cyber domain, it is unlikely that actors within and external to a state would understand the risks posed by cyber operations. Indeed, there is an *a priori* need to deliberately cultivate an epistemic community comprised of multidisciplinary and multinational academics, policy makers, the private sector, and operators/planners to arrive at a consensus on pivotal concepts and definitions that drive how actors operate in and through cyberspace similar to the epistemic community that developed during the Cold War to grapple with the implications of nuclear weapons. Additionally, in a thought piece on cyber CBMs, Jason Healey, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd note that, given the plethora of actors in cyberspace, a multistakeholder approach that incorporates the private sector and other nonstate actors is vital to the development and adoption of any measure.[41] However, the implications of this analysis focus on the influence of domestic-level veto players on a state's international bargaining position with respect to the creation of specific CBMs. Therefore, there are opportunities for scholars to make conceptual and analytical contributions to cyber CBM development to better inform policy making.

A Framework for Cyber Confidence Building Measures

The objectives of CBMs—to foster exchanges that help states avoid conflict, rather than actually change the military balance of power—may make these mechanisms more amenable to application to the cyber domain than arms control. Indeed, continued efforts by governments and international organizations to support the development of cyber CBMs are important because they represent the first step in injecting stability and transparency into a domain characterized by secrecy and uncertainty. However, even the most "successful" efforts at developing CBMs have thus far been disappointing. Developing a framework to conceptualize and evaluate different categories of cyber CBMs, taking into account how cyber CBMs are likely to differ from previous types of CBMs, is a necessary foundation to support future CBM development efforts. Therefore, as an initial contribution, we use a model for categorizing CBMs developed during the Cold War as a benchmark for assessing the extent to which it is applicable to the cyber domain, identifying important gaps, and developing cyber-specific approaches

for evaluating CBMs. Johan Holst argued in 1983 that CBMs come in four varieties (information, notification, observation, and stabilization) and noted that some measures may encompass several of these categories.[42] Information measures involve the sharing of defense-related information, such as budgets and organizational structures, between interested parties. Notification pertains to the advanced warning of major military activities within a geographic concentration, such as a military exercise or a major change in force distribution. Observation measures include activities such as inviting potential adversaries to physically observe military exercises, the fielding of new weapon systems, or other related military activities firsthand. However, as Holst notes, stabilization measures were multifaceted and encompass three dimensions: "crisis stability (relative absence of pressures to take early military action to forestall moves by the adversary); arms-race stability (relative absence of inducement to expand military forces); and political stability (relative absence of pressures for breakdown of the international order)."[43] Applying Holt's framework to the cyber domain, we identify three different categories of information CBMs (with the exception of crisis stability), incorporating into our analysis important factors that were not considered in Holt's framework; demonstrate why the notification, observation, and stabilization categories of CBMs are likely to be particularly difficult and complex in cyberspace; and account for the development of administrative measures that are designed to promote transparency and the role of the hosting institution. We organize all of the existing OSCE and GGE cyber CBMs into our new framework, which can be found in the appendix.

Three Categories of Information CBMs for Cyberspace

When Holt developed his framework for organizing CBMs during the Cold War, he envisioned the information category as simply an exchange of defense-related data. However, this category should be disaggregated given the diversity of threat actors and the unique complexities associated with operating in cyberspace. For instance, the multistakeholder nature of cyberspace and, in particular, the fact that the private sector owns and operates the vast majority of its infrastructure and is the primary target of cyberattacks means that including private industry as participants in CBMs is essential for their relevance and success.[44] Private actors may have better information than governments about adversary tactics, tech-

niques, and procedures (TTP) and capabilities. Relatedly, private actors already participate in information sharing independent of government actions. For example, private security firms are often quicker to publicly attribute malicious behavior than governments.

Therefore, information-based cyber CBMs should be categorized into three components: threat actor, security, and use.[45] First, the sharing of threat actor information identifies threat actors and emerging methods and means for exploitation and attack. This could include sharing information that pertains to specific online personas, country profiles, threat signatures, and TTPs as well as law enforcement information about state and nonstate actors. This type of threat actor information sharing contributes to stability by enabling states to proactively counteract malicious actors and activities in cyberspace directly, rather than defend solely within the perimeter of one's network. An example of this is the December 2013 CBM developed through the OSCE, encouraging states to establish "modern and effective national legislation to facilitate . . . time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating states, in order to counter terrorist or criminal use of ICTs."[46]

Second, security information pertains to the dissemination of system vulnerability reports as well as instructions for remediation. This contrasts with threat actor information in that it is oriented around systems and networks to be defended, rather than threat actors. Security information contributes to stability by enabling defenders to take proactive measures to protect networks and systems. A common element of both the GGE and the OSCE list of measures is a reliance on computer emergency response teams (CERT) for the dissemination of both threat and security information. Since the first CERT was created at Carnegie Mellon University in 1989, the concept has expanded to include over 420 teams operating in over 80 countries that mutually promote security cooperation by sharing technical vulnerability and remediation information.[47] Parties to the 2015 GGE, for instance, agreed to share information through the CERT infrastructure about "vulnerabilities, attack patterns and best practices for mitigating attacks."[48] For example, the US National Institute of Standards and Technology (NIST) publishes publicly accessible, real-time information about ICT vulnerabilities that defenders can use to bolster security.[49]

Third, use information incorporates Holst's conceptualization of the sharing of state-level defense related materials, such as doctrine and national policies. However, for the cyber domain this category should be broadened to incorporate other stakeholders, particularly the private sector as participants in CBMs. The recognized influence and role of the private sector is already evident in both the GGE and OSCE CBMs that address the sharing of information relating to "national attitudes" and views from both public and private sources.[50] An example of this is the July 2015 GGE CBM in which parties agreed to "the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs . . . and national organizations, strategies, policies, and programmes relevant to ICT security."[51] These CBMs reflect the fact that the actors in this space are not solely states and, therefore, information about the uses of cyberspace must extend beyond traditional state actors and should necessarily include information provided by—not simply about—private actors.

Furthermore, in addition to enhancing transparency regarding motivations and intent, several of the information-use cyber CBMs also serve the purpose of tracking and driving norm emergence and development. There is an essential interdependence and complementarity between CBMs and norms in international politics. CBMs can contribute to norms through creating shared expectations about appropriate behavior (such as acceptable targets) or capability development (such as offensive weapons); norms, in turn, can help foster stability through facilitating identification of defection.[52] Some cyber CBMs, for instance, are designed to share information concerning promoted norms of state and societal use of the internet within its borders, such as a desire for a free and open internet or a more closed protectionist posture, as well as other information, such as what it considers to be critical infrastructure.[53]

Finally, there are administrative measures that have been instituted to maintain cyber CBMs and disseminate information that reflect unique needs of the cyber domain and, therefore, are beyond the scope of Holt's initial framework. This also reflects the interdependence of CBMs and norms, because the latter are also often promulgated and propagated through institutions.[54] Indeed, private sector actors, such as global financial services firms, have used the G7 and G20 as forums to advocate for norms against targeting financial institutions. Specifically, these administrative measures are designed to enable the preservation and continued rele-

vance of the cyber CBMs, as well as the conservation of the respective organizations that facilitated their creation. Two notable examples of this are the CBMs developed in December 2013 through the OSCE in which parties, including allies and competitors, agreed to "exchange views using OSCE platforms and mechanisms" and "meet at least three times each year . . . to discuss information exchanged and explore appropriate development of CBMs."[55]

The Limitations of Notification, Observation, and Stabilization Measures for Cyberspace

While there is a plethora of information sharing CBMs that have a reasonable chance of successful adoption in cyberspace, significant hurdles remain for the acceptance of other categories of CBMs due to some of the same confounding factors that thus far have impeded the development of arms control regimes in the domain. This explains why there are few stability measures—with the exception of crisis stability—and no notification and observation measures present in both the UN GGE and OSCE frameworks.

Notification and Observation

Notification and observation CBMs are designed to provide advance warning of an exercise to other states so that the exercise is not misperceived to be preparations for an offense and to generally provide reassurance regarding motivations. However, notification of a cyber event or an exercise, to include allowing potential adversaries to observe it, is counterproductive in cyberspace due to the central importance of secrecy. Exercises would likely reveal information about vulnerabilities that an observing adversary could later exploit, or about capabilities or accesses against which an adversary could preemptively develop and employ defensive measures, making them ineffective. Thus, while some scholars such as Paul Meyer have promoted cyber CBMs calling for exchanges of personnel to observe "cybersecurity exercises" (defensive exercises) between potential adversaries, meaningful exchanges of this nature are unrealistic for the cyber domain given the necessary role of secrecy surrounding cyber capabilities and operations.[56]

Nevertheless, there is a role for observation of cyber exercises among allied states. Including allies as observers or even participants in defen-

sive exercises may be collectively beneficial for the purposes of building capacity. It could also demonstrate how an actor intends to respond to and remediate a cyberattack; help allies grow their own cyber defensive infrastructure, to include clarifying national authorities necessary to respond to a crisis; and identify opportunities for allies to augment and complement a state's efforts and enable a unified cyber defense. For instance, for the past 10 years NATO's Cyber Coalition cyber defensive exercise has grown to include over 700 participants from 25 allied countries.[57]

However, rather than solely observing defensive exercises, the spirit behind the exchange of observers in the Helsinki Final Act was to provide reassurance among potential adversaries regarding each other's offensive forces—in other words, those that could pose a threat to stability. However, building offensive cyber operations into existing defensive exercises is fraught with difficulties. Currently, cybersecurity exercises typically have a defensive focus and are used to identify both technical and procedural vulnerabilities on internal networks.[58] For example, most exercises spearheaded by the United States typically do not showcase the units that would conduct offensive operations or their capabilities and, therefore, are not designed to signal confidence in the command and control and efficacy of their offensive cyber forces.

It is possible to incorporate offensive actions into existing defensive exercises. For instance, a state could build into a defensive scenario a counterstrike that targets an infected server commanding the attack. However, any capability for access and attack that would be used in the scenario would most likely be limited to publicly available open source tools or would be fictionalized so as not to give away to the adversary the specific vulnerability in the target system it would be exploiting. Again, this reflects the fundamental requirement of secrecy for operational success. The ephemeral nature of offensive cyber capabilities and accesses means that revealing information about them effectively renders them moot.[59] If a state used real cyber weapons from its arsenal, it is likely that any observing state (including allies) would develop hardware and software upgrades to render the demonstrated capability inert. Similar to the paradox presented by cyber arms control, this may undermine the very stability CBMs seek to create. However, public notification of the successful execution of such an exercise could increase the adversary's confidence in the actor's ability to command and control cyber capabilities, thereby serving a confidence building purpose.

The Three Forms of Cyber Stabilization CBMs

Stabilization CBMs under Holst's framework come in three varieties: crisis, political, and arms racing. Crisis stability CBMs involve the exchange of points of contact and defense-related information and are designed to eliminate misperception. Unlike the political and arms racing CBMs, the crisis stability CBMs are cornerstones of the UN GGE and OSCE CBM agreements and are also prominent in several seminal bilateral agreements, as will be discussed in greater detail in the subsequent section.

Political stability CBMs. Achieving mutual consensus around political stability in cyberspace is one of the most significant hurdles for cyber CBMs and accounts for their absence from the current frameworks. The internet has created a relatively cheap and plausibly deniable avenue to undermine the political stability of other states—observed in spades in recent elections in Western democracies. Both authoritarian and democratic regimes view the internet as a medium to influence not only their own but also each other's citizenry. However, while there is some consensus on the utility of cyber capabilities to intervene in the political affairs of other states, there are sharp divisions between states—often reflected in differences in regime type—in terms of how they perceive the role and use of the internet internal to their physical sovereign borders. This tension has implications for stability.[60] Table 1 highlights the divergent view of the internet internal and external to the state according to regime type, although the latter is an imperfect but useful proxy for this distinction. These differences, we argue, are likely to confound the meaningful development of political stabilization CBMs across dyads of varying regime types.

Political stability CBMs are likely to be confounded by the varying perceptions of the internet internal to state borders on the one hand, and the profligate activities across cyber powers of all regime types to infringe on the sovereignty of their adversaries (or even allies) on the other hand. External to state borders, all major cyber powers perceive a strategic value in using cyber capabilities to conduct shaping operations in support of conventional war fighting and as a tool of coercion, influencing operations, and undermining political stability. The 2016 US presidential election, for instance, exposed how the internet could be used as a vehicle for a state (in this case, Russia) to intervene in the sovereign affairs of another through digital means to achieve strategic

Table 1. Contrasting Approaches to the Internet, by Regime Type

	View of the internet internal to their physical borders	View of the internet external to their physical borders
Authoritarian regimes	• Internet censorship and monitoring necessary for state security • States link allowing access to open internet as undermining regime stability	• Need for rigidly defined concept of cyber sovereignty • Internet affords a means to achieve strategic objectives through infringing on sovereignty of others
Democratic regimes	• Limited censorship across most democratic regimes; most restrictions deal directly with illicit activities[a] • Monitoring of online activity limited by civil liberty protections • Free and open access to the internet is in keeping with democratic ideals	• Access to a free and open internet may be a human right • Internet affords a means to achieve strategic objectives through infringing on sovereignty of others

[a]Variations exist among democracies as to the extent and means by which they block fake news and some forms of political speech

objectives.[61] Democratic governments, of course, also conduct information operations.[62] Democracies perceive a strategic benefit in the spread of democratic principles enabled by the internet.[63] For instance, the United States government has invested in the development of anonymity technology through the US State Department's Bureau of Democracy, Human Rights, and Labor, which historically has sought annual grants for the development of software that contributes to internet freedom.[64] It is also consistent with the US government spending "approximately $2 million annually during the past decade to help enable Internet users in China and other Internet restricting countries to access its websites, such as Voice of America and Radio Free Asia."[65]

Internal to state borders, most democratic states have viewed access to a free and open internet as consistent with broader democratic principles, with some going so far as to define such access as a human right and, therefore, a moral imperative for states to safeguard.[66] However, there are limits and nuances in these cases, as some democratic governments have taken steps to block or prevent access to illicit content or even limit some forms of political speech. For instance, following Russian interference in the 2016 US presidential election and pervasive information warfare campaigns in Europe, French President Emmanuel Macron advocated for new laws to ban "fake news" during elections, while Germany has enacted new hate speech laws (known as NetzDG) that levy fines on social media companies that fail to remove offensive content.[67]

While some democratic states have enacted measures to limit information on the internet, this stands in stark contrast to how authoritarian

governments view the internet within their borders. The latter perceive an open internet with fundamental suspicion, finding that it encroaches on their sovereign rights and threatens regime survival by undermining state efforts to control the population and by providing a forum for potential dissidents to coordinate and organize against the government. The most notable example of this is China's "Great Firewall," which is integral to the Chinese Communist Party's monitoring and control not only of its citizenry but also of anyone accessing the internet within Chinese borders. [68] However, other governments, such as those of Russia, Iran, and Turkey, employ similar mechanisms to surveil and control the domestic population. For instance, Russia—particularly in the wake of antigovernment protests in March 2017 that were enabled, in part, by online organizing and activism—attempted to institute limits on domestic access to the internet. The prior year, Russia invited Chinese experts on the Great Firewall to share information and expertise about internet control.[69]

An important wrinkle in the distinction between democratic and authoritarian governments is the role of private Western firms in enabling or collaborating with authoritarian governments to provide capabilities or enforce regulations that support internet control or sharing user information about citizens.[70] This again reflects the complexities of the multistakeholder nature of the internet. Facebook, for example, has shared user information with China through several data-sharing partnerships with parastatal Chinese electronics firms.[71]

Thus, the fact that the internet affords a means to directly reach the citizenry of another state in a way that was not previously possible has complicated the development of political stabilization CBMs. Many authoritarian regimes have moved to block this access through censorship, and many democratic governments struggle with finding policy solutions to thwart external or nefarious interference without sacrificing their democratic ideals. At the same time, all cyber powers benefit from the current ambiguities surrounding violating sovereignty via cyber means. Together, these factors prevent consensus regarding a set of political stabilization CBMs.

Arms racing stability CBMs. Arms racing stability CBMs are similar to more formal arms control agreements in that they typically limit the proliferation of certain technologies, but they are distinct in being entirely voluntary. In cyberspace, the viability of these types of CBMs is

tenuous. Arms racing stability CBMs appeared in the OSCE framework, but they were limited to periodic information exchanges intended to prevent misperceptions that could lead to arms racing behavior—specifically, pressures that encourage increasing forces or capability. Other types of self-imposed limits are unlikely due to the near-universal proliferation of cyber tools. For instance, many offensive tools are publicly available via online forums or for sale on the Dark Web, a section of the internet that is accessible through most web browsers and is known to facilitate illicit transactions.[72] The source code for Stuxnet as well as US National Security Agency capabilities for surpassing firewalls and other exploit technologies have been compromised and made publicly available by actors such as Shadow Brokers, among others; a tech-savvy actor could learn how to morph these into something even more advanced.[73]

Additionally, efforts have been made to control the export of information and communications technology that could support offensive operations through amending the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies to apply to cyberspace. However, the 2013 amendment was quickly met with industry opposition because the technology that supports offensive operations is also necessary to discover vulnerabilities that need to be patched, thus highlighting the offensive and defensive dual-use nature of many cyber security tools.[74] Indeed, this provision triggered significant resistance from the private sector, which felt it would inevitably and counterproductively lead to greater insecurity by placing restrictions on cybersecurity-related technology and activities, such as penetration testing technology, the sharing of threat information, and the use of multinational computer bug bounty programs.[75] This represents another example of the challenges of multistakeholder governance. To date, the provisions of ICT technology on cyber security capabilities of the Wassenaar Arrangement are still being refined both collectively by the Wassenaar Plenary and by member countries as they nest domestic regulation with their obligations under the Arrangement. For instance, in response to public feedback, the specific 2013 Wassenaar amendments that covered the training and employment of vulnerability detection systems were never implemented in the United States.[76] However, the 2016 Plenary relaxed or removed several of the contentious export controls given continued integration of these tools into consumer products.[77]

Since curbing the proliferation of technology is impractical, a potential alternative avenue for consideration would be for states to voluntarily curb the nonstate actors that take part in cyber operations by instituting domestic laws that make such activities illegal. Understandably, CBMs addressing criminal behavior were not part of Holt's framework because crime was perceived to be distinct from national security considerations. However, criminal activity and national security are profoundly interwoven in the cyber domain. States have used and provided safe haven to criminal actors as proxies to conduct plausibly deniable cyber operations at the behest of the state.[78] For example, in the spring of 2017 the US Department of Justice indicted members of the FSB, one of Russia's intelligence agencies, as well as two hackers who were alleged to have worked with the FSB to steal information from what is now reported to be 3 billion Yahoo user accounts in 2014. The hack was a joint endeavor by an intelligence agency and criminal actors and was carried out for both intelligence and criminal purposes, illustrating the nexus between these two forces.[79] Additionally, governments have directly engaged in crime via the cyber domain to circumvent economic sanctions or build military and industrial capability through intellectual property theft. North Korea has allegedly netted millions of dollars from cybercrime to evade the crippling effects of economic sanctions including, recently, the WannaCry ransomware attack in the spring of 2017 and financial theft operations targeting banks in the SWIFT network, including the Bank of Bangladesh in 2016 and Taiwan's Far Eastern Bank in 2017.[80]

While there have been ad hoc agreements between states to grapple with certain aspects of criminal activity in cyberspace (notably, the 2015 agreement between the US and China to refrain from economic espionage and intellectual property theft, discussed in greater detail below), there are no CBMs either in the GGE or OSCE lists that directly address cooperation on cybercrime. Most Western states have already institutionalized domestic laws criminalizing illicit cyber activity and have agreed to cooperate on the prevention of cybercrime by becoming signatories to the Budapest Convention on Cybercrime.[81] In contrast, the Russian Federation is the only member of the Council of Europe that has not signed the Budapest Convention.[82]

Opportunities and Recommendations

Extending the above analysis, we explore potential avenues for cooperation between rivals in cyberspace. Given recent disappointments at multilateral forums for cyber CBMs, we evaluate opportunities for bilateral CBMs when the conditions for effective multilateral CBMs are not met. Finally, we provide specific recommendations for new cyber CBMs.

Bilateral Cyber CBMs

Consistent with the CBM literature, the above discussion has focused primarily on assessing multilateral efforts to develop measures for cyberspace. However, there have been some notable examples of bilateral cyber CBMs outside of the GGE and OSCE, specifically between the US and Russia and the US and China.[83] These cases are consistent with the thrust of the analysis above: both of these dyads are cases in which there is a mutually recognized, non-negligible risk of escalation and inadvertent conflict in the domain and, therefore, would benefit from CBMs even as multilateral efforts involving the same countries have failed.

With respect to China and the US, some progress has been made in developing mechanisms that promote transparency and cooperation during peacetime as well as in a crisis. In 2015 Presidents Obama and Xi signed an agreement to abstain from cyber-enabled intellectual property theft for gaining a commercial competitive advantage, to exchange vulnerability and law enforcement information, and to create a working group to further discuss the UN GGE 2015 Report.[84] While advancing the agenda of the latter was clearly unsuccessful, as evidenced by the failed 2017 GGE summit, the 2015 agreement between the US and China did provide some clarity regarding how each state intends to use the domain (if only within the confines of economics). Furthermore, by mutually agreeing to refrain from economic espionage, the 2015 agreement enabled states to identify potential defections from a pattern of compliance. Most recently, following a meeting between Presidents Trump and Xi at Mar-a-Lago in April 2017, the US and China initiated another round of bilateral talks in October 2017 that reaffirmed the CBMs agreed to in 2015.[85] However, bilateral agreements have been limited to economic issues rather than political or national security ones. This likely reflects the enduring strategic value both governments perceive in developing cyber capabilities at a relatively low cost/risk for national security purposes. Moreover, the evidence is mixed with respect

to the extent of China's compliance with the 2015 agreement. In the March 2018 *Worldwide Threat Assessment*, the US Director of National Intelligence assessed that Chinese cyberespionage has decreased since the 2015 agreement but noted that "most Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide."[86] The findings of the March 2018 US Trade Representative report on China are similarly ambiguous about Chinese behavior post-2015.[87]

In a separate landmark agreement, in 2014 the US Department of Defense and the People's Liberation Army allowed the exchange of observers for major military activities and created a military crisis notification system utilizing the Defense Telephone Link between the two countries that was established in 2008.[88] Though neither of these agreements contained the term "cyber" or "ICT," it was understood at the signing that the catalyst was uncertainty stemming from the potential for inadvertent escalation during a crisis.[89] Again, however, the fact that this agreement did not directly address notification and observation for cyberspace highlights some of the major hurdles to effective cyber CBMs in these categories as much as it does the opportunities for cooperation. This reflects the delicate balance cyber powers such as the US and China must strike between preventing an inadvertent spiral into an unwanted conflict and protecting cyber assets and capabilities in the event they are needed if the former occurs.

In June 2013, the US and Russia created a working group within the context of the Bilateral Presidential Commission that sought to "promote transparency and reduce the possibility that an incident related to the use of ICTs could unintentionally cause instability or escalation."[90] Though the United States suspended its participation in the Bilateral Commission following Russia's invasion of Ukraine in 2014, the agreement mentioned three measures of note.[91] First was the continuous sharing of cyber threat information between the US CERT located at the Department of Homeland Security (DHS) and its Russian equivalent. Second was an agreement to utilize the Nuclear Risk Reduction Center (NRRC), first established in 1987, to facilitate inquiries about cybersecurity incidents. In the closing days of the 2016 presidential election, it was reported that the United States used the NRRC to deter Russia from directly interfering with US voting systems.[92] What is unique about this case is

not that the hotline was used but, rather, that it was used for deterrence rather than for détente. Finally, the commission also created a direct line between the White House's Cybersecurity Coordinator and the Kremlin's Deputy Secretary of the Security Council integrated into the Direct Secure Communications System that, like the NRRC, was first developed to manage nuclear crises during the Cold War. That said, while these are examples of confidence building measures developed with the intent to promote both peacetime and crisis stability, their efficacy remains to be seen. As noted earlier, the Russians succeeded in penetrating the voting systems of several states, although it is not known whether this occurred prior or subsequent to the use of the hotline.[93]

Specific Recommendations for New Cyber Confidence Building Measures

Based on the framework articulated in this article we identify several potential CBMs that could be adopted. Broadly speaking, these recommendations focus (not exclusively) on promoting stability. While there are non-negligible obstacles to CBM formation, particularly in reference to crisis and arms racing stability, the imperative to prevent unintended conflict escalation and promote crisis stability should compel policy makers to devote energy to this effort. Furthermore, crisis and arms racing stability CBMs are more practical to conceptualize and implement than notification, observation, or political stability measures. We submit the following five areas for CBM creation.

First, as an *a priori* CBM, stakeholders across adversaries and allies should work to build an epistemic community to work toward consensus on key concepts and definitions for cyberspace.

Second, the private sector should be systematically included as an actor in—not simply the subject of—information CBMs. This is particularly relevant for threat actor information CBMs because private actors play a central role in attribution, understanding adversary TTPs and capabilities, and information about their own vulnerabilities.

Third, states could make a commitment to state control of offensive cyber operations. Specifically, a CBM could articulate a concept of command and control (C2) for offensive cyber operations in which offensive operational capabilities remain in the hands of the military, while oversight and launch authorities reside with policy makers. This is similar to what many states have already done with respect to nuclear weapons. Cur-

rently, in cyberspace, many military organizations lack complete control of offensive cyber capabilities. This is due to several factors. First, often states rely upon proxy actors and maintain ambiguous C2 to buttress a government's plausible deniability of offensive cyber operations. Second, due to the often-superior capabilities of private actors, states may rely on civilian industry for expertise and development, or states operating parastatals may depend heavily on cyber espionage for economic growth. Relatedly, some states lack robust indigenous cyber capabilities, personnel, and the resources to produce them and are thus forced to employ cyber proxies to fulfill national security objectives.[94] This arms racing stability CBM could be built on existing efforts, such as the Budapest Convention, to standardize laws between states for prosecution of cyber crime and other types of nefarious cyber related activity. However, limiting nonstate actors that engage in cyber espionage and offensive operations may only be possible when the perceived risk of escalation outweighs the economic or plausible deniability benefits.

Fourth, and related to above, effort could be dedicated to a measure that addresses the delegation of authorities that each state mandates for the approval of various types of cyber operations. This would assist in understanding what organizations and individuals are behind specific operations, thus adding clarity to attribution efforts. Furthermore, such a measure would assist in building confidence between states that these operations are maintained through a rigid C2 structure.

Finally, states could achieve consensus on an arms racing stability CBM that limits the indiscriminate and mass compromise of a supply chain. States largely agree that espionage is acceptable under customary international law and, therefore, would be reluctant to ascribe to a CBM that limits cyber espionage. However, the mass targeting of a supply chain can be particularly destabilizing, especially if there is a concern that intrusions represent preparations for a cyber attack, rather than simply espionage. An example of this would be if a state maintained a backdoor into every computer that happens to employ a certain brand of antivirus software, or every cell phone manufactured by a specific developer (as allegedly occurred with both Russia and China, respectively).[95] Beyond the national security concerns, there are implications for international trade if states perceive the need to resist market forces and only purchase software and hardware manufactured domestically or by a trusted ally. While capable cyber powers will likely continue to

seek to disrupt the supply chain to gain access to an adversary, limiting mass (versus tailored) operations through a CBM could enhance stability among cyber rivals.

Creating new cyber CBMs and the continued maintenance of those already in existence is a necessary step toward mitigating the risk of inadvertent conflict in cyberspace. While traditional arms control regimes are unrealistic and ill-suited for managing the risks associated with cyber operations, CBMs that take into account the unique attributes and dynamics of operating in the cyber domain could help to share information, mitigate uncertainty, and facilitate crisis management, thereby promoting much-needed stability between states. SSQ

Notes

1. We are grateful to Robert Jervis and Richard Betts for their extensive and insightful feedback on earlier versions of this article. We are also thankful to individuals at the Army Cyber Institute at the United States Military Academy at West Point; the US Departments of Commerce, State, and Homeland Security; and the French Mission to the 2017 United Nations Group of Governmental Experts for sharing their candid thoughts with us on this topic.

2. For recent work on the cyber security dilemma, see Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford, UK: Oxford University Press, 2017). For a discussion of the debate regarding escalation dynamics in cyberspace, see Erica D. Borghard and Shawn W. Lonergan, "Escalation Dynamics in Cyberspace" (paper presented at the American Political Science Association annual conference, San Francisco, 31 August 2017). Also see Martin Libicki, *Crisis and Escalation in Cyberspace*, RAND Monograph MG-1215-AF (Santa Monica, CA: RAND, 2012); William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities" (Washington, DC: National Academy of Sciences, 2009); Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford, UK: Oxford University Press, 2018); Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," *Journal of Cybersecurity* 3, no. 1 (March 2017): 19–28, https://doi.org/10.1093/cybsec/tyw016; and Sarah E. Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics" (working paper, SSRN, Rochester, NY, January 2018), https://ssrn.com/abstract=3104014.

3. For a discussion of how the failure to establish norms for interstate relations in cyberspace underscores the imperative of constructing CBMs for the domain, see Alex Grigsby, "The End of Cyber Norms," *Survival: Global Politics and Strategy* 59, no. 6 (December 2017–January 2018): 109–22, https://doi.org/10.1080/00396338.2017.1399730.

4. This is not to suggest that arms control regimes and CBMs are always mutually exclusive. In many instances, states pursue formal, institutionalized arms control agreements in tandem with informal, voluntary CBMs. In the context of Cold War strategic rivalries, CBMs often preceded and sometimes evolved into more formal arms control regimes.

5. For further reference on soft law and information institutions, see Kenneth W. Abbott and Duncan Snidal, "Hard and Soft Law in International Governance," *International Organization* 54, no. 3 (Summer 2000): 421–56, http://www.jstor.org/stable/2601340; Martha Finnemore and Stephen J. Toope, "Alternatives to 'Legalization': Richer Views of Law and Politics," *International Organization* 55, no. 3 (Summer 2001): 743–58, https://home.gwu.edu/~finnemor/articles/2001_legalization_io.pdf; and Jutta Brunee and Stephen J. Toope, *Legitimacy and Legality in International Law* (Cambridge, UK: Cambridge University Press, 2010).

6. Jonathan Alford, "Confidence-Building Measures in Europe: The Military Aspects," *Adelphi Papers* 19, no. 149 (1979): 4–13, https://doi.org/10.1080/05679327908448540.

7. Kevin N. Lewis and Mark A. Lorell, *The Utility of Confidence-Building Measures in Crisis Situations: Some Case Studies*, RAND Paper P-6947 (Santa Monica, CA: RAND, January 1984), 2–7, https://www.rand.org/pubs/papers/P6947.html.

8. In this sense, states act according to Thomas C. Schelling and Morton H. Halperin's "positive-evidence principle," which notes that states are motivated to provide evidence that they are not violating the understanding; Schelling and Halperin, *Strategy and Arms Control*, (Washington, DC: Pergamon-Brassey, 1985), 97–98. However, providing the level of transparency that could completely mitigate the fears of defection is unlikely in cyberspace due to the necessary secrecy that surrounds these operations. CBMs that rely on inspection for compliance are unrealistic.

9. Johan Jørgen Holst and Karen Alette Melander, "European Security and Confidence-Building Measures," *Survival* 19, no. 4 (July/August 1977): 146–54, https://doi.org/10.1080/00396337708441688.

10. Johan Jørgen Holst, "Confidence-Building Measures: A Conceptual Framework," *Survival* 25, no. 1 (January/February 1983): 2–15, https://doi.org/10.1080/00396338308442072; and Rolf Berg, "Military Confidence-Building in Europe," in *Building Security in Europe: Confidence-Building Measures and the CSCE*, ed. Allen Lynch (New York: Institute for East-West Security Studies, 1986), 13–68.

11. Holst, "Confidence-Building Measures," 3. However, CBMs do not decrease mistrust of an adversary or limit its capabilities; that would require an arms control regime that addresses specific security concerns from two or more parties. Also see Richard E. Darilek, "Reducing the Risks of Miscalculation: The Promise of the Helsinki CBMs," in *Confidence-Building Measures in Europe,* ed. F. Stephen Larrabee and Dietrich Stobbe (New York: Institute for East-West Security Studies, 1983), 59–90.

12. *See* Richard K. Betts, "Hedging Against Surprise Attack," *Survival* 23, no. 4 (1981): 146–56, https://doi.org/10.1080/00396338108441973; and Thomas C. Schelling, "Confidence in Crisis," *International Security* 8, no. 4 (Spring 1984): 55–66, https://www.jstor.org/stable/2538562.

13. Holst and Melander, "European Security and Confidence-Building Measures," 148.

14. In addition to Holst, "Confidence-Building Measures," see James Macintosh, "Confidence-Building Measures: A Conceptual Exploration," in *Confidence Building Measures and International Security*, ed. R. B. Byers, F. Stephen Larrabee, and Allen Lynch (New York: Institute for East-West Security Studies, 1987), 9–29, for a conceptual overview of confidence building measures that a state may choose to enact.

15. US State Department, "Conference on Security and Co-operation in Europe Final Act," Department of State Publication 8829, August 1975, 84, https://www.osce.org/helsinki-final-act?download=true.

16. The Helsinki Final Act solely dealt with cooperation between the East and West during the Cold War. However, it has been used as the benchmark for other regional security competi-

tions. Similar agreements can be seen in Ariel E. Levite and Emily B. Landau, "Confidence and Security Building Measures in the Middle East," *Journal of Strategic Studies* 20, no. 1 (1997): 143–71, https://doi.org/10.1080/01402399708437667; Laurie Nathan, " 'With Open Arms': Confidence-and Security-Building Measures in Southern Africa," *South African Journal of International Affairs* 1, no. 2 (1994): 110–26, https://doi.org/10.1080/10220469409545106; Ralph A. Cossa, *Asia Pacific Confidence and Security Building Measures* (Washington, DC: Center for Strategic & International Studies, 1995); Michael Krepon, Dominique M. McCoy, and Matthew C. J. Rudolph, *A Handbook of Confidence-Building Measures for Regional Security* (Washington, DC: The Henry L. Stimson Center, 1993); and United Nations, Department for Disarmament Affairs, *Confidence and Security-Building Measures—From Europe to Other Regions* (New York: United Nations, 1991).

17. With only one exception between 1975 and 1982, the Soviet Zapad-81 military exercise, all signatories observed the reporting requirements of the original Helsinki Final Act. For a more detailed analysis of the exercises conducted during this period, see Holst, "Confidence-Building Measures," 7–11. However, in more recent times, the Russian Zapad military exercises in the summer of 2017 were said to have violated Cold War agreements. *See* Michael R. Gordon and Eric Schmitt, "Russia's Military Drills Near NATO Border Raise Fears of Aggression," *New York Times*, 31 July 2017, https://www.nytimes.com/2017/07/31/world/europe/russia-military-exercise-zapad-west.html.

18. For the exact language for the requirements of this provision, see State Department, "Conference on Security and Co-operation in Europe Final Act," 85–86.

19. For a concise history of CBMs up to the 1992 Vienna document, see James Macintosh, "Confidence Building Measures in Europe: 1975 to the Present," in *Encyclopedia of Arms Control and Disarmament,* ed. Richard Dean Burns (New York: Charles Scribner's Sons, 1993).

20. The 2011 Vienna document builds on previous agreements, specifically the 1975 Helsinki Final Act, the Document of the Stockholm Conference of 1986, the 1992 Helsinki Document, and the Vienna Documents of 1990, 1992, 1994, and 1999.

21. For a more detailed overview of the 2011 Vienna Document, see Organization for Security and Co-operation in Europe (OSCE), *Vienna Document 2011 on Confidence- and Security-building Measures* (Vienna: OSCE, 30 November 2011), http://www.osce.org/fsc/86597.

22. For instance, see Schelling and Halperin, *Strategy and Arms Control*, *ix*–6; and David W. Kearn Jr., *Great Power Security Cooperation: Arms Control and the Challenge of Technological Change* (Lexington, MA: Lexington Books, 2014), 15–48. Examples of arms control agreements designed to minimize instability include the 1963 "Hot Line" Agreement, the 1971 "Accidents Measures" Agreement, and the 1972 Antiballistic Missile (ABM) Treaty. Hedley Bull describes the objectives of arms control across economic, moral, and the international security domains in chapter 1 of his seminal work, *The Control of the Arms Race: Disarmament and Arms Control in the Missile Age*, vol. 2 (London: Praeger for the Institute for Strategic Studies, 1961). Bull's objectives of arms control that relate to inadvertent conflict escalation are of particular relevance to this article. Schelling and Halperin, *Strategy and Arms Control*, 141–42.

23. *See* Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 4 (2017): 452–81, https://doi.org/10.1080/09636412.2017.1306396; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 401–28, http://dx.doi.org/10.1080/01402390.2012.663252; Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance," *Contemporary Security Policy* 34, no. 1 (April 2013): 40–63, https://doi.org/10.1080/13523260.2013.771031; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41,

no. 3 (Winter 2016/17): 72–109, https://doi.org/10.1162/ISEC_a_00267; Jon R. Lindsay, "Stuxnet and The Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404, https://doi.org/10.1080/09636412.2013.816122. Additionally, it is difficult to differentiate between offensive and defense expenditures given that, at least from a military perspective, the forces that conduct offensive cyber operations may very well be the same as those that conduct defensive cyber operations.

24. As noted, there is no effective measure of relative offensive cyberpower between states. However, on a subjective scale, certain states (e.g., the United States, China, Russia, France, Great Britain, and Israel) are capable of wreaking widespread havoc against another actor via the offensive use of cyberpower.

25. Chris Wallace, "Gen. Dempsey Reacts to Paris Attacks; Sens. Hoeven, Coons Talk Keystone Showdown," Fox News Sunday, 11 January 2015, http://www.foxnews.com/transcript/2015/01/11/gen-dempsey-reacts-paris-attacks-sens-hoeven-coons-talk-keystone-showdown.html.

26. The existing CERT infrastructure, which fosters a common threat picture for state and nonstate actors alike, reduces some of the uncertainty and vulnerability that exists between actors in this volatile space. However, the CERTs do not help manage crisis escalation nor do they promote transparency beyond the technical threat and security information that participants freely share.

27. William M. Arkin, Ken Dilanian, and Cynthia McFadden, "What Obama Said to Putin on the Red Phone About the Election Hack," NBC News, 19 December 2016, http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116.

28. Cynthia McFadden, William R. Arkin, and Kevin Monahan, "Russians Penetrated U.S. Voter Systems, Top U.S. Official Says," NBC News, 8 February 2018, https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721.

29. For further information on these efforts, see Barbara Rosen Jacobson, Roxana Radu, and Vladimir Radunovic, "Towards a Secure Cyberspace via Regional Cooperation," *Diplo*, 9 December 2016, https://www.diplomacy.edu/blog/towards-secure-cyberspace-regional-cooperation. While these initiatives may eventually contribute to fostering stability in cyberspace within their respective regions, we focus on the UN and OSCE efforts because they are the most mature on promoting cyber confidence building to date.

30. Group of 7 (G7), *G7 Declaration on Responsible States Behavior in Cyberspace* (Taormina, Italy: G7, 11 April 2017), https://www.mofa.go.jp/files/000246367.pdf; Group of 20 (G20), *G20 Leaders' Communique* (Antalya, Turkey: G20, 15–16 November 2015), http://www.consilium.europa.eu/en/press/press-releases/2015/11/16/g20-summit-antalya-communique/.

31. UN General Assembly (UNGA), Resolution 58/32, A/RES/58/32, "Developments in the Field of Information and Telecommunications in the Context of International Security," 8 December 2003, 47, http://undocs.org/A/RES/58/32.

32. UNGA, Report A/65/201, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 30 July 2010, http://undocs.org/A/65/201.

33. UNGA, Report A/68/98, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 24 June 2013, reissued for technical reasons on 30 July 2013, http://undocs.org/A/68/98; and UNGA, Report A/70/174, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 22 July 2015, http://undocs.org/A/70/174.

34. See the appendix for a list of these CBMs. Also see Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of Inter- national Security" (Washington, DC: US State Department, 23 June 2017), https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm. For further commentary, see Adam Segal, "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?," *Council of Foreign Relations-Net Politics*, 29 June 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what; and Owen Bowcott, "Dispute Along Cold War Lines Led to Collapse of UN Cyberwarfare Talks," *The Guardian*, 23 August 2017, https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges; and Arun M. Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?," *Lawfare* (blog), 4 July 2017, https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

35. See, for example, Finnemore and Toope, "Alternatives to 'Legalization'; Brunee and Toope, *Legitimacy and Legality*; and Wayne Sandholtz, "Dynamics of International Norm Change: Rules against Wartime Plunder," *European Journal of International Relations* 14, no. 1 (March 2008): 101–31, http://journals.sagepub.com/doi/10.1177/1354066107087766.

36. Organization for Security and Co-operation in Europe, *Permanent Council Decision no. 1039*, 26 April 2012, http://www.osce.org/pc/90169.

37. Organization for Security and Co-operation in Europe (OSCE), *Permanent Council Decision*, no. 1106, 3 December 2013, http://www.osce.org/pc/109168; OSCE, *Permanent Council Decision*, no. 1202, 10 March 2016, http://www.osce.org/pc/227281. However, also see Transnational Threat Department, "Cyber/ICT Security," OSCE Secretariat, http://www.osce.org/secretariat/256071?download=true; and Lamberto Zannier, "Cyber/ICT Security: Building Confidence," *Security Community* 2 (June 2014): 4–5, http://www.osce.org/magazine/122525.

38. For instance, the need for cyber CBMs has been noted by James Andrew Lewis, "Confidence-Building and International Agreement in Cybersecurity," *Disarmament Forum: Confronting Cyberconflict* 4 (Geneva: UN Institute for Disarmament Research, 2011), 51–60, http://www.unidir.org/files/publications/pdfs/confronting-cyberconflict-en-317.pdf.

39. Herbert Lin, "Arms Control in Cyberspace: Challenges and Opportunities," World Politics Review (website), 6 March 2012, https://www.worldpoliticsreview.com/articles/11683/arms-control-in-cyberspace-challenges-and-opportunities.

40. Tughral Yamin, *Cyberspace CBMs between Pakistan and India* (Islamabad: National University of Sciences and Technology, 2014), 102.

41. Jason Healey, John C. Mallery, Klara Tothova Jordan, and Nathaniel V. Youd, *Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security* (Washington, DC: Atlantic Council, November 2014, http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf.

42. Holst, "Confidence-Building Measures," 4–5.

43. Holst, "Confidence-Building Measures," 4.

44. For literature on multistakeholder governance, see Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010); Tana Johnson, *Organizational Progeny: Why Governments Are Losing Control over Proliferating Structures of Global Governance* (Oxford, UK: Oxford University Press, 2014); Kenneth W. Abbott, Jessica F. Green, and Robert O. Keohane, "Organizational Ecology and Institutional Change in Global Governance," *International Organization* 70, no. 2 (Spring 2016): 247–77, https://doi.org/10.1017/S0020818315000338.

45. The CBMs in the appendix are classified by an updated version of John Holst's CBM classification guidelines.

46. See appendix, table 3: December 2013 OSCE—CBM 6.

47. Forum of Incident Response and Security Teams (FIRST), "FIRST Teams," accessed 25 June 2018, https://www.first.org/members/teams.

48. See appendix, table 2: July 2015 GGE—CBM D.

49. See the US National Institute of Standards and Technology (NIST) National Vulnerability Database, https://nvd.nist.gov/.

50. For example, see GGE Measure 3 and OSCE Measure 7, in appendix, table 1 and table 3, respectively.

51. See appendix, table 1: July 2015 GGE—CBM 3.

52. *See* Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (July 2016): 425–79, https://doi.org/10.1017/S0002930000016894; Emanuel Adler and Vincent Pouliot, "International Practices," *International Theory* 3, no. 1 (February 2011): 1–36, https://doi.org/10.1017/S175297191000031X; and Emanuel Adler and Michael Barnett, eds., *Security Communities* (Cambridge, UK: Cambridge University Press, 1998).

53. Though beyond the scope of this article, there are signs of states developing dramatically different strategies for operating militarily in the cyber domain that may reflect variation in strategic culture within those states. For instance, Russian interference in the 2016 US presidential election is consistent with the Soviet Union's approach to information warfare employed throughout the Cold War (Dov H. Levin, "Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset," *Conflict Management and Peace Science* 33, no. 4 [September 2016], https://doi.org/10.1177/0738894216661190). North Korea has reportedly benefited from financially motivated cybercrime to generate capital and circumvent economic sanctions (Paul Mozur and Choe Sang-Hun, "North Korea's Rising Ambition Seen in Bid to Breach Global Banks," *New York Times*, 25 March 2017, https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html). China has used cyber espionage to steal industrial and intellectual property to grow its economy (Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011* [Washington, DC: Director of National Intelligence, October 2011]). Finally, the United States has historically pressed for the "rules based order" that exists in the physical domains of strategic interaction to apply to cyberspace (for instance, see Dan Seifert, "President Obama Wants to Prevent a Cyber Weapon 'Arms Race,' " *The Verge*, 5 September 2016, https://www.theverge.com/2016/9/5/12798836/president-obama-prevent-cyber-weapon-arms-race; Harold Hongju Koh, "International Law in Cyberspace," *Faculty Scholarship Series*, Paper 4854 [2012], http://digitalcommons.law.yale.edu/fss_papers/4854/; and International Cyberspace Policy Strategy, Public Law 114-113, Division N, Title IV, Section 402, US Department of State, March 2016, https://www.state.gov/documents/organization/255732.pdf).

54. *See* Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (Autumn 1998): 887–917, https://www.jstor.org/stable/2601361.

55. See appendix, table 3: December 2013 OSCE—CBMs 10, 11.

56. Paul Meyer, "Cyber-Security through Arms Control: An Approach to International Cooperation," *RUSI Journal* 156, no. 2 (2011): 22–27, https://doi.org/10.1080/03071847.2011.576471. Note that Yamin, *Cyberspace CBMs between Pakistan and India*, 108–12, also takes a rudimentary step toward identifying cyber CBMs that could be established in a bilateral context;

however, many of the measures fall under the convention of norm creation, such as "avoiding hostile propaganda," and have limited applicability beyond the India-Pakistan relationship. For more on the role of secrecy surrounding cyber operations, see Shawn W. Lonergan, "Cyber Power and the International System" (PhD diss., Columbia University, 2017), 4–7, https://doi org/10.7916/D88D07PH.

57. "NATO's Flagship Cyber Exercise Begins in Estonia," NATO, 4 December 2017, https://www.nato.int/cps/ic/natohq/news_149233.htm.

58. For example, Cyber Guard is an annual defensive exercise cohosted by the US Cyber Command, the Federal Bureau of Investigation, and the Department of Homeland Security that incorporates the private sector and numerous governmental organizations to respond to a cyberattack against US public and private critical infrastructure. The exercise is focused on identifying existing technical vulnerabilities, developing and testing response actions, and improving defense of DOD information systems. For further information, see Mark Pomerleau, "Cyber Forces Prepare for Attack on a Grand Scale," *Defense Systems*, 20 June 2016, https://defensesystems.com/articles/2016/06/20/cyber-guard-dod-civilian-industry-exercise.aspx. However, US Cyber Command does have exercises, such as its annual Cyber Flag, which incorporate offensive capabilities and involve multinational coalition partners. During this exercise the offensive response actions may be fictionalized or involve real capabilities. However, despite the multinational representation at the exercise, the cyber weaponry used is employed on isolated test networks, and only those with appropriate security clearances are aware of the specific capabilities involved. In addition to promoting a common understanding of response actions between partners, the exercise, as is the case with Cyber Guard, is widely used by the military to validate the proficiency of cyber teams. Chief Warrant Officer Judy Esquibel (Army Cyber Institute), interview by the author, 30 April 2017.

59. Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, nos. 1–2 (2018): 6–32, https://doi.org/10.1080/01402390.2017.1288107.

60. Though beyond the scope of this article, there is a growing body of literature addressing the differences in internet policy across regime type. Most authoritarian states have instituted hierarchies in their intrastate internet infrastructure to prevent their citizens from accessing prohibited material. However, Western democracies (for the most part) have pursued a free and open internet that is largely devoid of state censorship. These conflicting visions for the internet were evident during the 2012 breakdown of the United Nation's International Telecommunications Union's World Conference on International Communication (WCIT), when China and Russia used the Arab Spring to get support from many Middle Eastern countries to push for a treaty that limited the openness of the internet and created restrictions on free speech. In response, most Western democracies refused to ratify the treaty. This divide has given rise to extensive debates about internet governance, state sovereignty in cyberspace, and the "Balkanization" of the internet. *See* James D. Fielder, "The Internet and Dissent in Authoritarian States," in *Conflict and Cooperation in Cyberspace: The Challenge to National security*, ed. Panayotis A. Yannakogeorgos and Adam B. Lowther (New York: Taylor & Francis, 2013), 161–94; Daniel W. Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119, no. 3 (Fall 2004): 477–98, https://doi.org/10.2307/20202392; Stephen K. Gourley, "Cyber Sovereignty," in *Conflict and Cooperation in Cyberspace*, 277–90; Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: UK: Cambridge University Press, 2013); Dana Polatin-Reuben and Joss Wright, "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet" (paper presented at the 4th USENIX Workshop on Free and Open Communications on the Internet, San Diego, CA, 18 August 2014). For a comprehensive report on state censorship

by country, see Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, and Mai Truong, *Privatizing Censorship, Eroding Privacy: Freedom on the Net 2015* (New York: Freedom House, October 2015), https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf.

61. A comprehensive report on Russian interference into the 2016 US Presidential election has yet to be written. However, there are multiple ongoing US government investigations across several agencies, as well as investigative journalists doing the same. Moreover, there is consensus within the US intelligence community regarding Russian interference of the election. The most comprehensive assessment to date is the Office of the Director of National Intelligence, National Intelligence Council, "Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

62. For a good discussion on the Western view of information operations and public diplomacy, see John M. Wilson, "The Hunting of the Snark: Organizing and Synchronizing of Informational Elements for Homeland Defense and Civil Support" (master's thesis, Naval Postgraduate School, Monterey, CA, June 2009), http://www.dtic.mil/dtic/tr/fulltext/u2/a501553.pdf; and Leigh Armistead, ed. *Information Operations: Warfare and the Hard Reality of Soft Power* (Lincoln, NE: Potomac Books, 2004).

63. Though beyond the scope of this article, this view is in line with the literature on the Democratic Peace Theory that holds that democracies are more likely to be peaceful with one another because of shared culture, norms, and structural mechanisms that promote peaceful conflict resolution. Additionally, scholarship has shown that common ideologies encourage alliance formation whereas divergent ideologies can have a positive effect on threat perception and domestic stability. Indeed, authoritarian regimes view access to the unfettered internet as a venue that can encourage civil unrest because it exposes their citizenry to differing ideological thought and serves as a venue for likeminded individuals to assemble in relative safety. This view is rational given the role social media played during the Arab Spring, which resulted in multiple regime changes. Some Western policy makers and strategists may hold that by keeping a free and open internet, democracies can spread democratic values in hopes that it will encourage democratic revolutions in authoritarian regimes—thus resulting in a strategic victory and an international environment where they face fewer threats and potentially new allies.

64. US State Department Bureau of Democracy, Human Rights, and Labor, "Internet Freedom Annual Program Statement," 2 June 2014, https://2009-2017.state.gov/j/drl/p/previouscalls/227048.htm. As an interesting aside, the development of the most commonly used anonymity software available, The Onion Router (commonly known as "Tor"), was sponsored by the Defense Advanced Research Projects Agency (DARPA) and the US Navy's Office of Naval Research (ONR).

65. Thomas Lum, Patricia Moloney Figliola, and Matthew C. Weed, "China, Internet Freedom, and U.S. Foreign Policy," *Congressional Research Service*, 13 July 2012.

66. UNGA, Report A/HRC/17/27, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue," 16 May 2011, http://undocs.org/A/HRC/17/27; UNGA Human Rights Council, A/HRC/32/L.20, "The Promotion, Protection and Enjoyment of Human Rights on the Internet," 27 June 2016, http://undocs.org/A/HRC/32/L.20. :However, the view that access to the internet is a human right remains hotly contested. For further reference, see Daniel Joyce, "Internet Freedom and Human Rights," *European Journal of International Law* 26, no. 2 (May 2015): 493–514, https://doi.org/10.1093/ejil/chv021; Vinton G. Cerf, "Internet Access Is Not a Human Right," *New York Times*, 4 January 2012, https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html; and Michael L. Best, "Can the Internet Be a Human Right?," *Human Rights*

& Human Welfare 4, no. 1 (2004): 23–31, https://www.du.edu/korbel/hrhw/volumes/2004/best-2004.pdf.

67. Angelique Chrisafis, "Emmanuel Macron Promises Ban on Fake News During Elections," *The Guardian*, 3 January 2018, https://www.theguardian.com/world/2018/jan/03/emmanuel-macron-ban-fake-news-french-president; Mark Scott and Janosch Delcker, "Free Speech vs. Censorship in Germany," *Politico*, 4 January 2018, https://www.politico.eu/article/germany-hate-speech-netzdg-facebook-youtube-google-twitter-free-speech/.

68. For instance, see Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Rev*iew 107, no. 2 (2013): 326–43, https://doi.org/10.1017/S0003055413000014; Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (Spring 2011): 32–61, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf; and Fielder, "Internet and Dissent in Authoritarian State."

69. Emily Parker, "Russia Is Trying to Copy China's Approach to Internet Censorship," *Slate*, 4 April 2017, http://www.slate.com/articles/technology/future_tense/2017/04/russia_is_trying_to_copy_china_s_internet_censorship.html.

70. Ronald J. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (Oxford, UK: Signal, 2013).

71. Michael LaForgia and Gabriel J. X. Dance, "Facebook Gave Data Access to Chinese Firms Flagged by U.S. Intelligence," *New York Times*, 5 June 2018, https://www.nytimes.com/2018/06/05/technology/facebook-device-partnerships-china.html.

72. For further information on the Dark Web marketplace, see Paul Stockton and Michele Golabek-Goldman, "Curbing the Market for Cyber Weapons," *Yale Law & Policy Review* 32, no. 1 (2013): 239–66, http://digitalcommons.law.yale.edu/ylpr/vol32/iss1/11/.

73. For instance, see "Stuxnet Source Code Released Online, Download Now," The Hacker News, 2 July 2011, http://thehackernews.com/2011/07/stuxnet-source-code-released-online.html; and Ellen Nakashima, "Powerful NSA Hacking Tools Have Been Revealed Online," *Washington Post*, 16 August 2016, https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html?noredirect=on&utm_term=.9e477b899afb.

74. "Wassenaar: Cybersecurity and Export Control," testimony before the US House of Representatives Subcommittee on Information Technology (Washington, DC: 12 January 2016), https://oversight.house.gov/hearing/wassenaar-cybersecurity-and-export-control/; and Trey Herr, *Malware Counter-Proliferation and the Wassenaar Arrangement, Proceedings of the 8th International Conference on Cyber Conflict* (Tallinn, Estonia, 4 January 2016), https://dx.doi.org/10.2139/ssrn.2711070.

75. Bug bounty programs offer financial rewards for "white hat" hackers who find vulnerabilities. Russell Brandom, "Google Says Controversial Exports Proposal Would Make the World 'Less Secure,' " *The Verge*, 20 July 2015, http://www.theverge.com/2015/7/20/9005351/google-wassenaar-arrangement-proposal-comments; and Chris Bream, Facebook U.S. Public Policy, "Wassenaar Rules Are Not the Right Direction," Facebook, 28 July 2015, https://www.facebook.com/uspublicpolicy/posts/1047027321981746. For a more comprehensive list of the public feedback the US Department of Commerce received regarding this regulation, see "Public Comments for Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items," Regulations.gov, comment period closed 20 July 2015, https://www.regulations.gov/docketBrowser?rpp=50&so=DESC&sb=postedDate&po=0&dct=PS&D=BIS-2015-0011.

76. Senior official (US Department of Commerce, Bureau of Industry and Security), interview with the author, 28 November 2016. Specifically, Wassenaar Arrangement Category 4 rules 4.A.5, 4.D.4, and 4.E.1.C were never added to the Commerce Control List as elucidated in the department's Export Administration Regulations in either 2014 or 2015 following the 2013 amendments. The concern here was that technology that is used to detect vulnerabilities within a network could also be used to exploit the network as an essential part of gaining access. This highlights the difficulties of dual-use technologies in this space.

77. "Summary of Changes: List of Dual-Use Goods & Technologies and Munitions List," Wassenaar Arrangement (website), 17 February 2017, https://www.wassenaar.org/app/uploads/2017/03/Summary-of-Changes-to-2016-Lists.pdf; also see Rainer Himmelfreundpointner, "Le Monde Wassenaar Arrangement," *Cercle Diplomatique*, Issue 1/2017, 62–66, https://www.yumpu.com/en/document/view/57005074/cercle-diplomatique-issue-01-2017.

78. For an in-depth discussion on the motivation of authoritarian states to employ cyber proxies, see Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" *Orbis* 60, no. 3 (Summer 2016): 395–416, https://doi.org/10.1016/j.orbis.2016.05.009.

79. Ellen Nakashima, "Justice Department Charges Russian Spies and Criminal Hackers in Yahoo Intrusion," *Washington Post*, 15 March 2017, https://www.washingtonpost.com/world/national-security/justice-department-charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html?utm_term=.e0993e6a74ea; and Alina Selyukh, "Every Yahoo Account that Existed in Mid-2013 Was Likely Hacked," NPR, 3 October 2017, https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo-account-that-existed-in-mid-2013-was-likely-hacked.

80. Mozur and Sang-Hun, "North Korea's Rising Ambition"; Ellen Nakashima, "The NSA Has Linked the WannaCry Computer Worm to North Korea," *Washington Post*, 14 June 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.5eb85debb0f8; and Jim Finkle, "North Korea likely behind Taiwan SWIFT cyber heist—BAE," Reuters, 16 October 2017, https://www.reuters.com/article/cyber-heist-north-korea-taiwan/north-korea-likely-behind-taiwan-swift-cyber-heist-bae-idUSL2N1MR1QC.

81. Council of Europe, "European Treaty Series no. 185, Convention on Cybercrime" (Budapest: 23 November 2001), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

82. Chart of Signatures and Ratifications of Treaty 185, Council of Europe, accessed 6 June 2017, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. However, it is important to note that in April 2017 Russia put forward its own convention on cybercrime to the United Nations as a direct replacement to the Budapest Convention. For further information, see "Russia Prepares New UN Anti-Cybercrime Convention—Report," RT, 14 April 2017, https://www.rt.com/politics/384728-russia-has-prepared-new-international/.

83. Though these bilateral agreements are examples between major state powers, there are other agreements between regional powers, particularly on cybersecurity coordination efforts, that are beyond the scope of this article.

84. The White House, "Fact Sheet: President Xi Jinping's State Visit to the United States," Office of the Press Secretary, 25 September 2015, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states. Note that intellectual property theft

that supports national security objectives is still permissible for espionage, for it is considered a necessary state practice by Customary International Law.

85. "First U.S.-China Law Enforcement and Cybersecurity Dialogue," Department of Homeland Security, https://www.dhs.gov/news/2017/10/06/first-us-china-law-enforcement-and-cybersecurity-dialogue.

86. Daniel R. Coats, Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*, 115th Cong., 2nd sess., 6 March 2018, 6, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1851-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

87. Office of the United States Trade Representative, "Findings of the Investigation into China's Act, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974" (Washington, DC: Executive of the President, 22 March 2018).

88. Secretary of Defense, "Memorandum of Understanding Between the United States of America Department of Defense and the People's Republic of China Ministry of National Defense on Notification of Major Military Activities Confidence-Building Measures Mechanism," 4 November 2014, http://archive.defense.gov/pubs/141112_MemorandumOfUnderstandingOnNotification.pdf; "Military Crisis Notification Mechanism for Use of the Defense Telephone Link," in US-China Crisis Communications, September 2015, http://www.defense.gov/portals/1/documents/pubs/us-china_crisis_communications_annex_sep_2015.pdf.

89. Senior official (United States Department of Homeland Security), interview by the author, 14 July 2016.

90. US State Department, *U.S.-Russia Bilateral Presidential Commission: 2013 Joint Annual Report* (2013), http://www.state.gov/p/eur/ci/rs/usrussiabilat/219086.htm#8.

91. The White House, "Fact Sheet: U.S.-Russian Cooperation on Information and Communications Technology Security," Office of the Press Secretary, 17 June 2013, https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

92. David Ignatius, "In Our New Cold War, Deterrence Should Come before Détente," *Washington Post*, 15 November 2016, https://www.washingtonpost.com/opinions/global-opinions/in-our-new-cold-war-deterrence-should-come-before-detente/2016/11/15/051f4a84-ab79-11e6-8b45-f8e493f06fcd_story.html?utm_term=.0f14161b193c.

93. Office of the Press Secretary, "DHS Statement on NBC News Coverage of Election Hacking," Department of Homeland Security, 12 February 2018, https://www.dhs.gov/news/2018/02/12/dhs-statement-nbc-news-coverage-election-hacking.

94. In addition to hiring cyber proxies due to a dearth of localized talent, states may also employ them for plausible deniability. For further reference to the state-proxy exchange, see Borghard and Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?" Note that the authors discuss the risks states face when they chose to employ a cyber proxy.

95. *See* Nicole Perlroth and Scott Shane, "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets," *New York Times*, 10 October 2017, https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html; and Matt Apuzzo and Michael S. Schmidt, "Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say," *New York Times*, 15 November 2016, https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html.

Appendix

Table A.1. United Nations General Assembly (UNGA) recommended confidence building measures (CBM) on 22 July 2015

Recommended CBM	CBM classification
1. The identification of appropriate points of contact at the policy and technical levels to address serious information and communications technology (ICT) incidents and the creation of a directory of such contacts;	Stability-crisis
2. The development of and support for mechanisms and processes for bilateral, regional, subregional, and multilateral consultations, as appropriate, to enhance inter-state confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;	Stability-arms race
3. Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;	Information-use, threat actor, and security
4. The voluntary provision by states of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:	Information-use
– a repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;	
– the development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;	
– the development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;	
– the adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.	

Table A.2. UNGA-recommended additional CBMs on a bilateral, subregional, regional, and multilateral basis

Recommended CBM	CBM classification
A. Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;	Information-security
B. Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;	Information-security
C. Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfill this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;	Information-threat actor and security Stability-crisis
D. Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;	Information-threat actor and security Stability-crisis
E. Cooperate, in a manner consistent with national and international law, with requests from other states in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.	Information-threat actor and security

Table A.3. CBMs adopted through OSCE Permanent Council Decision no. 1106 on 3 December 2013

Recommended CBM	CBM classification
1. Participating states will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing parties.	Information-security
2. Participating states will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.	Information- use and security
3. Participating states will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.	Stability-arms race
4. Participating states will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable internet.	Information-use

Table A.3. CBMs adopted through OSCE Permanent Council Decision no. 1106 on 3 December 2013 (*continued*)

Recommended CBM	CBM classification
5. The participating states will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating states will explore further developing the OSCE role in this regard.	Administrative
6. Participating states are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating states in order to counter terrorist or criminal use of ICTs. The OSCE participating states agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.	Information-threat actor
7. Participating states will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.	Information-use
8. Participating states will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating states will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating states will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating states will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.	Stability-crisis, Information-use
9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating states will, as a first step, voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating state will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating states will endeavor to produce a consensus glossary.	Information-use
10. Participating states will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE communications network, maintained by the OSCE secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.	Administrative
11. Participating states will, at the level of designated national experts, meet at least three times each year, within the framework of the security committee and its informal working group established by permanent council decision no. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals from the consolidated list circulated by the chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.	Administrative

Table A.4. CBMs adopted through OSCE Permanent Council Decision no. 1202 on 10 March 2016

Recommended CBM	CBM classification
12. Participating states will, on a voluntary basis, share information and facilitate inter-state exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating states to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.	Information-security
With respect to such activities participating states are encouraged, inter alia, to: – conduct such activities in the spirit of enhancing inter-state cooperation, transparency, predictability and stability; – complement, through such activities, un efforts and avoid duplicating work done by other fora; and – take into account the needs and requirements of participating states taking part in such activities. Participating states are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.	
13. Participating states will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision no. 1106.	Stability-arms race, crisis
14. Participating states will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.	Information-security
15. Participating states, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.	Information-security, threat actor
Collaboration may, inter alia, include: – sharing information on ICT threats; – exchanging best practices; – developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure; – adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident; – sharing national views of categories of ICT-enabled infrastructure states consider critical;	

Table A.4. CBMs adopted through OSCE Permanent Council Decision no. 1202 on 10 March 2016 (*continued*)

Recommended CBM	CBM classification
– improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and	
– raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.	
16. Participating states will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing cooperation and transparency within the OSCE region. OSCE participating states agree that such information exchange, when occurring between states, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision no. 1106, with a view to avoiding duplication.	Information-security

The Case for the US ICBM Force

Matthew Kroenig

Abstract

Since the 1960s, intercontinental ballistic missiles (ICBM) have been a central element of America's nuclear triad. In recent years, however, ICBMs have come under increasing attack. Prominent critics charge they are unnecessary for deterrence, they undermine nuclear strategic stability, and the cost of modernization is unaffordable. This article argues that these criticisms are misguided. Far from unnecessary, ICBMs possess a number of distinctive attributes that contribute to core objectives of US nuclear strategy, including the deterrence of nuclear attack, assurance of allies, and achieving US objectives should deterrence fail. Moreover, the argument that ICBMs are destabilizing rests on a logical contradiction and is inconsistent with the empirical evidence. Finally, while the cost of ICBM modernization is substantial, it is also affordable. This more careful analysis demonstrates that ICBMs contribute to US national security and should remain a core part of America's strategic deterrent.

❋❋❋❋❋

Since the 1960s, intercontinental ballistic missiles (ICBM) have been a central element of America's nuclear deterrent. Along with submarines and bombers, these long-range, ground-based missiles constitute one of the three legs of America's nuclear triad. The United States currently deploys 400 ICBMs in missile fields in Montana, North Dakota, and Wyoming, with another 50 silos "kept warm" for possible missile upload if necessary.[1] Although the ICBM force has been greatly reduced since the end of the Cold War, it remains a major component of the US nuclear triad. The Minuteman III missile (in operation since 1970) has

Matthew Kroenig is associate professor of government and foreign service at Georgetown University and deputy director for strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council. His most recent book is *The Logic of American Nuclear Strategy* (Oxford University Press, 2018).

exceeded its expected service life, however, and there is a widespread recognition that it must be replaced. In 2010, the Obama administration announced plans to modernize the country's nuclear forces, including ICBMs, over the next 30 years. The plan for a new ICBM, the ground-based strategic deterrent (GBSD), calls for the acquisition of 400 to 450 new missiles to be deployed in the late 2020s at an estimated price tag of $149 billion.[2] The Trump administration has declared its intention to follow through with Obama's modernization plans, which enjoys mainstream bipartisan support. In 2016, for example, then-Secretary of Defense Ashton Carter, speaking just steps from a missile field in North Dakota, declared that the nuclear triad, including the ICBM force, remains "the bedrock of our security."[3]

For decades, Republican and Democratic administrations have agreed that ICBMs were necessary for US nuclear deterrence. At the end of the Cold War, scholars debated whether the United States and Russia could jointly negotiate to eliminate all ballistic missiles, but those proposals never came to fruition.[4] In recent years, America's nuclear missiles have once again come under attack, but, in contrast to earlier debates, critics now claim that the United States should eliminate them unilaterally, since there is scant hope that Russia will do the same. Prominent advocates of this form of unilateral disarmament, including former Secretary of Defense William Perry and former Commander of US Strategic Command James Cartwright, argue that ICBMs are unnecessary for deterrence because the other elements of America's nuclear arsenal, namely bombers and submarines, are more than sufficient to provide the United States with an assured retaliation capability.[5] They also charge that ICBMs could be destabilizing in a crisis, giving rise to first-strike incentives and increasing the risk of accidental nuclear war.[6] Finally, they argue that the projected costs of modernization make them unaffordable and the United States can, therefore, save significant sums in the defense budget by canceling modernization plans and shedding this leg of the nuclear triad.[7]

These criticisms are misguided. There are valid reasons why ICBMs have remained a prominent feature of America's nuclear force for several decades. Far from unnecessary, ICBMs possess a number of distinctive attributes that contribute to key goals of US nuclear strategy, including the deterrence of enemies, assurance of allies, and the achievement of US objectives in the event deterrence fails.[8] ICBMs increase the dif-

ficulty of a successful nuclear first strike on the United States and contribute to limiting damage to the United States and its allies should conflict erupt. In addition, a US decision not to modernize the ICBM force could cause America's more than 30 treaty allies to question the US commitment to, and credibility of, extended deterrence. Moreover, the other objections raised by detractors do not hold up under scrutiny. The argument that ICBMs are destabilizing rests on a logical contradiction and is inconsistent with the empirical evidence. Finally, while the cost of ICBM modernization is substantial, it is also affordable. If one agrees with Secretary of Defense James Mattis, therefore, that maintaining an effective nuclear deterrent is the "number one priority of the Department of Defense," then ICBM modernization is also a good value.[9] This more careful analysis demonstrates that ICBMs contribute to US national security and should remain a core part of America's strategic deterrent.

This is not the first defense of America's ICBM force, but it goes beyond existing arguments in a number of ways.[10] First, the article provides a new articulation of the theoretical contradiction at the heart of critics' core arguments about strategic stability. Second, it provides a novel explanation and quantification of how ICBMs contribute to damage limitation. Third, it presents original evidence in support of the ICBM assurance mission. Finally, and most broadly, explanations for America's continued reliance on ICBMs must be updated in light of changing international conditions and to address a new and evolving set of criticisms.

This article will provide a review of debates about a "zero ballistic missile regime" in the immediate post–Cold War era. Next, it examines contemporary criticisms of US ICBMs and presents the case for the ICBM force, including a point-by-point rebuttal of the opponents. The article concludes with the implications of this analysis for scholarship on nuclear deterrence and US nuclear policy.

A Zero Ballistic Missile Regime

Although ICBMs have been a core part of America's nuclear deterrent for decades, the end of the Cold War created a belief that it might be possible for the United States, Russia, and other nuclear powers to eliminate all ground-based ballistic missiles.[11] Some even went further and argued that submarine-based ballistic missiles might also be placed on the chopping block.[12] In 1987, the United States and Russia did manage to negotiate the Intermediate Range Nuclear Forces Treaty (INF),

eliminating all intermediate-range (those with ranges from 500–5,000 km) missiles.[13] But, in the end, a complete zero ballistic missile regime (ZBM) proved beyond reach.

Proponents of a ZBM argued that ballistic missiles were exceptionally destabilizing.[14] Since they can be launched promptly, are not recallable, and are fast flying, they reduce time for decision making in a crisis and raise the risk of miscalculation. Moreover, their hard-target kill capability made them potentially attractive to aggressors contemplating a nuclear first strike. In contrast, a world with nuclear forces deployed only on slower-flying cruise missiles and aircraft (the latter of which can also be recalled) would improve crisis stability. Advocates also maintained that, since the United States enjoyed a technological edge over the Soviet Union in bombers and cruise missiles, American strategic superiority would be enhanced in a world without ballistic missiles.

Critics countered that Moscow was unlikely to agree to any such proposals precisely because they would cede a strategic advantage to Washington.[15] Moreover, they maintained, such an arrangement would simply produce a new arms race in bombers and cruise missiles that could be even more destabilizing than a world with ballistic missiles. After all, an ICBM launch at least provides an enemy with approximately 30 minutes of warning, but a nuclear detonation conducted with stealthy aircraft or cruise missiles of the future could occur before the targets of the attack even knew what hit them. Finally, critics argued that as long as nuclear weapons were also intended to deter large-scale conventional, not just nuclear, conflict, then the threat of prompt retaliation provided by ICBMs was necessary. In this view, the "instability" produced by ICBMs was at least partly an advantage, not limitation.

Still, proponents produced detailed proposals about how negotiations toward a ZBM could begin between the superpowers and then expand over time to include regional nuclear-armed states until the goal of zero ballistic missiles was finally achieved.[16] Debates in the immediate post-Cold War about worldwide ballistic missile elimination reflected an optimism about the future security environment that does not exist today.[17] The nuclear threat environment has deteriorated over the past several years, and great power political competition has returned. Moreover, even in the heady days of the early 1990s, eliminating ICBMs proved impossible. Nevertheless, arguments about ICBM elimination have recently returned. This time, however, proponents do not argue that the

risk is a deliberate Russian nuclear first strike but that the United States might use its ICBMs first by accident. Moreover, they maintain that the United States should unilaterally disarm, even if there is little prospect of Russia following suit.[18]

ICBMs Under Renewed Attack

Plans to maintain or modernize the ICBM force have come under renewed attack in recent years, despite ICBMs' long pedigree and broad bipartisan political support. Prominent critics charge that ICBMs are unnecessary for deterrence, that they undermine nuclear strategic stability, and that their modernization costs are unaffordable.

Unnecessary for Deterrence

Tom Collina, policy director for the Ploughshares Fund, argues that the ground-based strategic deterrent is redundant and unnecessary for nuclear deterrence since the United States already has "enough nukes on subs to deter any potential attacker."[19] He and other critics argue that because the other two legs of the triad are sufficient to deter any enemy nuclear attack, the ICBM force is expendable. They maintain that since a new strategic bomber will be necessary for conventional missions, its modernization is guaranteed.[20] They further stipulate that submarine-launched ballistic missiles (SLBM), deployed on submarines at sea, are survivable. ICBMs, on the other hand, located in fixed and known locations, are vulnerable to an enemy nuclear first strike.[21] Moreover, since ICBMs contain an older guidance system than SLBMs, they are also less accurate, rendering them less useful for counterforce targeting and increasing the potential for unnecessary collateral damage.[22] Finally, they maintain, SLBMs and bombers can carry sufficient nuclear firepower to impose unacceptable costs on an adversary. Given these considerations, critics conclude that the ICBM force is unnecessary. As journalist Fred Kaplan put the argument in *Foreign Affairs*, "the case for land-based ICBMs today is extremely weak."[23]

Undermine Nuclear Strategic Stability

The second charge against the ICBM force is that it undermines nuclear strategic stability and increases the risk of accidental nuclear war. For decades, the United States has maintained a launch under attack (LUA)

option.[24] Since ICBMs in fixed silos are potentially vulnerable to an enemy nuclear first strike, the United States announces that it will not wait to have its missiles destroyed but, instead, reserves the right to launch ICBMs upon receiving warning of an incoming attack. The LUA option is meant to contribute to deterrence by making it clear to adversaries they cannot count on destroying the US ICBMs in their silos, even if they strike first. However, ICBM critics charge—pointing to historical near misses—that this policy could lead to accidental nuclear war.[25] As Perry argues, "These missiles are some of the most dangerous weapons in the world. They could even trigger an accidental nuclear war."[26] And Perry and Cartwright aver that these are "higher risks of accidental war that, fortunately, we no longer need to bear."[27] A false alarm could cause a US president to launch a nuclear war under the mistaken belief that a nuclear war has already begun. To avoid this danger altogether, therefore, ICBM critics advocate eliminating ICBMs. Since submarines at sea are less vulnerable to a nuclear first strike and bombers can be sent into the air in a crisis, the pressures to "use them or lose them" are less intense. Detractors maintain that the risks of having ICBMs on "hair-trigger alert" are simply too great.[28]

Unaffordable

The final argument for eliminating the US ICBM force is that they are too expensive. Again, as Perry and Cartwright believe, "we are safer without these expensive weapons, and it would be foolish to replace them."[29] The Congressional Budget Office estimates that the price tag of modernizing America's nuclear triad over the coming 30 years will come to over $1 trillion.[30] This is a large sum, and those opposed to nuclear modernization argue that the United States can save money by scaling back its plans, including delaying modernization of, or scrapping altogether, the ICBM force.[31] In addition, critics argue that allocating large sums to nuclear forces takes away from investment in other more useable conventional military capabilities. For example, Collina argues that "avoiding production of a new ICBM would save tens of billions."[32] Perry maintains that the US modernization plan "is needlessly oversized and expensive" and will "crowd out the funding needed to sustain the competitive edge of our conventional forces and to build the capacities needed to deal with terrorism and cyberattacks."[33] Instead, Perry and

Cartwright maintain, Washington "should cancel plans to replace its ground-based ICBMs, which would save $149 billion."[34]

The Case for the ICBM Force

Contrary to the above claims, ICBMs are a necessary part of US nuclear strategy. They contribute to US nuclear strategy, do not undermine strategic stability, and are affordable. The analysis below shows that ICBMs should continue to occupy an important role in US nuclear posture.

ICBMs Are Necessary for US Nuclear Strategy

ICBMs possess a number of unique attributes that strengthen nuclear deterrence overall. They not only provide deterrence against attack on the United States, but they also contribute to other roles and missions, including assuring allies and achieving US objectives if deterrence fails.

Launching a successful nuclear first strike on a United States armed with hundreds of ground-based ballistic missiles in hardened silos spread throughout the interior of the country would be a near-insurmountable task. Without ICBMs such a first strike would be much easier to contemplate. This fact has long been recognized and has sometimes been described as the "sponge" or "warhead sink" argument for ICBMs.[35]

The existence of an ICBM force greatly raises the opening ante for a nuclear first strike on the United States. Major nuclear powers, like Russia and the United States, include counterforce nuclear targeting in their war plans.[36] In other words, they plan to use their nuclear weapons to destroy an enemy's nuclear weapons. The more enemy nuclear weapons that can be destroyed, the fewer that will land in retaliation on one's own territory. An adversary plotting a counterforce nuclear first strike on the United States would need to target at least 455 sites on the US mainland. This list of targets includes three strategic bomber bases in Louisiana, Missouri, and North Dakota and two strategic submarine bases in Georgia and Washington state.[37] Finally—and most importantly—the enemy would need to target and attempt to destroy 450 separate ICBM silos spread across hundreds of miles in Wyoming, North Dakota, and Montana. There are many other targets an enemy might also seek to destroy in a first strike, including those related to nuclear command and control, missile defense sites, war-sustaining industries, and others. But the bare minimum for a splendid first strike on US nuclear forces at

present requires destroying at least 455 targets. That is a daunting, if not impossible, objective, even for a major nuclear power like Russia.

The attempt would require an adversary to expend much of its nuclear arsenal. To ensure the destruction of a target, it is believed that states would want to allocate more than one warhead to each aim point; a common rule of thumb is two warheads per target.[38] An enemy nuclear strike on 450 hardened ballistic missile silos in the United States, therefore, would require the enemy to generate an offensive force package of approximately 900 nuclear warheads. Such an operation is simply not possible for two of America's three nuclear adversaries. China and North Korea are believed to possess arsenals numbering around 260 and 30–60 nuclear warheads, respectively.[39] While feasible for Russia, with its larger number of nuclear weapons, it would still require Moscow to expend roughly two-thirds of its deployed, strategic nuclear arsenal in a bid to destroy US ICBMs.[40]

It is difficult to imagine an adversary deciding to intentionally launch a nuclear first strike on the United States under these conditions. The attack would require detonating nearly one thousand nuclear weapons on hundreds of sites spread throughout the US homeland. It would be impossible to keep such a strike limited. There is a reasonable chance it would not succeed in destroying every target, and a US president would be compelled to respond. These considerations strengthen nuclear deterrence.

Subtract the ICBMs from this equation, however, and the picture greatly changes. Adversaries could concentrate their efforts on the remaining two legs of the triad. The opening ante for a nuclear attack on the United States plummets to only five sites. The number of nuclear weapons needed to cover these targets collapses to a mere 10 nuclear warheads. This greatly lowers the bar for nuclear deterrence. With a target set this small, Russia and China could conduct a first strike and still hold hundreds of nuclear warheads in reserve. Even a minimally armed rogue state such as North Korea could contemplate such an attack.

To be sure, even if an enemy attempted such an attack, the United States would retain a retaliatory nuclear force. The enemy might fail to destroy every target and US nuclear submarines on deterrence patrol would survive. This remaining force, however, would be diminished. Moreover, the enemy could attempt to combine the nuclear first strike with an antisubmarine warfare campaign, missile defense intercepts, and other efforts intended to deny America's retaliatory capability. In this

condition, the enemy might be tempted to conduct an attack and use its remaining nuclear forces to "deter our deterrent."[41] While an intentional enemy nuclear first strike on the United States would remain highly unlikely, it would undoubtedly be easier to plan and execute in the absence of a US ICBM force.

Some ICBM critics, including Fred Kaplan, recognize the value of ICBMs as a warhead sink, but they maintain that such a function could be served at much lower numbers, such as one dozen ICBMs.[42] This is a subject worth more serious discussion. Greatly reducing ICBM numbers, however, would begin to undermine the ICBM's deterrence function. Reducing numbers would make an enemy first strike more effective, allow larger adversaries to consider a nuclear first strike while holding a larger nuclear force in reserve, and place a first strike within reach for smaller powers, such as North Korea. Most importantly, deep ICBM reductions conflict with another important US goal: achieving its objectives if deterrence fails.

In addition, eliminating the US ICBM force may also weaken deterrence by encouraging adversaries to initiate or escalate crises against the United States and its allies, thus increasing the risk of a nuclear crisis and nuclear war. The debate continues over whether nuclear superiority is useful for deterrence and coercion—with many scholars arguing superiority does not matter. Recently one side of the argument finds that nuclear superior states are more likely to initiate militarized compellent threats against other nuclear-armed states and more likely to achieve their goals in high-stakes crises.[43] If the United States were to unilaterally eliminate its ICBM force, as some ICBM critics advocate, it would cede a large nuclear advantage to Russia, possibly increasing Moscow's willingness to challenge the United States and its allies in dangerous militarized disputes.[44]

Finally, the nuclear force envisioned in the current round of modernization efforts will need to last decades. Modern ICBMs will help ensure against potential technological breakthroughs that could soon make the seas more transparent, calling into question the survivability of the sea-based leg.[45] It would be unwise, therefore, for US nuclear strategy to depend on the assumption that nuclear-armed submarines will always be survivable. In sum, the US ICBM force strengthens nuclear deterrence, but not only for the US.

ICBMs also play a crucial role in extending deterrence and assuring US allies. The United States aims not only to deter attacks on itself but also to extend deterrence to over 30 allies and partners in Europe and Asia. The US nuclear umbrella helps maintain stability in important geographic regions and dissuades allies from taking steps that would be contrary to US interests, such as building independent nuclear arsenals.[46]

ICBMs have a number of positive attributes that can contribute to extended deterrence and assurance, including promptness and reliability. Unlike other legs of the triad, ICBMs are always on alert, and they can promptly strike any target on Earth in 30 minutes or less. Bombers and nuclear-capable fighter aircraft require hours to reach an intended target. SLBMs also generally take more time, depending on their position. Moreover, ICBMs are also the most reliable leg of the triad. There could conceivably be issues communicating to submarines at sea or bombers in flight, but the ground-based deterrent, securely located within the US homeland, possesses the most assured command and control links, allowing it to reliably receive and respond to launch orders.[47]

One can debate the value of these attributes, but America's security partners are the final arbiters of what policies, strategies, and capabilities they find reassuring, and they have consistently voiced support for the maintenance and modernization of the US ICBM force. Jacek Durkalec, a Polish defense expert, argues, "it is hard to imagine that without the ICBM force, the US would be able to maintain a parity in strategic forces with Russia."[48] He worries that this could undermine strategic stability, embolden Russia to behave more aggressively, and reduce Moscow's incentives to negotiate future arms control agreements. Most importantly, he is concerned that "if the US eliminates its ICBMs while Russia retains similar capabilities, this might improve Russia's psychological position to blackmail US allies."

Sugio Takahashi, a leading Japanese nuclear expert, argues that ICBMs are critical for the US ability to extend deterrence to Japan.[49] He maintains that to credibly extend deterrence, the United States must maintain a capability for nuclear preemption against North Korea, to physically protect Tokyo from any imminent nuclear attack. If the United States and Japan had credible evidence that Pyongyang were on the verge of mounting an attack, US nuclear-armed aircraft would be unlikely to arrive in time and Tokyo could not be certain about the position of SLBMs, but they would be assured that US ICBMs could arrive in less

than a half hour. In his view, the promptness and reliability of the ICBM contribute to assurance.

South Korean experts also see ICBMs as a critical component of extended deterrence and assurance. James Kim, a research fellow at the Asan Institute for Policy Studies in Seoul, has stated, "I do not see how one can make the case that the security interests of the US and its allies can be protected without a fully functioning and capable nuclear arsenal, including ICBMs."[50] He continues, "ICBMs are not the only requirements of extended deterrence, but they are necessary."

Moreover, there is the additional question of how a US decision to shed a leg of the nuclear triad would be interpreted around the world. Deterrence theorists argue that many threats and promises in international politics are nothing more than "cheap talk," but that states can signal credibility by "sinking costs."[51] In other words, threats and promises are more believable if states back up their words, by putting money where their mouths are. Investing billions to modernize the ICBM force sends a clear and "costly signal" of the US commitment to nuclear deterrence. If, on the other hand, the United States cancels plans to modernize its nuclear forces, allies may question whether Washington remains committed to the extended nuclear deterrence mission.[52] As Kim argues, "a significant portion of the South Korean public has begun to question the strength of US security guarantees. One way the United States can address this challenge is by continuing to update and strengthen force readiness and defense modernization. ICBM modernization is part of this process."[53]

Finally, ICBMs can save millions of American lives. This may be the most important role of US ICBMs. While many nuclear strategists focus exclusively on deterrence, policy makers must also consider what happens if, God forbid, deterrence fails.[54] The 2018 *Nuclear Posture Review* sets out "achiev(ing) US objectives should deterrence fail" as one of four major roles of US nuclear weapons. It explains that "US nuclear policy for decades has consistently included this objective of limiting damage if deterrence fails."[55] The maintenance of an ICBM force greatly contributes to America's damage limitation capability.

To explain this point, consider hypothetical nuclear exchanges between the United States and Russia. First, imagine that Russia conducts a nuclear first strike against the United States. As stated above, it is believed that Russia's nuclear strategy calls for counterforce strikes. In addition, it is

also believed that, in the event of a large-scale nuclear exchange, Moscow would use remaining forces for countervalue attacks aimed to maximize destruction to the US homeland or as bargaining leverage to end the conflict on its terms.[56] With a US ICBM force in place, Russia would need to allocate 900 nuclear warheads to destroying US ICBM silos. Again, this is why US ICBMs are sometimes referred to as a "warhead sink." If, however, the US ICBMs were eliminated, these 900 nuclear weapons would be available to attack other targets, including countervalue targets affecting hundreds of additional US population centers. Conducting detailed nuclear exchange calculations, I estimate that a Russian nuclear first strike on the United States with an ICBM force in place would result in 70 million US casualties.[57] With the ICBM force removed, this figure rises to approximately 125 million casualties. To argue, therefore, that the United States can safely eliminate ICBMs, one would have to maintain that it does not matter whether 55 million Americans live or die in the event of a Russian attack. This may be an acceptable cost to some, but the history of US nuclear strategy has shown that policy makers responsible for protecting American lives prefer a plan that limits damage if deterrence fails. They are not comfortable needlessly risking tens of millions of additional American lives in the event of enemy nuclear attack.

Indeed, the United States could strengthen damage limitation by increasing its number of ICBMs. This would reduce the adversary's warheads available for urban strikes, and the 2:1 shot ratio would force the opponent into an unfavorable cost position.

The result is similar if we consider a situation in which the United States strikes first with a large-scale nuclear attack. This scenario is unlikely but possible, if, for example, Russia launched a major conventional attack, a major nonnuclear strategic attack, or a limited nuclear attack against the United States or its allies. With ICBMs, the United States possesses 400 nuclear warheads it can use in counterforce strikes on Russia's nuclear forces. At two offensive warheads for every counterforce target, this would result in the destruction of up to 200 Russian nuclear weapons-related targets before those weapons could be used against US or allied territory. In contrast, if the United States eliminated its ICBMs, it would have fewer forces with which to blunt Russia's nuclear retaliatory capability. Indeed, if the United States were to eliminate ICBMs, Washington might need to consider abandoning counterforce targeting

and the damage limitation element of its strategy altogether. Assuming, however, that the United States persisted with a counterforce targeting strategy even without ICBMs, the US ability to limit damage would be greatly reduced. By my calculation, a Russian second strike on the United States, following a US first strike that included ICBMs, would result in 28 million US casualties. In contrast, the same scenario without US ICBMs would cause 82 million casualties. The difference is once again approximately 50 million American lives.

The United States can reduce its number of ICBMs as some critics suggest or eliminate them altogether, but for every US ICBM it cuts, it may expose additional American lives to the threat of direct nuclear attack. The existence of the ICBM force, therefore, can contribute to the goal of damage limitation.

ICBMs Do Not Undermine Nuclear Strategic Stability

Not only do ICBMs contribute to US nuclear strategy, they also do not undermine nuclear strategic stability as critics claim. Above, we saw how ICBMs contribute to the deterrence of US adversaries and, therefore, to strategic stability. To be sure, there is always some risk of accident involved with nuclear weapons, but the United States practices a number of safeguards to reduce the risks of an accidental nuclear launch. For example, the United States practices broad open ocean targeting, which would reduce the implications of any accident.[58] On balance, therefore, there is good reason to believe that ICBMs do more to contribute to stability than to undermine it.

But critics have recently argued that ICBMs increase the risk of accidental nuclear war, are destabilizing in the event of an impending nuclear attack, and therefore should be eliminated. This claim, however, rests on a logical contradiction and is inconsistent with decades of empirical evidence. Critics maintain that a US president would want to launch ICBMs before they could be wiped out in an enemy first strike. This pressure to act quickly increases the risk that the president could launch an accidental nuclear war due to a false alarm. But this argument raises the question: why is the president so eager to use ICBMs before they can be eliminated? Presumably, because the president believes that using ICBMs is critical for the United States to achieve its objectives. Indeed, this unstated objective must be fairly important if the president is willing to run a possible risk of launching an accidental nuclear war to

achieve it. If, launching ICBMs is so crucial to US strategy, then it does not make sense for the United States to eliminate them.

If, on the other hand, the critics are correct and the United States can safely eliminate ICBMs, then there is no reason why a president should be so eager to use ICBMs early in a crisis before they can be wiped out. If the United States can afford to eliminate its nuclear weapons now, in peacetime, then a US president can also afford to wait and ride out any attack on the ICBM force in the event of hostilities. If ICBMs are truly expendable, then there is no reason to risk an accidental nuclear war just to avoid losing them.

In sum, one can hold two logically coherent positions. First, one can maintain that US ICBMs are necessary for US nuclear strategy, but they carry some inherent risk of accidental nuclear use. Second, one can hold that ICBMs are unnecessary for US nuclear strategy and there is, therefore, no reason for a US president to launch them early in a crisis. But, the critics' position contains a logical contradiction. They maintain that ICBMs are both unnecessary and so essential that a US president would feel great pressure to use them early in a crisis.

Moreover, the argument that ICBMs increase the risk of nuclear war is not supported by the empirical evidence. The United States, Russia, and China have all possessed silo-based ICBMs for decades without an accidental nuclear launch. Critics such as Perry have argued that there have been scares and close calls, a debatable proposition, but the fact is, ICBMs have never been launched due to a false alarm or accident.[59] Further, those in a position of authority have consistently decided that the benefits of ICBMs outweigh the risks. The United States built and possessed ICBMs for decades and US adversaries are building and modernizing ICBMs today.

ICBMs Are Affordable

Finally, contrary to the arguments of the critics, ICBMs are affordable. The full cost of US nuclear modernization, estimated at over $1 trillion over 30 years, is certainly a large sum. Many figures for US government spending are so large, however, that they are hard to fathom. To put this number into perspective, nuclear modernization costs will make up approximately 5 to 7 percent of the US defense budget. This is also much smaller than historic levels of spending on nuclear forces, which regularly reached 10 to 15 percent of the defense budget during the

Cold War. In the end, cost arguments for nuclear reductions are not persuasive. As David Mosher argued, looking for savings in nuclear forces is a "hunt for small potatoes."[60] And, as former Secretary of Defense Ash Carter put it, "nuclear weapons don't actually cost that much."[61]

Furthermore, it is puzzling that critics cite costs as a reason to cut ICBMs, because they are the least costly leg of the triad. Placing a nuclear weapon in a fixed silo at existing sites is much cheaper than building a new stealth bomber or a new nuclear-powered submarine. The Congressional Budget Office projects that the cost of modernizing the ICBM, bomber, and SLBM comes to $149 billion, $266 billion, and $313 billion, respectively, over the next 30 years.[62] Moreover, the annual operating costs of each leg are estimated at $1.4 billion for ICBMs, $1.8 billion for bombers, and $3.8 billion for SLBMs. If cost savings are a top priority, then the ICBM force should not be the first leg on the chopping block.

Most importantly, beginning with Chuck Hagel, each successive US secretary of defense has maintained that nuclear deterrence is the most important mission of the Department of Defense.[63] Reasonable people can certainly disagree, but 5 to 7 percent of the defense budget for the most important defense mission of US should be interpreted as not only affordable but as a good bargain.

Conclusion: The Future of the ICBM Force

This article made the case for the US ICBM force. Contrary to the claims of critics, this article demonstrated that ICBMs contribute to US nuclear strategy by enhancing deterrence and assurance and helping Washington achieve its objectives should deterrence fail. Rather than scrapping the ICBM force as critics have advocated, therefore, the United States should maintain and modernize this leg of the nuclear triad as planned.

The argument here has implications for both scholars and practitioners. Leading theories of nuclear deterrence identify a secure second-strike capability as the distinguishing feature of the "nuclear revolution" and, therefore, the most important capability for ensuring nuclear deterrence.[64] States that lack such a capability may be vulnerable to a nuclear first strike, but states with an assured retaliatory capability can reliably deter enemy nuclear attack. This theoretical starting point biases scholars to a single-minded focus on survivability as the most important attri-

bute of a nuclear force. As the above analysis demonstrates, however, US nuclear strategy aims to achieve more with its nuclear weapons than simply deterrence of enemy nuclear attack on the US. There are other attributes of a nuclear force beyond survivability that matter for these other interests. Scholars can, therefore, broaden their aperture to consider other attributes of nuclear forces and how they influence world politics, including their ability to contribute to assurance and damage limitation.[65]

For practitioners, the most important implication of this analysis is that US national security requires the United States to maintain and modernize ICBMs. Technology has advanced significantly in the past 50 years, and Washington can use the upcoming modernization cycle as an opportunity to enhance the positive attributes of the ICBM force. ICBMs are currently less accurate than US SLBMs, and their relatively large warheads could result in high levels of collateral damage.[66] This could render them less credible as a deterrent or assurant or less desirable for employment in damage-limitation missions. These deficiencies can be addressed in the modernization process. The new GBSD can harness new technology to improve the missile's accuracy and provide lower-yield options that can be appropriately tailored to the threat environment. These enhancements can contribute to deterrence, assurance, and damage limitation and to US national security more broadly.

In sum, the ICBM force should retain a prominent role in America's nuclear posture. A robust nuclear force spread throughout the US homeland raises the bar for a successful enemy nuclear first strike and makes it less likely a US president will ever need to face an anguished decision about nuclear retaliation. As Secretary of Defense James Mattis put it, speaking in defense of US nuclear forces, "What we're trying to do is set such a stance with our triad that these weapons must never be used."[67] SSQ

Notes

1. Hans M. Kristensen and Robert S. Norris, "United States Nuclear Forces, 2017," *Bulletin of the Atomic Scientists* 73, no. 1 (14 December 2016): 50, https://thebulletin.org/2017/january/united-states-nuclear-forces-201710380.

2. Congressional Budget Office, *Approaches for Managing the Costs of US Nuclear Forces, 2017 to 2046* (Washington, DC: Congressional Budget Office, 31 October 2017), 2, 17–18, https://www.cbo.gov/publication/53211.

3. Aaron Mehta, "Carter: Nuclear Triad 'Bedrock of Our Security,' " Defense News, 26 September 2016, https://www.defensenews.com/pentagon/2016/09/26/carter-nuclear-triad-bedrock-of-our-security/.

4. Leon Sloss, "A World without Ballistic Missiles," *International Security* 12, no. 1 (1987): 184–89, https://www.jstor.org/stable/2538924; Alton Frye, "Zero Ballistic Missiles," *Foreign Policy*, no. 88 (1992): 3–20; Richard Perle, "Reykjavik as a Watershed in US-Soviet Arms Control," *International Security* 12, no. 1 (1987): 175–78, https://www.jstor.org/stable/2538922; J. Jerome Holton, Lora Lumpe, and Jeremy J. Stone, "Proposal for a Zero Ballistic Missile Regime," *Science and International Security Anthology* (Washington, DC: AAAS, 1993), 379–96, https://fas.org/asmp/library/articles/zerobal93.htm; Randall Forsberg, "Abolishing Ballistic Missiles: Pros and Cons," *International Security* 12, no. 1 (1987): 190–96, https://www.jstor.org/stable/2538925; and Thomas C. Schelling. "Abolition of Ballistic Missiles," *International Security* 12, no. 1 (1987): 179–83, https://www.jstor.org/stable/2538923.

5. William J. Perry, "Why It's Safe to Scrap America's ICBMs," *New York Times*, 30 September 2016, https://www.nytimes.com/2016/09/30/opinion/why-its-safe-to-scrap-americas-icbms.html; William J. Perry and James E. Cartwright, "Spending Less on Nuclear Weapons Could Actually Make Us Safer," *Washington Post*, 16 November 2017, https://www.washingtonpost.com/amphtml/opinions/spending-less-on-nuclear-weapons-could-actually-make-us-safer/2017/11/16/396ef0c6-ca56-11e7-aa96-54417592cf72_story.html; Tom Collina (policy director, Ploughshares Fund, San Francisco, CA), interview by Will Lowry, 2 August 2016, transcript, https://www.ploughshares.org/issues-analysis/article/its-time-retire-icbm; Fred Kaplan, "Rethinking Nuclear Policy," *Foreign Affairs* 95, no. 5 (September/October 2016), https://www.foreignaffairs.com/articles/americas/2016-08-01/rethinking-nuclear-policy; and Scot J. Paltrow, "Special Report: Nuclear Strategists Call for Bold Move: Scrap ICBM Arsenal," Reuters, 22 November 2017, http://mobile.reuters.com/article/amp/idUSKBN1DM1D2.

6. Perry, "Why It's Safe to Scrap America's ICBM's"; Perry and Cartwright, "Spending Less"; Collina, interview; Fred Kaplan, "*Dr. Strangelove* Was a Documentary," Slate, 4 December 2017, http://www.slate.com/articles/arts/books/2017/12/the_doomsday_machine_daniel_ellsberg_s_sobering_new_memoir_about_life_as.html?wpsrc=sh_all_dt_fb_ru; and Paltrow, "Nuclear Strategists Call for Bold Move."

7. Perry, "Why It's Safe to Scrap America's ICBM's"; Perry and Cartwright, "Spending Less"; Collina, interview; Tom Z. Collina, *The Unaffordable Arsenal: Reducing the Costs of the Bloated US Nuclear Stockpile* (Washington, DC: Arms Control Association, October 2014); and Kaplan, "Rethinking Nuclear Policy."

8. On these and other roles of US nuclear weapons, see the "Nuclear Posture Review of the United States of America," US Department of Defense, February 2018.

9. James Mattis, Secretary of Defense (address, Naval Base, Kitsap, WA, 9 August 2017).

10. See, for example, Roger Burg, "America's Nuclear Backbone: The Value of ICBMs and the New Ground-Based Strategic Deterrent," The Mitchell Institute, January 2017.

11. Sloss, "A World without Ballistic Missiles"; Frye, "Zero Ballistic Missiles"; Perle, "Reykjavik as a Watershed in US-Soviet Arms Control"; Holton, Lumpe, and Stone, "Proposal for a Zero Ballistic Missile Regime"; Forsberg, "Abolishing Ballistic Missiles: Pros and Cons"; and Schelling, "Abolition of Ballistic Missiles."

12. Sloss, "A World without Ballistic Missiles"; Frye, "Zero Ballistic Missiles"; Perle, "Reykjavik as a Watershed in US-Soviet Arms Control"; Holton, Lumpe, and Stone, "Proposal for a Zero Ballistic Missile Regime"; Forsberg, "Abolishing Ballistic Missiles: Pros and Cons"; and Schelling, "Abolition of Ballistic Missiles."

13. "Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Elimination of their Intermediate-Range and Shorter-Range Missiles," 8 December 1987.

14. Perle, "Reykjavik as a Watershed in US-Soviet Arms Control"; Schelling, "Abolition of Ballistic Missiles."

15. Sloss, "A World without Ballistic Missiles"; and Forsberg, "Abolishing Ballistic Missiles: Pros and Cons."

16. Frye, "Zero Ballistic Missiles"; and Holton, Lumpe, and Stone, "Proposal for a Zero Ballistic Missile Regime."

17. "Nuclear Posture Review of the United States of America," US Department of Defense, February 2018.

18. Perry, "Why It's Safe to Scrap America's ICBMs."

19. Collina, interview.

20. Perry, "Why It's Safe to Scrap America's ICBMs"; and Perry and Cartwright, "Spending Less."

21. Kaplan, "Rethinking Nuclear Policy."

22. Kaplan, "Rethinking Nuclear Policy."

23. Kaplan, "Rethinking Nuclear Policy."

24. William Burr, ed., "Launch on Warning: The Development of US Capabilities, 1959–1979," *National Security Archive Electronic Briefing Book*, no. 43 (Washington, DC: The National Security Archive – The George Washington University, April 2001), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB43/#3.

25. Kaplan, "Dr. Strangelove was a Documentary"; Paltrow, "Nuclear Strategists Call for Bold Move"; Perry, "Why It's Safe to Scrap America's ICBMs"; and Perry and Cartwright, "Spending Less."

26. Perry, "Why It's Safe to Scrap America's ICBMs."

27. Perry and Cartwright, "Spending Less."

28. For a rebuttal of the term "hair trigger alert" see Gen Kevin P. Chilton, USAF, retired, "Defending the Record on US Nuclear Deterrence," *Strategic Studies Quarterly* 12, no. 1 (Spring 2018): 16, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-12_Issue-1/Chilton.pdf?ver=2018-02-14-170000-437.

29. Perry and Cartwright, "Spending Less."

30. Congressional Budget Office, "Approaches for Managing the Costs," 1–2, 15–17.

31. Collina, interview; Collina, *The Unaffordable Arsenal*; Perry, "Why It's Safe to Scrap America's ICBMs"; and Perry and Cartwright, "Spending Less."

32. Collina, *The Unaffordable Arsenal*, 14.

33. Perry, "Why It's Safe to Scrap America's ICBMs."

34. Perry and Cartwright, "Spending Less."

35. Barbara G. Levi, Mark Sakitt, and Art Hobson, eds. *The Future of Land-Based Strategic Missiles* (New York: American Institute of Physics, June 1989), 3, 87–95.

36. Department of Defense, *Report on Nuclear Employment Strategy of the United States* (Washington, DC: Department of Defense, 12 June 2013), 4; and Matthew Kroenig, *Approaching Critical Mass: Asia's Multipolar Nuclear Future National Bureau of Asia Research*, June 2016, http://www.nbr.org/publications/element.aspx?id=897.

37. Kristensen and Norris, "United States Nuclear Forces, 2017."

38. Theodore A. Postal, "Targeting," in *Managing Nuclear Operations*, ed. Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket (Washington, DC: Brookings Institution, 1987), 373–406.

39. Hans M. Kristensen and Robert S. Norris, "Worldwide Deployments of Nuclear Weapons, 2017," *Bulletin of the Atomic Scientists* 73, no. 5 (31 August 2017): 290, 294, https://thebulletin.org/2017/09/worldwide-deployments-of-nuclear-weapons-2017/; and Joby War-

rick, Ellen Nakashima, and Anna Fifield, "North Korea Now Making Missile-Ready Nuclear Weapons, US Analysts Say," *Washington Post*, 8 August 2017, https://www.washingtonpost.com/world/national-security/north-korea-now-making-missile-ready-nuclear-weapons-us-analysts-say/2017/08/08/e14b882a-7b6b-11e7-9d08-b79f191668ed_story.html?utm_term=.1ca390cb6c21.

40. Hans M. Kristensen and Robert S. Norris, "Russian Nuclear Forces, 2017," *Bulletin of the Atomic Scientists* 73, no. 2 (28 February 2017): 116–20, https://thebulletin.org/2017/03/russian-nuclear-forces-2017/.

41. Paul H. Nitze, "Deterring our Deterrent," *Foreign Policy*, no. 25 (Winter, 1975–1976): 195–210, https://www.jstor.org/stable/1148029.

42. Kaplan, "Rethinking Nuclear Policy."

43. Matthew Kroenig, *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters* (New York: Oxford University Press, 2018). For aspects of the opposite argument, see Todd Sechser and Matthew Fuhrmann, *Nuclear Weapons and Coercive Diplomacy* (New York: Cambridge University Press, 2017).

44. Global Zero, *Global Zero US Nuclear Policy Commission Report: Modernizing US Nuclear Strategy, Force Structure, and Posture* (Washington, DC: Global Zero, May 2012).

45. See, for example, "Hunting Submarines with Magnets," *The Economist*, 12 November 2016, https://www.economist.com/news/science-and-technology/21709948-new-way-detect-even-quietest-boats-hunting-submarines-magnets; and Stephen Chen, "Has China Developed the World's Most Powerful Submarine Detector?," *South China Morning Post*, 24 June 2017, http://www.scmp.com/news/china/society/article/2099640/has-china-developed-worlds-most-powerful-submarine-detector.

46. Francis J. Gavin, "Strategies of Inhibition: US Grand Strategy, the Nuclear Revolution, and Nonproliferation," *International Security* 40, no. 1 (1 July 2015): 9–46, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00205.

47. Maj Gen C. Donald Alston, *Deterrence and the ICBM: A Practitioner's Perspective* (Vienna, VA: The Potomac Foundation, November 2017).

48. Jacek Durkalec, Polish defense expert, to the author, email, January 2018.

49. Sugio Takahashi, "Thinking about the Unthinkable: The Case of the Korean Peninsula," in *North Korea and Asia's Evolving Nuclear Landscape: Challenges to Regional Stability*, NBR Special Report, no. 67 (August 2017), 27–36, http://www.nbr.org/publications/specialreport/pdf/sr67_north_korea_and_asias_evolving_nuclear_landscape_august2017.pdf.

50. Interview by the author, 2 January 2018.

51. James D. Fearon, "Signaling Foreign Policy Interests: Tying Hands versus Sinking Costs," *Journal of Conflict Resolution* 41, no. 1 (1 February 1997): 68–90, http://www.jstor.org/stable/174487?origin=JSTOR-pdf.

52. The US could try to manage this problem by re-allocating funds to conventional weapons to defend allies, but this would do little to alleviate allies' concerns about the credibility of US nuclear deterrence.

53. Interview by the author, 2 January 2018.

54. Department of Defense, *Report on Nuclear Employment Strategy of the United States*, 4–5; and Harold Brown, *Annual Report FY 1981* (Washington, DC: Department of Defense, 29 January 1980), 66.

55. US Nuclear Posture Review, February 2018.

56. Russian nuclear expert, interview by the author, January 2016. Information obtained under conditions of nonattribution.

57. All estimates from Kroenig, *The Logic of American Nuclear Strategy*, chap. 2.

58. Andrew Quinn, "U.S. Reveals Nuclear Target: Oceans," *Tales from the Trail* (blog), 6 April 2010, http://blogs.reuters.com/talesfromthetrail/2010/04/06/u-s-reveals-nuclear-target-oceans/.

59. Perry, "Why It's Safe to Scrap America's ICBMs."

60. David Mosher, "The Hunt for Small Potatoes: Savings in Nuclear Deterrence Forces," in *Holding the Line: US Defense Alternatives for the Early 21st Century*, ed. Cindy Williams (Cambridge, MA: MIT Press, 2001), 119–40.

61. Ashton Carter, "Remarks by Deputy Secretary of Defense Carter at the Aspen Security Forum at Aspen, Colorado" (discussion, Aspen Security Forum, Aspen, CO, 18 July 2013), transcript, http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5277.

62. Congressional Budget Office, "Approaches for Managing the Costs," 2, 15–18.

63. Chuck Hagel, "Statement on the Nuclear Enterprise Review and Reforms" (speech, Pentagon Press Briefing Room, Washington, DC, 14 November 2014), transcript, https://www.defense.gov/News/Speeches/Speech-View/Article/606634/statement-on-the-nuclear-enterprise-review-reforms/.

64. Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946); Thomas Schelling, *Arms and Influence* (New Haven: Yale University Press, 1969); Charles L. Glaser, *Analyzing Strategic Nuclear Policy* (Princeton, NJ: Princeton University Press, 1990), 361–70; Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, NY: Cornell University Press, 1989), 8–13; and Robert Powell, *Nuclear Deterrence Theory: The Search for Credibility* (New York: Cambridge University Press, 1990), 114–15.

65. "Nuclear Posture Review of the United States of America," US Department of Defense, February 2018; and Keir A. Lieber and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (1 April 2017): 9–49, https://doi.org/10.1162/ISEC_a_00273.

66. Kaplan, "Rethinking Nuclear Policy."

67. Aaron Mehta, "Mattis Enthusiastic on ICBMs, Tepid on Nuclear Cruise Missile," Defense News, 12 January 2017, https://www.defensenews.com/space/2017/01/12/mattis-enthusiastic-on-icbms-tepid-on-nuclear-cruise-missile/.

Russian Information Warfare: Implications for Deterrence Theory

Media Ajir and Bethany Vailliant

Abstract

The advanced threat of Russian disinformation campaigns against Western democracies and the United States in particular begs the questions: What are Russia's strategies for information warfare, and how can the United States combat them? This article explores the evolution of anti-Western propaganda coming from Russia in three ways: state-funded global social media networks, controlling Western media outlets, and direct lobbying of Western society. Recommendations to combat these threats include analysis of deterrence theory and its applicability to the domain of information warfare.[1]

❋❋❋❋❋

Having struggled to establish its place in the world, Russia has increasingly moved away from its short stint with democracy and toward its past authoritarianism. Formerly bound to promote Communist ideology, Russia is now a nation characterized by statism. Vladimir Putin and his cronies have largely defined this path. Since taking power in 2000, Putin has developed a strong nationalistic narrative, especially since his third term as president. This narrative incorporates traditional values at the individual level and a focus on returning the glory of the Soviet Union on the national level. To restore Russia's greatness, Putin has focused on solidifying his own power within Russia as well as returning to imperialist

Media Ajir is instructor of political science and international relations at the University of Nebraska–Omaha and Bellevue University. She holds a master of science degree in political science and a certificate in intelligence and national security from the University of Nebraska–Omaha. She is the recipient of the 2017 USSTRATCOM General Larry D. Welch Deterrence Writing Award.

Bethany Vailliant is a researcher for the National Strategic Research Institute (NSRI) and an instructor of international relations at the University of Nebraska–Omaha. She holds a master of science degree in political science and a certificate in intelligence and national security. She is a two-time winner of the USSTRATCOM General Larry D. Welch Deterrence Writing Award.

tendencies to grab land and people in the Russian "near-abroad" (the former Soviet Union states that have now gained their independence).

However, his ability to hold on to power and forays into Russia's near-abroad have not been enough. Russia continues to view itself in an ongoing and fierce competition with the Western world—and in particular the United States. For example, incidents such as the release of the Panama Papers, the annexation of Crimea, the passing of the Magnitsky Act, and the Olympic doping scandal have all inflamed the tension between Russia and the US. Therefore, Putin's recent power plays are made with a zero-sum mentality. Put simply, destabilization of the West is a means by which Putin pursues his goal of restoring Russia's lost greatness and holding on to power.

While it is a common perception in the West that Russia is acting offensively, there lies explanatory power as well in understanding that the Russians view their actions as being defensive in nature. In the Russian view, technology is a particular method the West uses to "attack" it—but less for inflicting crippling blows than as a way to spread unacceptable ideas, norms, practices, and behaviors. Russian intelligence services are increasingly worried about the potential detrimental national security effects arising from the internet. In fact, the vast majority of Russian writing on information conflict is defensive in tone and focused on information security due to their perception of the global information space as a serious threat to Russian sovereignty. The original Russian source government document "Doctrine of Information Security of the Russian Federation" states that there is a trend in foreign media to publish biased information about Russian state policy and that there is discrimination against Russian mass media. Additionally, they observe what they perceive as increasing pressure on the Russian population through Western propaganda efforts that "erode Russian traditional and spiritual and moral values."[2] The belief that the West was heavily involved in the color revolutions and in the Arab Spring, as well as with the protests preceding Putin's reelection in 2012, is a deeply held one. In response, Russia views the media and the internet as tools to defend its authoritarian state and ideology both at home and abroad through dissemination of its own views and propaganda efforts. To understand this fully, one must first consider Russian information warfare concepts before examining three specific Russian information warfare tools.

Russian Information Warfare Concepts

Information warfare, according to the original Russian government document *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*, is defined as confronting a state in the information space by damaging information systems, processes, and resources. These are of critical importance to undermine any political, economic, or social system, through what Russia deems "massive brainwashing" of the population to destabilize the society and the state. It also forces the confronted state to make decisions in the interests of the confronting party.[3] However, this is nothing new; the Soviet regime also used information weapons to help achieve these greater long-term goals. The first known use of the words "active measures" was in a Bolshevik document in 1919. By definition, active measures involve influencing events and behavior in, and the actions of, foreign countries.[4]

The Soviet intelligence active measures budget was reportedly $3–4 billion annually and employed well over 15,000 personnel. Active measures were employed to influence nations around the globe; however, the United States was always considered the main enemy, and the Soviets did not differentiate between peacetime and war.[5] Today, the same logic is employed. According to the Russian government, "The leadership and the command staff of all levels directly participate in the organization of the activity in the information space during peacetime and in wartime."[6]

The Soviets created the most threatening influence of its kind in the modern world.[7] To capture this, figure 1 shows how disinformation plays into the grand scheme of active measures. It begins with the overall goal of achieving an advantage in political warfare. There are several ways to operationalize this objective, of which disinformation is only one. Active measures that focused on disinformation represented a carefully constructed false message secretly introduced into the opponent's communication system to deceive decision makers and the public.

The next concept to understand is reflexive control theory—a term used to describe the practice of predetermining an adversary's decision-response by altering key factors in the adversary's perception of the world.[8] It takes the concept of disinformation one step further in that the crafted information message is inserted into an adversary's decision-

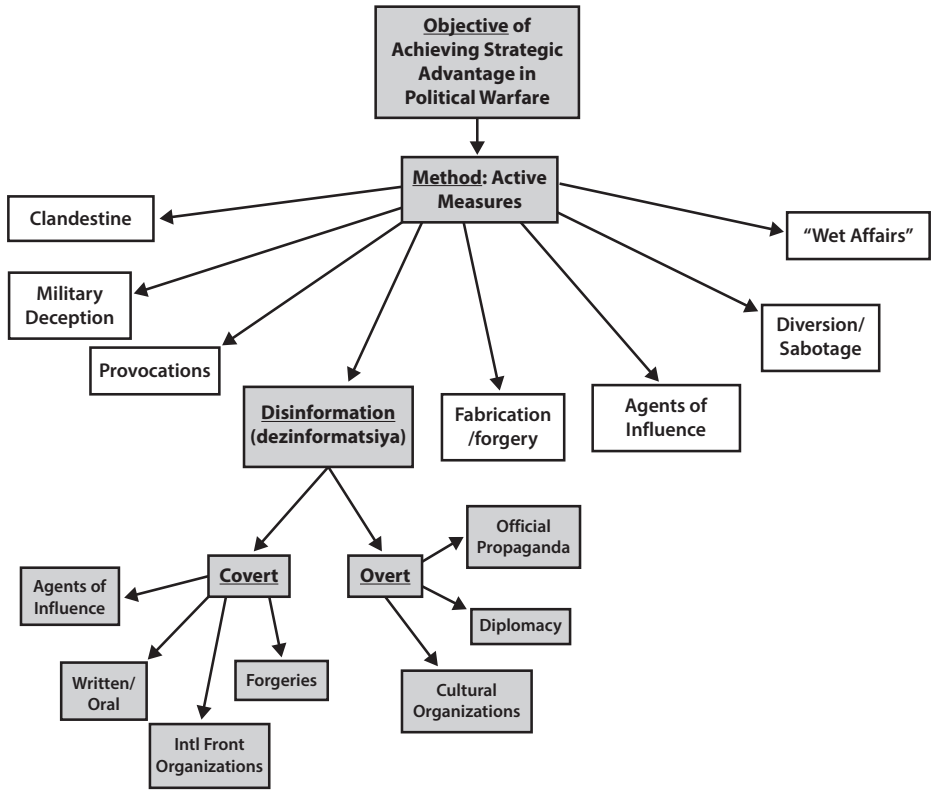

Figure 1. **Disinformation dissemination as subset of active measures.** "Agents of Influence" are used both as a subset of active measures and a subset of disinformation. (Source: Kevin McCauley, *Russian Influence Campaigns against the West: From the Cold War to Putin* [North Charleston, SC: Amazon Digital Services, 2016], 94, Kindle edition.)

making process to guide the opponent into making predetermined decisions and actions that are unfavorable to himself.[9] The central focus of reflexive control is on the less tangible aspects of decision making, such as the enemy's inner nature—his ideas and concepts—which is the filter through which passes all data about the external world.[10] Therefore, reflexive control requires the study of another's filter and the exploitation of it for one's own ends. The Soviet and Russian armed forces have studied the use of reflexive control for nearly 40 years. Over these years, many intellectual "giants" have emerged in the field of reflexive control theory in the military, academic, and civilian sectors of society. They've done so particularly at the tactical and operational levels, both for deception and disinformation purposes and to control the enemy's decision-making processes.[11] It is important to note that the target for

reflexive control activity is not limited to key decision makers but can include broader sections of the population as well, including mass and individual cognitive domains.

There is a distinct continuity of Soviet active measures and reflexive control into the present day practices of the Russian Federation. However, the advent and rapid progress of technology has enabled the Russians to be far more successful in their disinformation campaigns than the Soviets ever were. The Russian distinction between "cyber" and "information warfare" is an artificial one. Instead of cyberspace, Russia refers to it as the "information space," which includes both computer and human information processing.[12] Today, information in the media, on TV, on the computer, or in someone's mind is all subject to the same targeting procedures.

Russia has implemented a high-level, modernized propaganda effort with four main developments:

1. unprecedented budgets for its propaganda efforts,
2. modernized propaganda machinery employed by all modern media to support the Kremlin's message,
3. sophisticated technical expertise of the Kremlin's information warfare that allowed access to a greater variety of foreign audiences, and
4. utilization by the Kremlin of the relative openness of Western media for the Russian propaganda offensive.[13]

Recognition that Russia cannot compete directly in conventional terms has led to persistent emphasis in public statements and in annual budgets on finding asymmetric responses.[14] Information warfare does this in two important ways. First, Russia recognizes that information operations offers an opportunity to achieve a level of dominance. Second, it provides a significantly less costly method of conducting operations since it replaces the need for conventional military forces. According to Putin, "We must take into account the plans and directions of development of the armed forces of other countries. . . . Our responses must be based on intellectual superiority; they will be asymmetric, and less expensive."[15] Russia makes these concepts effective by using a multitude of information warfare tools.

Russia's Information Warfare Tools

A common development of state actors with fewer defense resources has led to the development of tools that are low cost and high impact (LCHI). Since Russia does not have the military or economic strength to directly counter the United States, it relies on nonconfrontational and asymmetric methods of power to ward off US normative influence. Some of the tools Russia relies upon to fulfill its asymmetric information warfare campaign include state-funded global social media, control of Western media outlets, and direct lobbying of Western society.

Exploiting Global Social Media

Cyber platforms have given the Kremlin capabilities to accomplish political foreign policy goals it would not otherwise be capable of. Whether the Kremlin wishes to inject propaganda, coerce, or gather data from individuals, these cyber capabilities hold the potential to influence multiple strata of society and are cost effective, difficult to attribute, and accessible from any location.

Current use of information warfare operations by the Russian Federation simply represents a modern, internet-age version of already well-established Soviet reality-reinventing tactics. In the information age, Russian analysts have recognized that information technologies can be used in coming conflicts where there will be no clearly drawn battle lines and the fighting will take place in several dimensions and arenas. There is a new "race" moving into the sphere of technology, including disinformation and propaganda.[16] Russia has therefore developed multiple capabilities for information warfare, such as computer network operations, electronic warfare, psychological operations, deception activities, and the weaponization of social media, to enhance its influence campaigns.[17]

Of particular importance is the injection of propaganda through social media as the nexus of information operations and cyberwarfare, whether it be through Twitter, Facebook, or YouTube. There are countless examples of this, including the recycling and spreading of a YouTube video of Russian soldiers with the title "Punitive Ukrainian National Guard Mission throwing dead bodies near Kramatorsk (Donetsk region) on 3 May 2014."[18] Another example involves the Twitter accounts of Russian embassies, who have taken an active role in using propaganda and unusual content in their tweets—something the typical foreign embassy account would not engage in. An example of this behavior is when the Russian

Embassy based in London tweeted "pundits call on @Theresa_May to disrupt possible Russia-US thaw. No trust in Britain's best friend and ally?" during Prime Minister Theresa May's first state visit to the United States during the Trump presidency. The obvious goal here was to convince sympathetic Americans that Theresa May should not intervene in Russia-US relations, seemingly with a condescending tone to undermine US relations with its greatest ally, Great Britain.

A more technical approach to social media propaganda allows for Russian troll campaigns and bots, otherwise known as the Kremlin Troll Army, to sow discord, spread fear, influence beliefs and behaviors, discredit institutions, diminish trust in the government, and ultimately destroy the possibility of using the internet as a democratic space. According to Lt Col Jarred Prier, this "hinges on four factors:

1. a message that fits an existing, even if obscure, narrative;
2. a group of true believers predisposed to the message (when presented with information within one's belief structure, bias is confirmed and propaganda is accepted easily);
3. a relatively small team of agents or cyber warriors; and
4. a network of automated 'bot' accounts." These factors allow a proactive approach to spreading a narrative at an extremely fast rate, what Prier has defined as "commanding the trend."[19]

This leaves mainstream media outlets unsure as to whether or not the comments pages are filled with real accounts or trolls with an agenda. To put this into perspective, "each troll is expected to post 50 news articles daily and maintain six Facebook and 10 Twitter accounts, with 50 tweets per day." In 2014, Twitter estimated that only 5 percent of accounts were bots; that number has grown along with the total users and now tops 15 percent.[20] For example, "Following the first presidential debate, the #TrumpWon hashtag quickly became the number one trend globally. Using the TrendMap application, one quickly noticed that the worldwide hashtag seemed to originate in Saint Petersburg, Russia."[21]

As future conflicts come into existence in the technological and cyber domain, "He who controls the trend will control the narrative- and ultimately, the narrative controls the will of the people."[22] This form of information warfare capability is often oversimplified and underestimated and therefore leads the target audience to exploitation through already

existing vulnerabilities. The Russian *Bulletin of the Academy of Military Sciences* states: "The victim country does not even suspect that it is being subjected to information-psychological influence. This leads in turn to a paradox: the aggressor achieves his military and political aims with the active support of the population of the country that is being subjected to influence,"[23] fulfilling the objectives of reflexive control theory.

Controlling Western Media Outlets

The Kremlin's peculiar definition of "soft power" has more to do with official state propaganda and less with the accustomed standard of results of attractive policies. While remembering the history of Russian information warfare, it is important to note that Soviet propaganda had almost no access to the Western mass media as it does today. After the collapse of the Soviet Union, Russia gained access to Western markets, paving the way for buying space in the West. By 2011, Russia had spent $1.4 billion on international propaganda,[24] a massive increase from the old Soviet era. The openness of the Western media has found itself hostage to this new tactic. The Kremlin has effectively been able to adapt its message with great freedom and flexibility to selective audiences worldwide.[25] In reality, the Kremlin has twisted one of the most fundamental and cherished values of liberal democratic societies, free speech and free press, into validation for its behavior, exploiting a very real vulnerability. Furthermore, Russia has in numerous ways weaponized this new form of soft power.

A version of this broad strategy can be found in the Russian primary military source *Information-Psychological Warfare in Modern Conditions* and includes:

- Direct lies for the purpose of disinformation both of the domestic population and foreign societies;
- Concealing critically important information;
- Burying valuable information in a mass of information dross;
- Simplification, confirmation, and repetition (inculcation);
- Terminological substitution: use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events;

- Introducing taboos on specific forms of information or categories of news;
- Image recognition: known politicians or celebrities can take part in political actions to order, thus exerting influence on the worldview of their followers;
- Providing negative information, which is more readily accepted by the audience than positive[26]

The real-world repercussions of these objectives are identified through several forms of attack. The first is through disseminating official Russian state propaganda abroad via foreign language news channels as well as Western media. Most notable is the creation of the very successful government-financed international TV news channel, Russia Today (RT). The content began as aiming to improve Russia's image abroad by stressing the nation's positives such as "its unique culture, its ethnic diversity, its role in World War II, and so on."[27] It was not until 2009 that the channel shifted from a defensive soft power tool to an offensive one. To do so, it began to extensively cover the negative aspects of the West, zeroing in on the United States. Examples of topics included mass unemployment, social inequality, and the banking crisis; furthermore, it became a platform for American conspiracy theorists explicitly questioning the September 11 attacks, the terrorist attack on the Boston Marathon, and Barack Obama's birth location. An *Economist* article titled "Russia Today Goes Mad" defines the channel's programs as "weirdly constructed propaganda" characterized by "a penchant for wild conspiracy theories."[28] Russia Today is not the only state-sponsored television channel; its other media outlets have waded into overt attempts at political disruption in foreign governments as well.

The Lisa Affair is a recent example of how Russian State TV perpetuates confusion and disinformation. In the summer of 2016, a 13-year-old Russian immigrant in Eastern Germany claimed to have been raped by a group of "immigrants."[29] Channel One, an English-language TV station funded and directed by the Russian government, picked up the story before local authorities had time to verify the allegations. Only days later, after police questioning, the girl admitted that the story had been a fabrication. Russian State TV and on their social media sites then accused German police of covering up the assault. Ethnic Russians immediately took to the streets demanding "justice." Far-right political

groups also capitalized on the incident for their anti-immigration rhetoric. The most baffling part was Russian Foreign Minister Sergey Lavrov appearing in a press conference also doubting the veracity of German authorities, implying a cover-up was under way. The coordination from the state television services in Germany to the Foreign Ministry of Russia, launched a process to instigate political instability.

The second form of attack is takeover of Western newspapers. One method used is buying space in its publications to manipulate Western readers. Once a month, an eight-page Russian supplement, "Russia Beyond the Headlines," is added to a list of established and influential Western newspapers including the *Washington Post*, the *New York Times*, the *Daily Telegraph* (United Kingdom), *Le Figaro* (France), *Repubblica* (Italy), *El Pais* (Spain), and the *Suddeutsche Zeitung* (Germany), with arrangements in more countries currently being made. The two main maneuvers employed to beguile readers consist of, first, mitigating cognitive dissonance by "adapting the contents and the style of the articles to fit their 'critical' Western mind."[30] These "critical" articles "would never stand a chance of being published in their mother paper, *Rossiyskaya Gazeta*; their only function is to give the Kremlin a 'liberal' image."[31] The second maneuver is applying the two-step flow of communication theory, which implies that information provided to the public through mass media is not directly inherited but rather channeled indirectly through opinion leaders.[32] To do this, a handful of newspapers have been purchased in foreign countries, in an attempt to create popular, far right, Kremlin-friendly publications. It is important to note the lack of economic incentive in buying these unprofitable papers and highlight the strategic reasons behind them. A notable example of this was the acquisition of the dying French newspaper *France-Soir* by the son of Russian oligarch Alexander Pugachev in 2009. Although it ultimately failed by 2012, it had succeeded in changing the image of the far-right nationalist, anti-EU, anti-NATO, and pro-Putin party of Marine Le Pen: The National Front. An even more chilling example is Russian oligarch and former KGB lieutenant colonel Alexander Lebedev (who had worked undercover at the Soviet embassy in Britain), who bought two loss-making British newspapers in 2009 and 2010. It was "an astonishing moment in British press history, the first time a former member of a foreign intelligence service has owned a British title."[33]

Lobbying Western Society

Incentivized to weaken democracy abroad and increase political influence, Russian businessmen, especially ex-Soviets, have long been attempting to generously finance campaigns of Western politicians and/or political parties. Areas of weakness in Western democracies have been identified to be taken advantage of, such as the "lack of strict regulations concerning party funding,"[34] along with overt and covert lobbying measures. These are both particularly high-risk in relation to corruption. A most notable example of this buying of elite political opinion is the influential group "Conservative Friends of Russia." This initiative was launched in August 2012 and has engaged with countless Tory party MPs and Tory peers of the UK government. They were even invited on a 10-day trip to Moscow and Saint Petersburg, where they attended a number of gala dinners and "in between, they had meetings with politicians of Putin's United Russia Party. Their trip was paid for by Rossotrudnichestvo, the Kremlin's new soft-power organization."[35] Another tactic can be seen with the usage of NGOs and civil society groups after realizing the central role they played during the "Orange Revolution." This tactic was developed to rival ideologies supported by existing NGOs with its own "counterrevolutionary" ideology through think tanks, roundtables, and conferences to export its own brand of political and economic influence.[36] Examples of umbrella organizations that covertly channel funds to Russia-friendly NGOs include the Institute of CIS Countries, as well as Russian World. A primary Russian source summarizes this idea clearly:

> It is preferable to have a foreign nonprofit nongovernmental organization (NGO) that could best contribute to the attainment of the goal of a hybrid operation. It can be established beyond the Russian Federation under the rules of a foreign country and can draw its members from residents of the disputed territory and its political objectives will include discrediting the current government agencies, eroding the prestige and public standing of the law enforcement agencies, particularly the armed forces, buying up mass media and conducting information operations purportedly to protect democracy, and nominating delegates for local government elections, and infiltrating them into the elected government authorities.[37]

The last tactic is the hiring of Western lobbying firms to improve the Kremlin's image abroad. While this strategy is not a new one in the world of politics, it has been something new for post-Soviet Russia. The

Kremlin's newfound wealth has given it the ability to reach out to the most prestigious lobbying and communication firms that "possess the necessary know-how . . . because they often employ former politicians, ambassadors, and other highly placed officials, who have direct personal access to government circles."[38]

Former Secretary of State Henry Kissinger is an example of a prominent lobbyist in good favor with the Kremlin, with a mutual admiration for Putin. He abstains from asking questions about democracy and human rights, making him an excellent asset to Putin's objectives. Kissinger's private lobbying firm, called Kissinger Associates, published a report in 2009 to influence the then-new President Obama's foreign policy goals, specifically with Russia. The following are excerpts from the report: "America's essential goal is not securing NATO's long-term future as the central element of our engagement with Europe, no matter how valuable an instrument of U.S. Policy in Europe NATO has been in the past. The United States should stop criticizing Russia on human rights and the lack of democratic standards. Issues of democratic development should be raised in a non-confrontational and non-accusatory manner" because Russia "is deeply sensitive about any appearances of interference in its domestic affairs."[39]

This report, on balance, perfectly exemplifies the way in which Kremlin-US public-private ties have given a platform for pro-Russian sentiment in the United States. The reader could easily believe the report was written by a Kremlin pundit or by Putin himself.

Another Western lobbyist hired by the Kremlin is New York-based firm Ketchum. Hired in 2006, they have consistently attempted to improve the Kremlin's image, even when it has been at historical lows, such as during the war with Georgia or the annexation of Crimea. Despite criticism from within, the firm persisted in helping make Russia more attractive to investors, which meant "helping them disguise all the issues that make it unattractive: human rights, invasions of neighboring countries, etc."[40] Ketchum also played a main role in the publication of Putin's highly political op-ed piece in the *New York Times* in September 2013.[41] One can also classify this move as a soft power play through western newspapers.

Long-Term Implications and Recommendations

Clausewitz's fog of war theory has been a useful term in a traditional sense for conveying the lack of situational awareness, and it has become a useful concept in information warfare as well. Russia has found an incredibly effective way to marry the ideas of disinformation, psychological warfare, reflexive control, and technology to create a very powerful fog of war that has disoriented the West. Their success in this endeavor has led to a climate of confusion, leading many to believe that problems are internal rather than external. This is because in some ways, they are. Russia merely has had to exploit an existing narrative—that is, the divisions in the West created by the fundamental principles of democratic societies: the freedom of individuals to attach themselves to a group they identify with and choose political leaders accordingly.

The implications of this are truly daunting. In the long term it serves to create distrust by the public in democratic institutions. It also elevates distrust in the press, in technology, in social media platforms and the businesses that are involved in creating them. This quite literally creates a modern fog of war. Scrambling to determine the truth as well as whom to blame, political disagreements transcend into extreme polarization and fuel tribalism that can tear a country apart.

In past conflicts, there has often been a "rally around the flag" effect where the nation comes together, despite differences, against a common enemy. However, an information war that uses disinformation as its weapon of choice destroys this unification by bringing the war directly into our homes and our minds.

Rethinking the Applicability of Deterrence

On 31 May 2018, the State Department released "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats." While the document recommends "a fundamental rethinking" of deterrence policy, the proposed strategies merely touch upon old ideas and fail to encompass a larger problem. The report continues to view information operations exclusively within the cyber domain, particularly because cyberspace has not yet been categorized as distinct and separate parts, as conventional warfare has been (that is, land, sea, air, and space). Due to the fact that modern times have forced us to move from a purely physical space into a virtual one, and because information warfare has been made so much

more effective within the virtual space, it seems that multiple types of information warfare are artificially being lumped together under the cyber domain. Instead of rethinking deterrence, we recommend rethinking the applicability of deterrence to cyber domain of warfare.

Introducing a Sixth Domain

Therefore, the evolution of military operations must include a sixth official domain of warfare, psychological, overlapping but distinctly separate from cyber. Vulnerabilities in cyberspace are concerned with malicious activity of a kind that needs to be separate from a psychological domain. For example, cyber focuses heavily on computer network defense and defense of critical infrastructure, among other malicious cyber activities within information security. On the other hand, psychological warfare focuses on the more human-related aspects of abstract information processing. It is critical that we differentiate this type of activity from particular tools of disinformation that Russia has used to wage war on the human psyche throughout the West.

The weaponization of information changes the application of deterrence, both within the cyber domain and in a psychological domain. There is currently plenty of scholarly research on the former. Although both of these dimensions can operate at a level beneath the use of force, there are disinformation operations that simply do not fall within the category of cyber, and we are left with nowhere to place them. In this article we have identified several tools Russia has used to enhance its information campaign in the West—social media, Western media outlets, and lobbying of civil society—all of which have the capacity to manipulate the human mind, but all of which do not necessarily benefit from virtual space exclusively.

We do not wish to undermine the valuable nature of cyberspace in spreading psychological disinformation campaigns. It has undoubtedly created a particularly ideal set of opportunities for Russia to accomplish its goal of destabilizing the West to increase its own power. While information warfare can operate independently from the cyber domain, it is important to note that it also benefits greatly from realities of virtual spaces to disperse its message. Social media platforms, for example, are a way for our adversaries to cost effectively and asymmetrically reach broad audiences of average people, tailoring active measures and reflexive control to achieve their objectives on a massive scale. This is, essentially,

how Russia classifies this domain. It does not distinguish between cyber and information warfare. The problem is that this ignores the reality of information operations as two-fold: both virtual and non-virtual. This means we are not creating a complete picture of the human dimension of information warfare, which only serves to limit the discussion on how deterrence theory can be modified to address all types of warfare.

Figure 2 illustrates the differences and similarities between the traditional perceptions of deterring conventional threats and achieving deterrence in cyberspace compared to our proposed psychological domain. While there are unchanging deterrence elements and concepts that allow deterrence to function in all domains, the applicability of these elements does not look the same across domains.

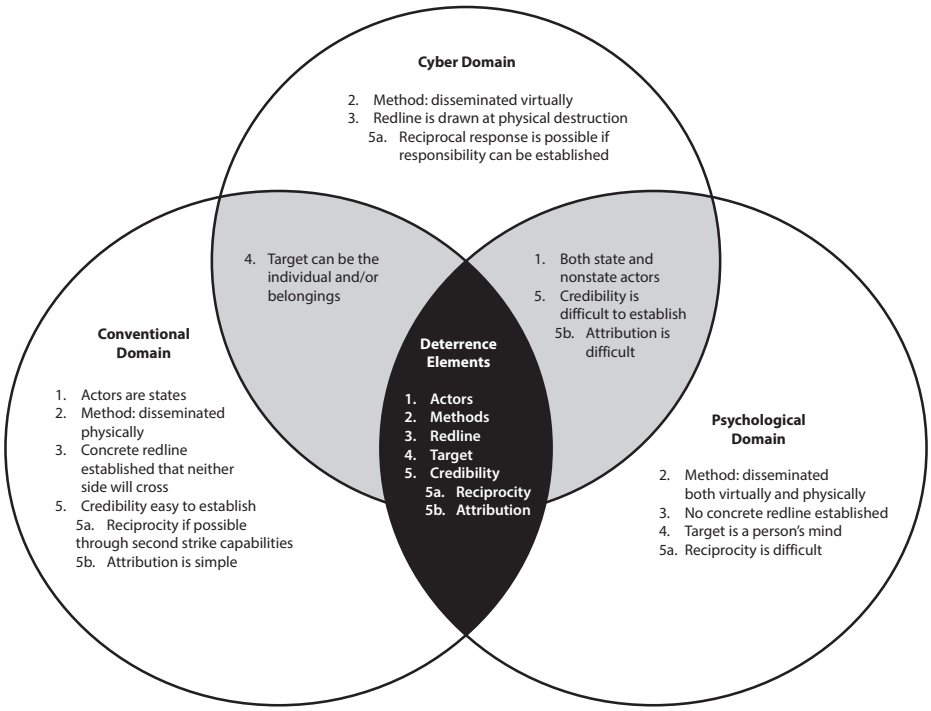

Figure 2. **A comparison of domain characteristics in relation to deterrence theory**. (Note: the numbers within the circles correlate with the numbers of the deterrence elements in the black center.)

Specifically, five areas of difference exist:

Actors. First, cyber has allowed nontraditional actors, such as individuals or transnational criminal organizations, to play an active

part in destabilization. As the world moves away from traditional, black-and-white norms concerning the sovereignty of states due to globalization, so too our ability to deter threatening actors has had to accept as reality the breakdown of the state as a concept. Therefore, while nuclear deterrence fits nicely into a traditional state-centric international relations framework, the more one moves into the cyber and psychological domain with the inclusion of nonstate actors, the less relevant the state becomes.

Methods. Warfare in the conventional domain consists of specific methods of attack, being those that cause physical destruction. Those in the cyber domain consist of virtual dissemination and destruction. Lastly, the psychological domain consists of multiple approaches, both physical and virtual. This illustrates the increasing complexity of the latter domains.

Redlines. Traditional deterrence strategy has been effective because a distinct redline generally exists that both sides are unwilling to cross based on the simple cost-benefit analysis of mutually assured destruction (MAD). The same cannot be said about the cyber and psychological domains, as Russia's actions have highlighted. While the nuclear redline is clear, the cyber redline becomes more obscure. Currently, the redline in cyber is drawn at any sort of physical harm, which is then considered to be an act of war. Anything short of this, however, is merely considered a nuisance. This line becomes even more obscure in the psychological domain because no physical line exists, despite the incredible amount of destruction and confusion it can cause.

Target. The object of conventional domain attacks can be the individual and/or possessions. In a strictly cyber domain, the target is normally a person's belongings (information, hardware, money). However, in the psychological domain the target is a person's mind.

Credibility. Credibility is a critical component of ensuring successful deterrence. To be deterred, an adversary must believe its actions will incur a cost. Credibility relies on two important factors: reciprocity and attribution.

Reciprocating an attack relies on quantifying or measuring the level of destruction incurred to determine proportionality. While this is relatively easy to do in the conventional domain, it is challenging but possible within the cyber domain dependent on establishing those responsible behind an

attack. It becomes even more difficult in the psychological domain due to the inability to measure effects and respond in kind.

Attribution becomes increasingly difficult as one moves outside of the physical world into a virtual and cognitive space. Attributing a physical attack is much simpler than attributing a virtual act to a state actor, and the involvement of nonstate actors in the cyber and information realms only seems to complicate this issue. This begs the question: can we deter an adversary we cannot identify? This problem degrades the ability to create credibility, along with the ability to follow up with requisite punishment.

In sum, given an increase in actors and methods, along with the blurring of redlines and sophistication of the targets, Clausewitz's fog of war is exponentially increased, which reflects the difficulty presented in reciprocity and attribution. The closed and carefully censored nature of Russia's society inhibits a proportional response by the West, since the media is primarily a tool of the Russian state. Conversely, the openness of democratic societies creates an opportunity for exploitation. Due to basic values in Western democracies for freedom of expression and their requisite legal foundations, limiting access to disinformation will be problematic and ultimately ineffective as a form of punishment. If we cannot fully reciprocate or attribute an attack correctly, we cannot threaten punishment, which leads to a decrease in overall credibility. And while the impact that can be had on a human's psyche is by no means new, it has only recently reached a level of magnitude that surpasses any other time in history.

However, this is not an argument against the establishment of a sixth domain. Instead, this strengthens the need for one. Given the difficulties that arise when information warfare is conducted on the human psyche, it is important to distinguish types of attacks as clearly as possible rather than lumping all of them under one category, as Russia has done. Russia is essentially viewing information itself as the weapon as well as a "space" (or domain) of warfare. In contrast, the US should see the cyber and psychological domains as being the space within which information is being used as the weapon of choice. Doing so will allow the US to create new and more specifically targeted deterrence policies, giving us an upper hand in future warfare. Information warfare should be classified under two separate domains of warfare: the cyber domain (virtual) and a psychological domain (cognitive).

Conclusion

While we have certainly moved beyond the days of a nuclear arms race with the Soviet Union and deterrence has subsequently evolved, our views of deterrence still rest upon nuclear and conventional forces to avoid escalation of conflict. Russia's recent emergence into the global dialogue among nations has been one of antagonism and active hostility, emphasizing its motives to be an established power on its own with a zero-sum mentality. This means reemergence as a world power while keeping the West out of its internal affairs of nationalistic authoritarianism. The means to this end include destabilizing their adversaries in the West, NATO, and the EU, using a variety of disinformation and cyber-enabled, low-cost, high-impact tools to facilitate operations. These capabilities are used to achieve different objectives in each target country with an asymmetric advantage. An underlying theme in Russia's success in this war is the rise of technology, allowing for the reinvention of old Soviet tactics. Propaganda, whether in the form of social media, traditional media outlets, or lobbying, is easily dispersed with the help of twenty-first-century machinery.

Today, conventional battlefield tactics remain a necessary component for deterring our adversaries, but we must now move away from traditional measures and transcend our thinking to reflect modern warfare. This includes accepting and understanding a new domain and how to navigate it to successfully deter Russian information warfare. We cannot, as a nation, create viable defense policies based on an old understanding of the application of deterrence theory. Furthermore, there has been no evidence to date to suggest that outside powers will not continue to exploit our vulnerabilities as a Western democratic nation. Therefore, we must take a proactive approach in confronting this new kind of weapon. Though Russia has been engaging in nonconfrontational methods of attack, it is time the US shifts from a pacifist stance to a more dynamic one in the psychological domain. SSQ

Notes

1. This research uses a thorough review of open-source literature of military and original source government documents. Secondary-source information from the Russian Federation and the United States was also used. It includes a qualitative analysis of developments in information warfare.

2. Russian Federation, "Decree of the President of the Russian Federation," The Ministry of Foreign Affairs of the Russian Federation, 5 December 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

3. Russian Federation, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*, Information Security Doctrine of the Russian Federation approved by the President of the Russian Federation on 9 September 2000, NATO Cooperative Cyber Defence Center of Excellence, 2000, http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

4. Kevin McCauley, *Russian Influence Campaigns Against the West: From the Cold War to Putin* (North Charleston, SC: Amazon Digital Services, 2016), Kindle edition, 121.

5. McCauley, 121.

6. Russian Federation, *Conceptual Views.*

7. McCauley, *Russian Influence*, Kindle edition, 109.

8. Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016), 19.

9. McCauley, *Russian Influence Campaigns*, 2015.

10. T. L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17 (2004): 237–56, https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

11. Thomas, "Russia's Reflexive Control."

12. Giles, *Handbook*, 8.

13. Marcel Van Herpen, *Putin's Propaganda Machine*: *Soft Power and Russian Foreign Policy* (Lanham, MD: Rowman & Littlefield, 2016), 202.

14. Giles, *Handbook*, 5.

15. Giles, 3.

16. Roland Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm: Swedish Defense Research Agency, 2010), 15, http://www.highseclabs.com/data/foir2970.pdf.

17. McCauley, *Russian Influence Campaigns*, 86.

18. Van Herpen, *Putin's Propaganda Machine*.

19. For more information on how to command the trend, see Lt Col Jarred Prier, "Commanding the Trend: Social Media as Information Warfare," *Strategic Studies Quarterly* 11, no. 4 (Winter 2017): 50–85, http://www.airuniversity.af.mil/SSQ/Display/Article/1349602/volume-11-issue-4-winter-2017/.

20. Alex Lubben, "Twitter's Users Are 15 Percent Robot, but That's Not Necessarily a Bad Thing," VICE News, 12 March 2017, https://news.vice.com/story/twitters-users-are-15-percent-robot-but-thats-not-necessarily-a-bad-thing.

21. Prier, "Commanding the Trend," 74.

22. Prier, 81.

23. Yu. Kuleshov et al., "ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ПРОТИВОБОРСТВО В СОВРЕМЕННЫХ УСЛОВИЯХ: ТЕОРИЯ И ПРАКТИКА" ("Information-Psychological Warfare in Modern Conditions: Theory and Practice"), *Vestnik Akademii Voyennykh Nauk* 46, no.1 (2014): 106.

24. Luke Harding, *Mafia State: How One Reporter Became an Enemy of the Brutal New Russia* (London: Guardian Books, 2011).

25. Van Herpen, *Putin's Propaganda Machine*, 1863.

26. Yu. Kuleshov et al., "ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ПРОТИВОБОРСТВО В СОВРЕМЕННЫХ УСЛОВИЯХ: ТЕОРИЯ И ПРАКТИКА" ("Information-Psychological Warfare in Modern Conditions"), 107.

27. Van Herpen, *Putin's Propaganda Machine*, 71.

28. "Airwaves Wobbly—Russia Today Goes Mad," *Eastern Approaches* (blog), *The Economist*, 6 July 2010, https://www.economist.com/eastern-approaches/2010/07/06/airwaves-wobbly.

29. "German Media Worries about Russian-Led Disinformation Campaign," Deutsche Welle, 19 February 2016, http://www.dw.com/en/german-media-worries-about-russian-led-disinformation-campaign/a-19061955.

30. This tactic illustrates what is known as "indirect strategy," in that propaganda at home and abroad may differ. Andre Beaufre, *Introduction a la Strategie* (Paris: Librairie Armand Colin, 1963).

31. Van Herpen, *Putin's Propaganda Machine*, 79.

32. Theory by sociologist Paul Lazarsfeld, which states that "the mass media does not find its way directly to the broader public but is rather channeled indirectly to it via opinion leaders." Quoted in Van Herpen, *Putin's Propaganda Machine*, 75.

33. Luke Harding, "Russian Oligarch Alexander Lebedev to Buy London Evening Standard," *The Guardian*, 14 January 2009, https://www.theguardian.com/media/2009/jan/14/russian-oligarch-alexander-lebedev-buy-london-evening-standard.

34. Van Herpen, *Putin's Propaganda Machine*, 100.

35. Van Herpen, 100.

36. Nicu Popescu and Andrew Wilson, *The Limits of Enlargement-Lite: European and Russian Power in the Troubled Neighbourhood*, Policy Report 14 (London: European Council on Foreign Relations, June 2009), 29.

37. I. N. Vorobyov and V. A. Kiselev, "Гибридные операции как новы вид военного противоборства" ("Hybrid operations as a new form of armed conflict"), *Voyennaya mysl'*, no. 5 (2015): 41–49.

38. Van Herpen, *Putin's Propaganda Machine*, 48; and Thomas Graham, *Resurgent Russia and U.S. Purposes: A Century Foundation Report* (New York: Century Foundation, 2009), http://russiaotherpointsofview.typepad.com/files/graham_resurgent_russia.pdf.

39. Graham, *Resurgent Russia*.

40. Ravi Somaiya, "P.R. Firm for Putin's Russia Now Walking a Fine Line," *New York Times*, 31 August 2014, https://www.nytimes.com/2014/09/01/business/media/pr-firm-for-putins-russia-now-walking-a-fine-line.html.

41. Vladimir Putin, "A Plea for Caution from Russia," *New York Times*, 11 September 2013, https://www.nytimes.com/2013/09/12/opinion/putin-plea-for-caution-from-russia-on-syria.html.

The Strategic Promise of Offensive Cyber Operations

Max Smeets

Abstract

Could offensive cyber operations provide strategic value? If so, how and under what conditions? While a growing number of states are said to be interested in developing offensive cyber capabilities, there is a sense that state leaders and policy makers still do not have a strong conception of its strategic advantages and limitations. This article finds that offensive cyber operations could provide significant strategic value to state-actors. The availability of offensive cyber capabilities expands the options available to state leaders across a wide range of situations. Distinguishing between counterforce cyber capabilities and countervalue cyber capabilities, the article shows that offensive cyber capabilities can both be an important force-multiplier for conventional capabilities as well as an independent asset. They can be used effectively with few casualties and achieve a form of psychological ascendancy. Yet, the promise of offensive cyber capabilities' strategic value comes with a set of conditions. These conditions are by no means always easy to fulfill—and at times lead to difficult strategic trade-offs.

❋ ❋ ❋ ❋ ❋

At a recent cybersecurity event at Georgetown Law School, Richard Ledgett, former deputy director of the National Security Agency (NSA), told an audience "well over 100" countries around the world are now capable of launching cyber-attacks.[1] Other senior policy makers and experts have made similar statements about the proliferation of offensive cyber capabilities.[2] Yet, offensive cyber operations are not considered to be an "absolute weapon," nor is their value "obviously beneficial."[3] There is also a sense that state leaders and policy makers, despite calling for

Max Smeets is a postdoctoral cybersecurity fellow at Stanford University Center for International Security and Cooperation (CISAC). He is also a nonresident cybersecurity policy fellow at New America and research associate at the Centre for Technology & Global Affairs, University of Oxford.

the need to acquire offensive cyber capabilities, do not have a clear conception of their strategic advantages.[4] Henry Kissinger in *World Order* writes that "internet technology has outstripped strategy or doctrine—at least for the time being. In the new era, capabilities exist for which there is as yet no common interpretation—or even understanding. Few if any limits exist among those wielding them to define either explicit or tacit restraints."[5] Former CIA and NSA director Michael Hayden notes in his book that "[f]rom their inception, cyber weapons have been viewed as 'special weapons,' not unlike nuclear devices of an earlier time. But these weapons are not well understood by the kind of people who get to sit in on meetings in the West Wing, and as of yet there has not been a Herman Kahn [of *On Thermonuclear War* fame] to explain it to them."[6] Similarly, former commander of the US Strategic Command James Ellis notes that the current strategic thinking on cyber conflict is "like the Rio Grande [River], a mile wide and an inch deep."[7]

This article offers more strategic scrutiny of offensive cyber operations. It does not aim to provide a descriptive or explanatory exercise, trying to understand why military cyber operations have been conducted in the past. Instead, it proposes the conditions under which these activities could effectively be conducted. After all, offensive cyber operations can only be successfully conducted in practice, once we have carefully considered the theoretical parameters of effectiveness.

The focus of this article is on a state actor in the international system that has established a well-resourced military cyber command (or equivalent) able to conduct a range of offensive cyber operations. Assuming a state is well resourced, this assessment underemphasizes the obstacles actors have to overcome to develop or acquire these capabilities.[8] It also excludes defender characteristics from this analysis and only assesses the value of these capabilities from the perspective of the state actor using these capabilities.[9] In addition, even though there is said to be an ongoing proliferation of capabilities to nonstate actors—worthy of analysis on their own terms—the state remains the principal legitimate actor to use these capabilities. Finally, an offensive cyber capability could potentially have strategic value short of actual use. Indeed, the coercion literature makes clear that a credible threat of military action could affect the behavior of other actors.[10] Even though these mechanisms could potentially be important, they are not part of the argument.

Unlike what some scholars and policy makers have suggested, offensive cyber operations could provide significant strategic value to state actors. The availability of offensive cyber capabilities expands the options available to state leaders across a wide range of situations. Offensive cyber capabilities can be both an important force-multiplier for conventional capabilities as well as an independent asset. They can be used effectively with few casualties and achieve a form of psychological ascendancy. However, the strategic value of different offensive cyber capabilities comes with a set of conditions. These conditions are by no means always easy to fulfill—and at times lead to difficult strategic trade-offs.

The article first addresses the strategic value offensive cyber operations. Then it clarifies the nature of offensive cyber operations, distinguishing between counterforce cyber capabilities (CFCC) and countervalue cyber capabilities (CVCC). Finally, it creates four propositions on the use of offensive cyber capabilities and specifies the conditions in which they could provide strategic value.

The Strategic Value of Offensive Cyber Operations

There is no single method to measure the strategic value of offensive cyber operations. Strategic value can mean at least two different things. First, it can refer to whether an offensive cyber operation can provide value in support of a national strategy.[11] The assessment of value then is highly dependent on defining what the strategy is. Following this perspective, one could, for example, analyze how offensive cyber operations contribute to the pursuit of deterrence—the most frequently referred-to strategy. Yet, it remains unclear to what degree deterrence (or any other strategy for that matter) is in fact the correct strategy to pursue.[12] Hence, if we use cyber deterrence as a measure, one may come to the conclusion that offensive cyber operations do have strategic value or they do not.[13]

Second, the term "strategic value" could also refer to cyber's ability to produce an outcome of conflict itself or, even more broadly, to state competition. Here, we use a different set of measures for "value": how the conduct of offensive cyber operations helps to avoid and/or affect the strategic outcome of a conflict.[14]

According to international relations scholar Erik Gartzke, "'cyber war' is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence."[15] Although offensive cyber capabilities should

not be conceived as the most authoritative asset, an analysis of their strategic value is nevertheless valuable. If one uses "final arbitration" as a criterion for analysis, almost no capability would pass the test. Hence, the approach here is more closely aligned with Colin Gray's review of military assets' strategic utility.[16] In the final part of his book *Explorations of Strategy* Gray writes the following about special operations: "[I] will avoid the trap of immoderate and unrealistic tests of strategic value. More specifically, the test of independent decisive effect on the course of a war is a criterion that special operations would fail in most instances. Since navies, armies, and air forces also fail the 'test' of independent decisive effect, one should not hold the special operations community to a higher standard."[17]

Similarly, an offensive cyber operation should not be considered by itself but with reference to both its direct and indirect effect upon conflict. This reveals an intricate relationship between mission excellence and strategic success. A well-written piece of code might provide great tactical value but does not guarantee strategic value, while failed usage of a cyber capability might provide strategic gains. An example of this seemingly counterintuitive logic might be Shamoon, the wiper malware that targeted the world's largest oil company, Saudi Aramco, in August of 2012.[18] The malware contained multiple coding errors and was badly executed.[19] Yet, with reference to Iran's broader conflict situation and posture in the region, it might have had a positive contribution. Not least, Iran showed it was unwilling to immediately back down following others' usage of a capability it had hardly developed at the time. The deployment showed Iran's military perseverance and perhaps even enhanced its political standing relative to other states.

The Nature of Offensive Cyber Operations

Offensive cyber operations in this article refer to computer activities to disrupt, deny, degrade, and/or destroy.[20] Offensive cyber operations generally take place across multiple stages. We commonly distinguish between reconnaissance, intrusion, privilege escalation, and payload dropping.[21] When thinking about the strategic value of offensive cyber operations, a useful distinction to consider is that of "counterforce" and "countervalue" targeting. The terms have been long used in nuclear planning as the two main courses of military action.[22] Counterforce is when an actor decides to strike at the opponent's military forces or infra-

structure. This is differentiated from countervalue strikes, which target the sources of an opponent's national strength.[23] In this context, counterforce cyber capabilities concern an offensive cyber capability designed to be used against targets relevant to the military operation. Countervalue cyber capabilities refer to an offensive cyber capability designed to be used against vital assets of the adversary. These two categories are presented as Weberian "ideal-types," meaning that in reality the distinction might become blurred.[24]

Table 1 lays out the dimensions of the two capabilities, revealing in which areas they likely overlap and differ. First, the conventional notion of "range" is not part of the definition and not a characteristic of either type of capability. Normally, range refers to the distance that a projectile may be sent by a weapon. Range is thus inherently connected to geography, a principle which has little meaning in cyberspace.[25] "Places have become geographically disembedded, that is, they are less and less determined and defined by physical-geographical features," as Philip Brey writes.[26] A capability may be counterforce even though it is used against an adversary geographically distant (but on the battlefield). And, conversely, one may attack a country nearby with a countervalue capability. There is also no inherent feature in the vulnerability, access, or payload of an offensive cyber capability that makes it either a countervalue or counterforce asset. Both capabilities can exploit software, hardware, or network vulnerabilities and can access air-gapped or non-airgapped systems. Indeed, despite some of the uncertainty about the exact vulnerability exploited in the case of Operation Orchard, it can be classified as a CFCC.[27]

The discussion on payload is associated in nuclear terminology as "yield." Also, yield is not and cannot be considered a defining feature of classifying offensive cyber capabilities. Yield is conventionally calculated using precise, physical standards. For example, it was alleged that the early Soviet intercontinental ballistic missile could carry a three megaton warhead (RDS-37) or a five megaton warhead (RDS-46).[28] A similar classification for cyber capabilities' payload is not possible; there is no convention for calculating "maliciousness" in a code as it is target dependent.[29] Having said that, for strategic purposes, as becomes clear below, it is more likely that a CFCC intends to cause less direct harm or damage than a CVCC. CVCC's principal target is the critical infrastructure of state actors. Targets may be facilities for water supply, telecommunication, electricity generation, or public health. CFCC targets military and

operational infrastructure of state and possibly nonstate actors.[30] Most nonstate actors are less dependent on territorial assets, making it more difficult to effectively use these capabilities.

Understanding the costs of these capabilities is not straightforward. Individually, a CFCC may be cheaper than a CVCC. The obstacles actors have to overcome to conduct a cyberattack against an industrial control system of a critical infrastructure are significant.[31] Yet, overall, CFCC may actually be more expensive to maintain and use, especially when these capabilities are used in response to the actions of other actors. To clarify this dynamic, imagine a situation in which there are multiple domains of potential conflict. To ensure a state actor can use counterforce capability when an adversary mobilizes its military capability in one of those domains, it must develop a capability for each domain—or at least several domains.[32] Yet, a state can use the same CVCC regardless of where the adversary will attack. The additional costs of relying on CFCC then comes from two sources: an actor needs to increase its arsenal size to impose costs on an adversary (if used reactionary), and a more constant effort to maintain the effectiveness of these capabilities is required given the transitory nature of offensive cyber capabilities.[33] This notion echoes John Lewis Gaddis's conclusion on strategies of containment.[34] A more limited form of containment, heavily relying on nuclear weapons, is cheaper but also less flexible. The more extensive form of containment—following the notion that the US would defend any territory regardless of means and area—provides more flexibility, but it also strains budgets. The aggressor chooses the location, and the receiver reacts accordingly.

Table 1. Countervalue and counterforce dimensions of offensive cyber capabilities

Dimension	CVCC	CFCC
Target	Vital asset adversary	Operationally relevant asset
Type of target	Often civilian	Often military
Range	Irrelevant	Irrelevant
Vulnerability	Undetermined	Undetermined
Access	Undetermined	Undetermined
Type of payload	Undetermined	Undetermined
Nature of adversary	Normally a state actor	Both state and nonstate actors
Costs	Individually, likely more expensive Collectively, cheaper	Individually, likely cheaper Collectively, more expensive

Numerous examples exist of counterforce targeting by state actors using offensive cyber capabilities.[35] In July and August 2008, Russia launched a DDOS-attack against Georgia's network, coinciding with troops entering the Georgian province of South Ossetia.[36] The attack, conducted in two phases, initially focused on Georgian news and government websites and later embraced a broad set of targets including educational institutions, financial institutions, businesses, and Western media.[37] The attacks complicated Georgia's efforts to manage its logistics, command forces, and deliver its war materials on time.

Another example of a CFCC is the Israeli use of the Suter Program developed by BAE systems.[38] The Israeli Air force allegedly used the technology to conduct an airstrike against a nuclear reactor in Northern Syria.[39] On 6 September 2007, F-15Is and F-16Is fighters flew into Syrian airspace, bombing the precise location of the nuclear plant in the Deir ez-Zor region of the country. Syria's air defense systems were fed a false-sky picture that allowed the Israeli fighters to conduct the entire process completely unnoticed.[40]

What are cases of CVCCs? Stuxnet can be categorized as a CVCC. Another example is the attack on the Ukraine power grid. On 23 December 2015, hackers took down almost 60 electrical substations in Ukraine, leaving more than 230,000 people without electricity for several hours.[41] As Kim Zetter writes, "They were skilled and stealthy strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, then launching a synchronized assault in a well-choreographed dance."[42] Overall, there are fewer examples of countervalue cyber capabilities known today used far from national borders and fielded military forces. Herein also lies an important observation: there is still much strategic room for states to explore.

Strategic Value of Counterforce and Countervalue Cyber Capabilities

Having laid out the dimensions of CVCC and CFCC, we can now look at the distinct advantages and disadvantages of these capabilities. Four propositions emerge. The first is considered to be the "master" proposition, as the other observations follow from it.

Proposition 1: Offensive Cyber Capabilities Provide an Extra Option for State Leaders

Gray, in his review on the strategic value of special operation forces, writes:

> Special operations can expand the options available to political and military leaders. . . . In theory, there are always alternatives to the use of force—diplomacy, economic sanctions, and the like. In practice, however, there are some situations that one cannot resolve successfully without resort to physical coercion. The availability of a special operations capability means that a country can use force flexibly, minimally, and precisely. The realization by the enemy that one has a special operations capability can have beneficial effects on calculations made abroad. In time of war, both in its independent and supporting roles, special operations enhance the flexibility with which one can use force.[43]

The value of offensive cyber capabilities is very similar; having the choice to use a cyber capability expands the options available to leaders. David Sanger writes in *Confront and Conceal* that "the origins of the [US] cyberwar against Iran goes [*sic*] back to 2006, midway through George W. Bush's second term. Bush had often complained to his secretary of state, Condoleezza Rice, and his national security adviser, Stephen Hadley, that his options regarding Iran looked binary: let them get the bomb or go to war to stop it. 'I need a third option,' Bush told them repeatedly. When that option emerged, it came from inside the bowels of the US Strategic Command, which oversees the military's nuclear arsenal."[44] The product was Olympic Games. Sanger writes that the motivation behind this operation was twofold: "[t]he first was to cripple, at least for a while, Iran's nuclear progress. The second, equally vital, was to convince the Israelis that there was a smarter, more elegant way to deal with the Iranian nuclear problem than launching an airstrike that could quickly escalate into another Middle East war, one that would send oil prices soaring and could involve all the volatile players in the region."[45]

In simple terms, it is said that offensive cyber operations allow for action within the "gray zone" of foreign activities, neither war nor peace. As scholar Herb Lin argues, "Nuclear comes AFTER conventional conflict has commenced. . . . Escalation concerns involve moving from conventional conflict to nuclear conflict. Going nuclear is escalatory. . . . [Instead,] cyber comes in the early stages of conflict (BEFORE kinetic war). In principle, cyber [is] just another weapon to be used by . . . military forces. . . . Going cyber is pre-escalatory."[46] Even though offensive cyber

operations provide an extra option, they are not the "prewar capabilities" that simply add another rung to the ladder of escalation. Offensive cyber capabilities can be used in times of both peace and war, in conflicts with different intensity, with and without kinetic force and can influence the activities of all other domains of warfare and lead to escalation or de-escalation. The exact nature and utility of usage, however, inherently differs for countervalue and counterforce capabilities, as will become clear.[47]

Proposition 2: Offensive Cyber Capabilities Can Be Used Effectively in Conjunction with Other Military Capabilities

Several scholars note that "unlike weapons of mass destruction, cyber weapons are an integral part of the commander's arsenal in conducting force-on-force and asymmetric warfare and will be used in concert with kinetic weapons to soften up the adversary's defenses."[48] Indeed, there is little question that CFCCs can be deployed in conjunction with other military capabilities—in fact, that is what makes them attractive to use. Like small amounts of investments can create much larger changes in total output of an economy through a multiplier effect, so can the use of a relatively simple CFCC greatly alter the outcome of a conflict.[49] Yet, the effectiveness of CFCCs in this manner is dependent on one key condition: force integration.

The required nature of force integration depends on the form of interdependence between the offensive cyber operations and conventional military operations.[50] First, there can be, what I call "pooled interdependence," when CFCCs and conventional capabilities perform separate functions. While the activities may not directly depend on each other, each provides individual contributions to the same goal. This is very much in line with the activities of Russia against Georgia in 2008 and more recently against Ukraine.[51] The use of multiple attack vectors caused a "mashup" of indirect dependencies leading to success of the overall engagement.

Second, there can be "sequential interdependence" when the use of a CFCC in the overall military process produces an outcome necessary for the success of subsequent conventional capability. Operation Orchard is an excellent example of how CFCCs can dramatically increase the effectiveness of other military capabilities in this manner. The F-15s and F-16s used by the Israeli air force against Syria in 2007 were not equipped with stealth technology. But tripping off Syria's air defense

radar system nevertheless ensured the Israeli air force could accomplish the missions while remaining undetected. Note that the multiplier effect may be larger for situations of sequential interdependence, yet the risks are also higher. Failed use of a CFCC may have disastrous consequences for the follow-on operation, leading to a failure of the overall process.[52]

Even though CVCCs typically are not integrated with kinetic forces on the battlefield, there are still incentives to use these capabilities in conjunction with other forces in certain conflict situations. Consider a scenario in which actor A attacks our imagined state actor (actor B) through either conventional or cyber means. The most obvious response of actor B (or ally of actor B) would be to raise the cost of the attacker (actor A) by deploying defense capabilities on the battlefield. But actor B can further raise the costs of the attack by means of using a CVCC against a vital asset of actor A. There are three conditions that could make this response particularly effective.

The first condition is perhaps the most obvious: actor B must be able to inflict enough harm or damage against actor A that it is perceived to be a substantive cost (which in turn can be leveraged). Offensive cyber capabilities that have the potential to cause high levels of harm or damage often go beyond effects created in cyberspace. One could, for instance, consider the sabotage of a water dam or power plant through a cyberattack, leading to the physical destruction of this infrastructure.

In discussions on the use of conventional capabilities for coercive purposes, the focus is generally on a geographical area. In the case of a nuclear bomb, we can calculate the different radii of serious and less serious contamination. What we cannot do is differentiate within that area. The usage of a CVCC does not come with these restrictions; its effects can be selectively dispersed across a large geographical space (e.g., all hospitals in a certain country running on a certain system). This opens up new ways of thinking when it comes to countervalue capabilities. Instead of taking down one vital asset of a country, there is also an opportunity to paralyze the country through attacking a large amount of geographically dispersed systems.

The second condition is that actor A must be able to discern with a high level of certainty that the retaliatory act through cyberspace comes from actor B. This condition might seem trivial, and it is for conventional capabilities, but for CVCCs there are two complications. First, actor A must be aware that the attack came from actor B. Plausible

deniability is normally said to be to an advantage to the attacker. Yet, in this case it is an additional hurdle for actor B, as the aim for actor B is to show that it is retaliating in response to actor A's actions. This discussion has led to early talk about the need to develop "loud" cyberweapons.[53] Second, actor A must be able to delineate actor B's cyber response from the more constant state of cyber activity. Cyberspace, given its interconnectedness, is said to be a space of constant contact, action, hostility, and change.[54] In February 2017, the director of UK's National Cyber Security Centre said that the country had experienced 188 "high-level cyber attacks" in the previous three months.[55] If allegedly a government is attacked multiple times a day by state-sponsored actors, how does it know this particular attack is part of a retaliatory strike?[56]

The third condition is that the actor designs the CVCC in such a manner that it is able to control the temporal nature of the harmful or damaging effects. Scholars often talk about the effect of offensive cyber operations only being able to be temporal.[57] But a truly intelligent design of a capability goes beyond this and aims to control the duration of effect. Control refers to the defender's inability to stop or reverse the effects of the cyberattack and the attacker's ability to stop or reverse the effects of the attack at any given time.

This type of capability design would allow for CVCC to be used somewhat similarly to economic sanctions. The simplest design for this type of capability would be large-scale DDOS attacks with multiple C2 servers and a large number of zombie computers (infected with different malware). Another type of design would be a variant of a wiper. The wiper would copy all the relevant data before it executes the disk-wiping command. The leverage is that the attacker could give the data back following conflict termination (in the scenario described above). Overall, if the usage of a CVCC is discernible and its effects controllable, it can be used as an independent asset—and even allow for the prevention of further conflict and the maintenance of stability in a certain region.[58]

In fact, countervalue cyber capabilities also have a distinct advantage compared to economic sanctions. Sanctions are inherently public, which leads to additional reputational costs for the aggressor if it backs down post-action. The value of CVCC is that these activities could potentially take place in a covert manner, making it easier for a leader to save face after it backed down. Overall, this leads to new possibilities of compellence, that is to change the behavior of actors.

Ultimately, combining the above three conditions leads to a dilemma for the use of a CVCC. After all, it is difficult to combine the first and last conditions. If an effect is created beyond cyberspace, it is hard to reverse this effect at a later time. And, the reverse is true as well: if the direct effects of an operation do remain within cyberspace, the effects may not be substantial enough to be leveraged against the opponent.

Proposition 3: Offensive Cyber Capabilities Can Be Used to Achieve a Form of Psychological Ascendancy

An extensive body of military research has been devoted to understanding the psychological impact of military operations. In particular, numerous scholars have sought to assess how the psychological effects of air operations during major conflicts—such as World War II, the Korean War, the Vietnam War, and the Persian Gulf wars—have helped to coerce and/or demoralize the adversary.[59] Also offensive cyber operations may have psychological effects. The nature of this effect, however, tends to differ from most conventional military operations: rather than frightening the adversary, the effects are subtler and relate to humiliation and confidence degradation. It is also less about threatening escalation and more about exposing vulnerability for offensive cyber operations.

An old example illustrates this particularly well. On an afternoon in June 1903, the Italian inventor and electrical engineer Guglielmo Marconi was about to demonstrate how Morse code messages could be wirelessly transmitted over long distances.[60] In the lecture theater of the Royal Academy of Sciences, Marconi's assistant John Ambrose Fleming was waiting to showcase the powerful point-to-point system technology in front of a large audience. Marconi himself was about 300 miles away, preparing to send a signal to London from a clifftop station in Cornwall, UK. Yet what followed was not in Marconi's playbook:

> Minutes before Fleming was due to receive Marconi's Morse messages from Cornwall, the hush was broken by a rhythmic ticking noise sputtering from the theatre's brass projection lantern, used to display the lecturer's slides. . . . Someone, [Fleming's assistant] Blok reasoned, was beaming powerful wireless pulses into the theatre and they were strong enough to interfere with the projector's electric arc discharge lamp. Mentally decoding the missive, Blok realized it was spelling one facetious word, over and over: "Rats." A glance at the output of the nearby Morse printer confirmed this. The incoming Morse then got more personal, mocking Marconi: "There was a young fellow of Italy, who

> diddled the public quite prettily," it trilled. Further rude epithets—opposite lines from Shakespeare—followed.[61]

A trick was played by Nevil Maskelyne, a British magician using Morse code for his illusions, enlisted by the Eastern Telegraph Company. Maskelyne's actions highlighted that Marconi's technology was nowhere near as secure as he claimed. After the incident, Marconi did not immediately respond publicly: "I will not demonstrate to any man who throws doubt upon the system." The *New Scientist* writes that, "Fleming, however, fired off a fuming letter to The Times of London. He dubbed the hack 'scientific hooliganism', and 'an outrage against the traditions of the Royal Institution'. He asked the newspaper's readers to help him find the culprit."[62]

The century-old hack aptly demonstrates a potent ability of offensive cyber operations today: the ability to humiliate an enemy. This is also demonstrated for more recent CVCC and CFCC usage. The goal of Stuxnet (a CVCC) was not to maximize damage but (in part) to embarrass the Iranians.[63] And the worm has done so successfully. Natanz was a hardened fuel enrichment plant (FEP), buried deep underground, seemingly impossible to strike. Some of the country's most renowned scientists and engineers were dismissed as incompetent, unable to explain what was going on with the industrial control systems in Natanz. The malware was only discovered after non-Iranian security researchers started to analyze the code, another sign that the Iranians were unable to protect their own most secretive and prestigious program.[64]

Operation Orchard (a CFCC) is one of the Israeli military's finest moments. For Syrian President Bashar al-Assad, it was a humiliating experience. After the attack the Syrian government initially claimed that its antiaircraft weapons had fired at Israeli fighters, which had bombed an empty area in the desert. Later, Assad insisted during an interview with *Der Spiegel* at his palace that "[t]he facility that was bombed was not a nuclear plant, but rather a conventional military installation."[65]

These types of cyberattacks remind us of the psychological effects of some of the special operations Colin Gray describes. For example, "during the war of attrition with Egypt in 1968–70, Israeli commandos attacked one of the 'crown jewels' of the Egyptian economy, the Naj Hamadi transformer station and bridge which were 320 kilometers inside Egypt. [It is an example of] a state being revealed as unable to

protect its assets."[66] Overall, both special operations and cyberattacks can "inflict exemplary punishment as well as actual loss."[67]

To achieve some form of psychological ascendancy could be both the main purpose and side effect of using an offensive cyber capability.[68] From the perspective of our imagined state actor assuming the defender and/or other third party does not disclose the intrusion, there are three options: attack and immediately disclose; attack and conceal, but disclose later; or attack and conceal. If an attacker postpones disclosure it can expose the intrusion at a time when the strategic context is more favorable (e.g. when target is particularly exposed to this news, during, for example election season, or when distraction away from internal problems is convenient). If an attacker never discloses, it can enhance credibility and make compellence easier in the future, as was stated above.

Proposition 4: Offensive Cyber Capabilities Can Be Used Effectively with Few Casualties

In 2015, when India's Prime Minster Narendra Modi launched "Digital India Week" he stated that "clouds of a bloodless war are hovering" in the world.[69] It was a reference to the global cyber threat that he believed India could play a lead role in countering.

The uses of CVCCs and CFCCs so far have indeed not been lethal, but the argument is not that it cannot happen. A civilian can be a direct and indirect target of a cyberattack. A potential example of a direct attack concerns the alteration of medical devices that could give a deadly shock if hacked. The doctor of former Vice President Dick Cheney ordered the wireless functionality of his heart implant to be disabled due to fears it might be hacked in an assassination attempt.[70] This has proven to be a valid fear following Barnaby Jack's demonstrated research on vulnerability in medical devices.[71] More indirect forms of harm can be caused by using an offensive cyber capability against transportation networks (causing airplane/train crashes) or dam facilities (causing pollution or flooding).

Instead, the notion of "bloodless war" rests on two pillars. The first pillar directly connects to the earlier debate on whether cyberwar makes for a more or less violent world. Tim Maurer concludes "cyberwarfare might be how we will fight the battles of the future. The evidence so far suggests, however, that a digital Pearl Harbor would cost fewer lives than the attack 70 years ago. It might not be pretty, but from a humanitarian

point of view, that's good news." Maurer notes that Stuxnet delayed Iran's nuclear development without killing anyone. Hence, his argument is that if actors use a Stuxnet-like capability more often, it would reduce the human costs of war.[72] Similar conceptions are provided by Thomas Rid and John Arquilla.[73]

The other pillar on which the bloodless war conception rests is that of the attacker's casualty sensitivity.[74] Though the literature is divided on whether mounting casualties by themselves drive public attitudes toward conflict and inherently lead to reduced public support, the scholarly consensus is that public attitudes toward war are not indifferent to the human costs of its soldiers.[75] The common conception is that the public makes some kind of "end-means" calculus about war.[76] A cyber warrior sits far away from the battleground—whether developing a tactical or strategic cyber capability. It is hard to conceive how these individuals can suffer bodily harm during an offensive cyber operation.[77]

Although the bloodless war perception provides a powerful push factor to use an offensive cyber capability, there is a major caveat with respect to this discussion. Offensive cyber operations can have the ability to limit casualties on both sides.[78] Yet imprudent use can severely increase the undesired impact of these capabilities. As Steve Bellovin, Susan Landau, and Herb Lin note, "indiscriminate targeting is not an inherent characteristic of all cyberattacks."[79] Historically, there has often been mismatch between the intent and the actual damage caused by cyberattacks. When graduate student Robert Morris released one of the first computer worms distributed via the internet in 1988, he never intended to create an overall system downtime leading computers to slow down to the point of being unusable. The worm's alleged purpose was to measure the size of the internet, but a critical bug in the spreading mechanism transformed it into a highly disruptive attack.

Bellovin, Landau, and Lin examine the requirements and policy implications of targeted cyberattacks.[80] Their main conclusion is that "precise targeting requires good technical design . . . [and] intelligence . . . of the target's environment."[81] The scholars indicate that precise intelligence on the configuration of target machines is especially important when cyberattacks focus on physical assets, considering the high risk of collateral damage.[82]

What should also be noted is that, as discussed for Proposition 2, the relationship between spatial area of damage and collateral damage is

more complex for CVCCs compared to the use of conventional capabilities. There does not have to be any correlation between the geographical distribution of effects and the distinctive or targeted nature of an offensive cyber operation. Overall, the belief held in many military quarters is that with sufficient testing and retesting prior to usage, offensive cyber operations can achieve a designed effect and minimize damage to entities that should remain unharmed.[83] But it does mean that the costs for developing an offensive cyber capability are substantially higher too.

Conclusion

This article examined the strategic value of offensive cyber operations, distinguishing between counterforce and countervalue cyber capabilities. While distinct advantages exist for using offensive cyber operations, it should be clear that there are many things offensive cyber operations cannot do. The cyber warrior is much more anonymous, and the way cyber operations unfold will not create the kind of heroics that raise public morale. At the same time, the effective use of offensive cyber capabilities comes with a number of conditions that can sometimes be difficult to meet and might even conflict. A better conceptualization of these conditions and potential trade-offs helps set the required technical parameters of future cyber capability development.

Ultimately, offensive cyber operations can lead to significant strategic advantages for a state actor. They can serve as a force multiplier as well as an independent strategic asset. Above all, the potential use of offensive cyber capabilities provides an extra option to state leaders across a range of situations. SSQ

Notes

1. Quoted in Mike Levine, "Russia Tops List of 100 Countries that Could Launch Cyberattacks on US," ABC News (18 May 2017), http://abcnews.go.com/US/russia-tops-list-100-countries-launch-cyberattacks-us/story?id=47487188.

2. Jamie Shea, "Lecture 6—Cyberattacks: Hype or an Increasing Headache for Open Societies?" (transcript, 29 February 2012), http://www.nato.int/cps/en/natolive/opinions_84768.htm; and INFOSEC, "The Rise of Cyber Weapons and Relative Impact on Cyberspace," Infosec Institute, (5 October 2012), http://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/.

3. Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401–28, https://

doi.org/10.1080/01402390.2012.663252; and Bernard Brodie, *The Absolute Weapon: Atomic Power and World Order* (New York: Brace and Company, 1946).

4. The post-2000 literature's primary focus has been on the disruptive or destructive effects of cyberattacks. The mainstream debate on the potential for cyberwar is notably illustrative. An often-cited quote from Thomas Rid's article "Cyber War Will Not Take Place" reads, "no cyber offense has ever injured a person. No cyber attack has ever damaged a building." The statement has been debated repetitively and at length, from both theoretical and empirical perspectives. John Stone writes in a theory-driven response to Rid's article that cyberattacks could constitute acts of war, but "it depends on the meaning and relationship of the terms 'force,' 'violence,' and 'lethality.' " From an empirical perspective, scholars have criticized Rid because many of the attacks cited were in fact much more violent. Perhaps not the direct effects but the indirect effects of the DDOS attacks on Estonia, one scholar argues, were consequential. Similarly, others have argued that Stuxnet was more than just an act of sabotage. *See* Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, http://doi.org/b4fkhh; John Stone, "Cyber War Will Take Place!," *Journal of Strategic Studies* 36, no. 1 (2013): 101–8, http://doi.org/cp6d. For direct discussions on this quote, see, for example, Gary McGraw, "Cyber War Is Inevitable (Unless We Build Security In)," *Journal of Strategic Studies* 36, no. 1 (2013): 109–19, http://doi.org/cp6f; Isabelle Duyvesteyn, "Between Doomsday and Dismissal: Cyber War, the Parameters of War, and Collective Defense," Atlantische Commissie (2012), accessed 23 May 2018, https://www.atlcom.nl/ap_archive/pdf/AP%202014%20nr.%207/Duyvesteyn.pdf; Shruti Tulpule, "Are We Headed towards Web War I?," *International Journal of Law and Legal Jurisprudence Studies* 1, no. 7 (2014), accessed 23 May 2018, http://ijlljs.in/wp-content/uploads/2014/11/Are-we-headed-towards-Web-War-I-Shruti-Tulpule.pdf; on Estonia and student, see "Stuxnet: Computer Worm Opens New Era of Warfare," *60 Minutes*, CBS News (4 March 2012), transcript, https://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/; Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 57–64, http://doi.org/bm7g9s.

5. Henry Kissinger, *World Order: Reflections on the Character of Nations and the Course of History* (London: Penguin Books Limited, 2014), 334.

6. Michael Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Random House, 2016).

7. Cited in Patrick Cirenza, "The Flawed Analogy between Nuclear and Cyber Deterrence," *Bulletin of the Atomic Scientists* (22 February 2016), http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179.

8. *See* Max Smeets, "What It Takes to Develop a Cyber Weapon: Nobody Knows," Council on Foreign Relations: Net Politics, 21 November 2016, https://www.cfr.org/blog/how-much-does-cyber-weapon-cost-nobody-knows; and Herbert Lin, "Oft-Neglected Cost Drivers of Cyber Weapons," Council on Foreign Relations: Net Politics, 14 December 2016, https://www.cfr.org/blog/oft-neglected-cost-drivers-cyber-weapons.

9. In reality, of course, the defender has a great deal of agency in terms of the outcome of a cyberattack.

10. Thus far, the literature is divided on whether the threat of using a cyber capability can coerce. Christopher Whyte, "Ending Cyber Coercion: Computer Network Attack, Exploitation and the Case of North Korea," *Comparative Strategy* 35, no. 2 (2016): 93–102, http://doi.org/cp6g; Travis Sharp, "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony," *Journal of Strategic Studies* 40, no. 7 (2017): 1–29, http://doi.org/cp6h; Erica D.

Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (May 2017): 452–81, http://doi.org/cp6j; Richard J. Harknett, "Article Review 84 on 'The Logic of Coercion in Cyberspace' and on 'Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony,' " International Security Studies Forum, 26 September 2017, https://issforum.org/articlereviews/84-cyber.

11. For an overview of strategies, see Robert J. Art, "To What Ends Military Power?," *International Security* 4, no. 4 (1980): 3–35, http://doi.org/cjgtvg.

12. Indeed, opinions range from "leave it—it's working," to "tweak it and it'll work," to "get rid of it and start thinking about other strategies." At the same time, the table also shows much overlap in viewpoints on cyber deterrence, which often goes unacknowledged.

13. There is also disagreement on the meaning of the term "cyber deterrence."

14. I adopt the definition used by Colin Gray with two alterations. Gray looks at "how a military directly contributes to the strategic outcome of a war." First, the effects can be direct as well as indirect. Second, strategy can relate to a broader context than "war." I therefore refer to "conflict" instead. Colin S. Gray, *Explorations in Strategy* (Westport, CT: Praeger Publishers, 1996).

15. Erik Gartkze, "The Myth of Cyberwar," *International Security* 38, no. 2 (Fall 2013): 42, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136.

16. I avoid using the term "strategic utility" as the modern use of the term is associated with economic cost-benefit analysis.

17. Gray, *Explorations in Strategy*, 166.

18. Lucian Constantin, "Kill Timer Found in Shamoon Malware Suggests Possible Connection to Saudi Aramco Attack," *Computerworld*, 23 August 2012, http://www.computerworld.com/article/2491501/malware-vulnerabilities/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-ar.html.

19. Dmitry Tarakanov, "Shamoon the Wiper: Further Details (Part II)," SecureList, 11 September 2012, https://securelist.com/shamoon-the-wiper-further-details-part-ii/57784/.

20. A common distinction is made between three types of computer network operations (CNO): computer network defense (CND), which is protecting your own networks from being attacked or exploited; computer network exploration (CNE), which refers to computer espionage; and computer network attack (CNA), which concerns cyber activities to disrupt, deny, degrade, and/or destroy. I focus on the latter type of activity, which I term offensive cyber operations. This also means that this research does not focus on information weapons or disinformation campaigns.

21. For more information, see Max Smeets, "Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks," *Proceedings of the 9th International Conference on Cyber Conflict, Defending the Core*, ed. H. Roigas, R. Jakchis, L. Lindstrom, T. Minarik (Tallinn, Estonia: NATO CCD COE Publications, 2017), http://doi.org/cp7w.

22. Dieter S. Lutz, "A Counterforce/Countervalue Scenario—or How Much Destructive Capability is Enough?," *Journal of Peace Research* 20, no. 1 (1983): 17–26, http://doi.org/ckgb7t.

23. William A. Stewart, "Counterforce, Damage-Limiting, and Deterrence," RAND Corporation, July 1967, accessed 24 May 2018, https://www.rand.org/content/dam/rand/pubs/papers/2008/P3385.pdf.

24. Austin Long has previously made a similar distinction. However, the scholar does not go into detail on the strategic advantages of each capability. *See* Long, "A Cyber SIOP? Operational Consideration for Strategic Offensive Cyber Planning," *Journal of Cybersecurity* 3, no. 1 (2017): 19–28, https://doi.org/10.1093/cybsec/tyw016.

25. This does not mean that geography and borders do not matter at all in cyberspace.

26. Philip Brey, "'Space-Shaping Technologies and the Geographical Disembedding of Place," in *Philosophy & Geography vol. III: Philosophies of Place*, ed. A. Light and J. M. Smith (New York: Rowman & Littlefield, 1998), 239.

27. *See* Adlee's discussion on the possibility of backdoors. Sally Adlee, "The Hunt for the Kill Switch," IEEE Spectrum, 1 May 2008, https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.

28. John Pike, Charles Vick, Mirko Jacubowski, and Patrick Garrett, "R-7/SS-6 SAPWOOD," Federation of American Scientists, 29 July 2000, https://fas.org/nuke/guide/russia/icbm/r-7.htm.

29. For similar points, see Michael Fischerkeller, "Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies," *Survival* 59, no. 1 (2017): 103–34, http://doi.org/cp7z.

30. Notice that in practice, operational infrastructure and critical infrastructure may overlap. For example, the distinction becomes blurred if one takes down the electricity grid that feeds a town and a military base.

31. More research should be conducted to better understand these costs dynamics. For an initial discussion see Max Smeets, "What It Takes to Develop a Cyber Weapon" (working paper, Columbia School of International and Public Affairs Tech & Policy Initiative, Working Paper Series 1, 2016), 49–67, https://sipa.columbia.edu/sites/default/files/WorkingPaperSeries_1.pdf.

32. This depends on the overlap in weaknesses to exploit.

33. Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, no. 1–2 (2018): 6–32, http://doi.org/cp75.

34. John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War* (Oxford, UK: Oxford University Press: 1982).

35. One may consider counterforce operations also in a broader sense, that is, those operations that did not cause any harm or damage. An interesting case of this kind concerns a variant of X-Agent malware for Android devices created by Fancy Bear to collect intelligence on Ukrainian field artillery units. A Ukrainian officer had developed an app to simplify artillery troops' targeting data for the D-30 towed howitzer. See Crowdstrike Global Intelligence Team, "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," Crowdstrike, 23 March 2017, https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

36. Asmus Ronald, *Little War that Changed the World: Georgia, Russia and the Future of the West* (New York: Palgrave Macmillan, 2010); and Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* 91, no. 6 (November–December 2011): 63–64, https://www.questia.com/library/journal/1G1-273195159/the-2008-russian-cyber-campaign-against-georgia.

37. Numerous patriotic hackers are said to have joined the campaign in the second phase.

38. A good overview of this capability is provided by Zheng. Ye Zheng, "From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond," trans. Yang Fan, in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford, UK: Oxford University Press, 2015).

39. David A. Fulghum, Robert Wall, and Amy Butler, "Cyber-Combat's First Shot," *Aviation Week & Space Technology*, 26 November 2007, 28–31, http://archive.aviationweek.com/issue/20071126; Richard A. Clarke and Robert K. Knake, *Cyber War* (New York: Harper Collins, 2010); and Zheng, "From Cyberwarfare to Cybersecurity."

40. Although most scholars and media sources have looked at the event in 2007, it can be said that first part of this operation started much earlier. As *Der Spiegel* reports:

> [i]n late 2006, Israeli military intelligence decided to ask the British for their opinion. But almost at the same time as the delegation from Tel Aviv was arriving in London, a senior Syrian government official checked into a hotel in the exclusive London neighborhood of Kensington. He was under Mossad surveillance and turned out to be incredibly careless, leaving his computer in his hotel room when he went out. Israeli agents took the opportunity to install a so-called "Trojan horse" program, which can be used to secretly steal data, onto the Syrian's laptop. The hard drive contained construction plans, letters and hundreds of photos. The photos, which were particularly revealing, showed the Al Kibar complex at various stages in its development. At the beginning—probably in 2002, although the material was undated—the construction site looked like a treehouse on stilts, complete with suspicious-looking pipes leading to a pumping station at the Euphrates.

See Erich Follath and Holger Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Der Spiegel*, 2 November 2009, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-2.html.

41. Initially, 30 substations were taken down. The attackers later targeted two other power distribution centers. For overviews, see Kim Zetter, "Everything We Know About Ukraine's Power Plant Hack," *Wired*, 20 January 2016, https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/; Kaspersky Lab, "BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents," SecureList, 28 January 2016, https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents /73440/; and Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, 3 March 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

42. Zetter, "Inside the Cunning, Unprecedented Hack."

43. Gray, *Explorations in Strategy*, 174.

44. David E. Sanger, *Confront and Conceal* (Portland, OR: Broadway Books, 2012), 190–91.

45. Sanger, *Confront and Conceal*.

46. Herb Lin, "Thinking about Nuclear and Cyber Conflict: Same Questions, Different Answers" (presentation, Hoover Institution / Center for International Security and Cooperation, Stanford University, CA, 15 May 2015), https://sipa.columbia.edu/sites/default/files/Thinking%20about%20Nuclear%20and%20Cyber%20Conflict-Columbia-2015-05-14.pdf.

47. Kinetic warfare "involve[s] the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles." US Air Force, "Air Force Glossary: Doctrine Document 1-2," 11 January 2007, http://www.globalsecurity.org/military/library/policy/usaf/afdd/1-2/afdd1-2-2007.pdf.

48. James Bret Michael, Eneken Tikk, Peter Wahlgren, and Thomas C. Wingfield, "From Chaos to Collective Defense," *Computer* 43, no. 8 (August 2010): 91–94, http://doi.ieeecomputersociety.org/10.1109/MC.2010.228; and US Department of Defense (DOD), Quadrennial Defense Review Report (Washington, DC: DOD, February 2010) https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf.

49. However, whereas the multiplier effect in economics takes time to work—often, several months pass before some of the effects are felt—this is not the case for offensive cyber operations, where (expected and desired) multiplier effects tend to take place over the course of days, or shorter. Also, this notion of CFCC as a force multiplier has led to the view that "cyber" is a key dimension of modern hybrid warfare. Frank Hoffman writes that "[h]ybrid wars are not new, but they are different. In this kind of warfare, forces become blurred into the same

force or are applied in the same battlespace." Sorin Dumitru Ducaru, "The Cyber Dimension of Modern Hybrid Warfare and its Relevance for NATO," *Europolity* 10, no. 1 (2016): 7–23, http://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf; James N. Mattis and Frank G. Hoffman, "Future Warfare: The Rise of Hybrid Warfare," *Naval Institute Proceedings* 131, no. 11 (November 2005): 30–32, https://www.usni.org/magazines/proceedings/2005-11/future-warfare-rise-hybrid-wars. For a more elaborate discussion also see Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Warfare* (Arlington, VA: Potomac Institute for Policy Studies, 2007).

50. James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory* (London: Transaction Publishers, 1967). These categories are adapted from Thompson's work on interactions and behaviors within an organizational structure.

51. A report from the UK House of Commons states "[a] recurring theme in Russian military strategy is the ability to combine tools seamlessly, to give a fully integrated, comprehensive approach. The Russian attitude to cyber as a tool for warfare is no different, with a full-spectrum approach integral to the strategy of the Russian Government." The use of the word "seamless" might be misleading considering Russia's conscious ongoing efforts to develop this approach, learning from its mistakes along the way. Indeed, Russia's attack on Georgia in 2008 was only partially successful, yet the more recent attacks on Ukraine suggests that it studied the lessons learned. Defense Committee, UK Parliament, "Russia: Implications for UK Defence and Security," House of Commons, 30 June 2016, https://www.publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/10710.htm; and David J. Smith, "How Russia Harnesses Cyberwarfare," *Defense Dossier* 4 (August 2012): 7–11, http://www.afpc.org/files/august2012.pdf.

52. This is in many ways similar to the industrial process of product-line development. Ironically, this also leads to the conclusion that, although integration is necessary, more integration is not necessary better.

53. The discussion of "loud cyber weapons" has primarily been about deterring future intrusions. Yet, it should also be considered in light of mitigating current intrusions and conflict. Quote from Chris Bing, "U.S. Cyber Command Director: We Want 'Loud,' Offensive Cyber Tools," FedScoop, 3 August 2016, https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016; Herb Lin, "Developing 'Loud' Cyber Weapons," *Lawfare* (blog), 1 September 2016, https://www.lawfareblog.com/developing-loud-cyber-weapons; Herb Lin, "Still More on Loud Cyber Weapons," *Lawfare* (blog), 19 October 2016, https://www.lawfareblog.com/still-more-loud-cyber-weapons; Adam Segal, "Takeaways From a Trip to the National Security Agency," *NetPolitics* (blog), 21 December 2016, https://www.cfr.org/blog-post/takeaways-trip-national-security-agency; and Timothy M. Goines, "Overcoming the Cyber Weapons Paradox," *Strategic Studies Quarterly* 11, no. 4 (Winter 2017): 86–111, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-4/Goines.pdf.

54. Richard J. Harknett and Michael P. Fischerkeller, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 61, no. 3 (2017): 381–93, http://doi.org/cp9b.

55. Quoted in Nick Ismail, "Under Attack: The UK Exposed to Constant Hostile Cyber Threats," Information Age, 13 February 2017, http://www.information-age.com/uk-constant-threats-cyber-attacks-123464417/.

56. For high-level counterforce cyber retaliation, it might nevertheless be possible, but if retaliation is used on a smaller scale it will be substantially more difficult.

57. According to Gartzke, this dimension is a key limitation: "Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable

harm on an adversary." The argument here is that cyberattacks can be turned into a strategic advantage as well. *See* Gartzke, "Myth of Cyberwar," 43.

58. There are, however, a set issues which have not been well-considered. For example, even if an effect is reversible, the targeted actor is likely to have lost general confidence in the integrity of the systems.

59. The effectiveness of these campaigns remains contested. *See* E. B. Strauss, "The Psychological Effects of Bombing," *Royal United Services Institution Journal* 84, no. 534 (1939): 269–82, http://doi.org/djj3h3; Stephen T. Hosmer, "Psychological Effects of U.S. Air Operations in Four Wars, 1941–1991: Lessons for U.S. Commanders," RAND Monograph Report RB-38 (Santa Monica, CA: RAND Corporation, 1998), https://www.rand.org/pubs/monograph_reports/MR576.html; and Martin Obschonka, Michael Stuetzer, P. Jason Rentfrow, Jeff Potter, Samuel D. Gosling, "Did Strategic Bombing in the Second World War Lead to 'German Angst'? A Large-Scale Empirical Test across 89 German Cities," *European Journal of Personality* 31, no. 3 (2017): 234–57, http://doi.org/cp9d.

60. Paul Marks, "Dot-Dash-Diss: The Gentleman Hacker's 1903 lulz," *New Scientist*, 20 December 2011, https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/?full=true. Telegraphy companies had invested in a dense network of land and sea cable network. The transatlantic wireless messaging service was a major threat to their competitive position.

61. Marks, "Dot-Dash-Diss."

62. Marks.

63. Sanger, *Confront and Conceal*, 199.

64. The worm was found by Sergey Ulasen in 2010 from VirusBlokAda, a relatively unknown security firm in Belarus. The worm was subsequently analyzed by researchers from Symantec, the Langner Group, and, later, others. Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, 7 November 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

65. *Der Spiegel*, "S*piegel* Interview with Syrian President Bashar Assad: 'Peace without Syria Is Unthinkable,'" *Spiegel* Online, 19 January 2009, http://www.spiegel.de/international/world/spiegel-interview-with-syrian-president-bashar-assad-peace-without-syria-is-unthinkable-a-602110.html.

66. Gray, *Explorations in Strategy*, 178.

67. Gray, 178.

68. Many talk about the reputation damage a company suffers after it falls victim of a successful cyberattack. For a major cyber incident—like those experienced by Target, J. P. Morgan, Ashley Madison, or Sony Pictures Entertainment—a company is said to face significant financial consequences (and management shake-ups). These reputation costs are often much higher than the cost to replace or restore the computer network that was initially damaged by the attack. (While companies normally suffer a drop in stock value directly after the breach/hack, stock prices normally quickly bounce back up. But the company suffers other breach/hack-related costs—also often including lawsuits.) Though governments might not run a "reputation risk" when their systems get compromised, which is quantifiable in company losses, successful compromise by an adversary can reduce general public trust authority (or factions which are responsible for a specific program)—which in turn can be exploited by other states. *See* Elena Kyochko and Rajiv Pant, "Why Data Breaches Don't Hurt Stock Prices," *Harvard Business Review*, 31 March 2015, https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

69. Quoted in PTI, "World Facing 'Bloodless' Cyber War Threat: Modi," *The Hindu*, 1 April 2016, http://www.thehindu.com/news/national/world-facing-bloodless-cyber-war-threat-modi/article7375190.ece.

70. Sanjay Gupta, "Dick Cheney's Heart," *60 Minutes*, CBS News, 20 October 2013, http://www.cbsnews.com/news/dick-cheneys-heart/; Andrea Peterson, "Yes, Terrorists Could Have Hacked Dick Cheney's Heart," *Washington Post*, 21 October 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.ea14d571e5fc.

71. William Alexander, "Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode," VICE, 25 June 2013, https://www.vice.com/en_se/article/i-worked-out-how-to-remotely-weaponise-a-pacemaker. In 2012, Jack demonstrated how a model of an insulin pump could be lethally hacked to administer incorrect dosages from up to almost 100 meters away. In 2013, he hacked into a pacemaker to show he was able to explode it.

72. Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, 19 October 2011, http://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/. Maurer considers a scenario in the past in which former Vice President Dick Cheney describes the decision-making process that occurred as the US considered whether or not to bomb a Syrian nuclear facility in 2007. Despite Israeli requests to do so, President George W. Bush decided to pursue a diplomatic rather than military option. So Israel took matters into its own hands. Cheney writes, "[u]nder cover of darkness on September 6, 2007, Israeli F-15s crossed into Syrian airspace and within minutes were over the target at al-Kibar. Satellite photos afterward showed that the Israeli pilots hit their target perfectly." (Quoted in Maurer, "Case for Cyberwarfare.") For Maurer, this highlights an important point: "Despite the attack being a perfect hit, a few people were probably still killed." (ibid.)

73. Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016). Libicki does not buy into the "peaceful nature thesis" as it only holds in a few theoretical scenarios. Libicki does not contest that cyberattacks have the potential to cause fewer casualties as the alternative is less often chosen than others conceive it to be. The key question here seems to be whether cyber capabilities are used instead of war or doing nothing. Most examples cited by proponents of the "peaceful nature" argument focus on when a state could have gone to war but used a cyber capability instead. The Iranian attack against Saudi-Aramco and the North Korean attack against Sony may be two cases that follow the reverse pattern; instead of doing nothing, a cyberattack was conducted.

74. Christopher Gelpi, Peter D. Feaver, and Jason Reifler, *Paying the Human Costs of War: American Public Opinion and Casualties in Military Conflicts* (Princeton, NJ: Princeton University Press, 2009).

75. For an excellent overview see Christopher Gelpi, Peter D. Feaver, and Jason Reifler, "Success Matters: Casualty Sensitivity and the War in Iraq," *International Security* 30, no. 3 (2005–2006): 7–46, https://www.belfercenter.org/publication/success-matters-casualty-sensitivity-and-war-iraq; and Peter D. Feaver and Christopher Gelpi, *Choosing Your Battles: American Civil-Military Relations and the Use of Force* (Princeton, NJ: Princeton University Press, 2004).

76. Bruce Jentleson, "The Pretty Prudent Public: Post-Vietnam American Opinion on the Use of Military Force," *International Studies Quarterly* 36, no. 1 (March 1992): 49–74, https://www.jstor.org/stable/2600916; Rebecca L. Britton and Bruce Jentleson, "Still Pretty Prudent," *Journal of Conflict Resolution* 42, no. 4 (1998): 395–417, https://www.jstor.org/stable/174436; Eric Larson, *Casualties and Consensus: The Historical Role of Casualties in Domestic Support for U.S. Military Operations* (Santa Monica, CA: RAND, 1996); Steven Kull, "What the Public Knows That Washington Doesn't," *Foreign Policy*, no. 101 (Winter 1995–1996):

102–15, https://www.jstor.org/stable/1149411; and Peter Feaver and Christopher Gelpi, "How Many Deaths Are Acceptable? A Surprising Answer," *Washington Post*, 7 November 1999, http://www.washingtonpost.com/wp-srv/WPcap/1999-11/07/061r-110799-idx.html. Several factors are listed in the literature as to what can shape this calculus. Jentleson's "pretty prudent" public argument is that tolerance is based on the objective of the military operation. Larson argues that tolerance depends on "elite consensus" behind the mission. Kull believes that the international support for a mission is the essential factor. And Feaver and Gelpi identify expectation of success as a key factor of explaining public casualty tolerance.

77. Interestingly, this conclusion was also drawn in an article written by a senior National Security Agency official, William Black, in 1997. Black states, "Another aspect of warfare that came with the Information Age is that actual, physical combat be viewed in living rooms of America via television. The horrors of war cannot be hidden. As a result, in the simplest of terms, 'body bags' are no longer acceptable. There is considerable societal pressure to find non-lethal means of accomplishing tasks that once called for conventional military action." William B. Black, "Thinking Out Loud About Cyberspace," *Cryptolog* 23, no. 1 (Spring 1997): 1–4, https://nsarchive2.gwu.edu//dc.html?doc=2700088-Document-11.

78. Thomas Rid, *Rise of the Machines*: *A Cybernetic History* (New York: W. W. Norton, 2016). As Rid writes in chapter 7, *Omni* was one of the first magazines depicting the changing nature of war in 1979. Talking about the future of cybernetic war, *Omni* envisioned four features: speed, automation, espionage, and precision.

79. Steve Bellovin, Susan Landau, and Herb Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity* 3, no. 1 (March 2017): 59–68, https://doi.org/10.1093/cybsec/tyx001.

80. There is nothing inherent to either CVCC or CFCC that makes one or the other more likely to cause undesired impact.

81. Bellovin, Landau, and Lin, "Limiting the Undesired Impact," 59.

82. Bellovin, Landau, and Lin, 59.

83. Bellovin, Landau, and Lin, 59. The main argument of Bellovin, Landau, and Lin's article is that precise targeting requires a "good technical design" and "good intelligence." At minimum, this conclusion is unspecified, as it is unclear what "good" means. A potentially more severe critique is that the empirical cases cited do not support the authors' conclusions. The scholars consider the DDOS attacks on Estonia and Georgia as two cases in which cyber-attacks were discriminate. Analysis of both these cases suggests, however, the technical and intelligence requirements were rather limited.

Soft Power in China's Security Strategy

LTC Mikail Kalimuddin, SAF
David A. Anderson

Abstract

The concept of "soft power" came to prominence in Chinese political and academic discourse in the mid-2000s and is now arguably a deliberate and integral part of Chinese foreign policy, facilitating China's rise by shaping the external environment. Examples of Chinese soft power include economic diplomacy with the global South, the "Beijing Consensus," public diplomacy initiatives like Confucius Institutes, and even tourism. This study expands on the existing body of scholarly literature on Chinese soft power by exploring its integration with China's security strategy. Two cases are examined: (1) the territorial disputes in the South China Sea and (2) cross-strait relations. The study demonstrates that soft power is integrated into China's security strategy and involves a wide range of sources of power.[1]

❋❋❋❋❋

> *The history of mankind tells us that problems are not to be feared. What should concern us is refusing to face up to problems and not knowing what to do about them. In the face of both opportunities and challenges of economic globalization, the right thing to do is to seize every opportunity, jointly meet challenges and chart the right course for economic globalization.*
>
> — Xi Jinping, World Economic Forum Annual Meeting 2017

In what was the single most headline-grabbing moment of the World Economic Forum's 2017 annual meeting in Davos, Switzerland, the president of the People's Republic of China, Xi Jinping, spoke at the opening plenary in defense of economic globalization. This took place

LTC Mikail Kalimuddin is a field artillery officer in the Singapore Army. He holds a BA in political science and economics and an MA in economics from Brown University. He is a graduate of the US Army Command and General Staff College (CGSC), Fort Leavenworth, Kansas.

Dr. David A. Anderson is a supervisory professor in the Department of Joint, Interagency, and Multinational Operations at the US Army CGSC.

against the backdrop of the recently concluded US presidential elections and growing concern about the incoming Trump administration's apparent willingness to embrace trade protectionism and isolationism. (As of 22 March 2018, President Trump did impose trade sanctions against China.) Whether merely an honest attempt to safeguard one of the critical requirements for China's continued economic growth or a deliberate masterstroke in strategic communications, the impact of Xi's comments on the narrative surrounding China's role in the international system was both immediate and profound. Many media outlets were quick to declare China as what *Newsweek* termed "the linchpin of global economic stability"—a title that would almost certainly have been heretofore reserved for the United States.[2]

Ostensibly, Xi's speech had not changed anything of material significance. Neither China's economy nor its military had increased in strength as a consequence of the speech. Yet China, at least according to the mainstream media, appeared to have assumed a new mantle of some importance. Clearly, then, some element of the relative power of actors in the international system had changed, but not in a manner that would be captured in any measurement of gross domestic product, troop numbers, nuclear missiles, or other metrics of that nature. What the meeting participants listening to Xi in Davos witnessed firsthand, whether they had realized it or not, was a palpable increase in Chinese soft power.[3]

By many estimates, major powers such as the US, the UK, Germany, France, and Japan currently enjoy a commanding lead over China in soft power terms.[4] Consequently, policy makers who focus solely on the role of hard power in state-to-state relations must recognize that their analysis is premised on the existence of this soft power disparity. While this may remain the case in the short term, China's continued development could result in this gap closing, if not at least narrowed. Indeed, soft power now enjoys a distinct role in China's security strategy. This article assesses the role of soft power in China's security strategy so policy makers dealing with China are equipped to conduct a holistic assessment of Chinese power and adjust their strategies accordingly. Then it analyzes the territorial disputes in the South China Sea (SCS) and China's handling of its relations with Taiwan. The case studies are delimited in two ways. First, the cases will be bounded in time from 2010 to the present. Second, the analysis will seek only to explain how soft power is used—not

whether it is effective. Dealing with the rise in Chinese soft power has implications for policy makers.

Assessing Soft Power and Chinese Security

Accumulating and exercising soft power has become a deliberate component of Chinese foreign policy. The paramount leaders of the Chinese political establishment have spoken and continue to speak on this subject. Then-Chinese President Hu Jintao made reference to soft power (*ruan li liang*), while addressing the Chinese Central Foreign Affairs Leadership Group in 2006.[5] This emphasis on soft power has continued a decade into Xi's tenure and is viewed as one of the elements necessary to realize the "Chinese Dream"—the revitalization of Chinese society and achievement of national glory.[6] The concept of soft power is also prevalent in Chinese academic discourse, with works by Chinese intellectuals forming a large part of the body of literature on Chinese soft power. Regardless of the extent to which Chinese politicians and intellectuals speak and write about soft power, the real world is rife with examples of Chinese soft power at work. Confucius Institutes—nodes of Chinese culture and language—number in the hundreds and are present on six continents. The Asian Infrastructure Investment Bank (AIIB), a Chinese initiative that came to fruition at the end of 2015, has a membership of 50 states and half as much capital as the World Bank. More importantly, China controls over a quarter of the votes in the AIIB. The list of soft power tools at China's disposal is long and growing, the significance of which actors in the international system can ill afford to ignore.

For the purposes of this research, "soft power" is defined as the "ability to obtain desired outcomes through attraction rather than coercion or payment."[7] The characteristic feature of soft power is that it enables a country to "structure a situation so other countries develop preferences or define their interests in ways consistent with its own."[8] Critically, this definition does not limit soft power to any particular type of power; it deals instead with the intended effects of power. For completeness, the antithesis of soft power is "hard power," which is defined as the use of power by a country to coerce or induce other countries to take certain actions or adopt particular positions.[9] Whereas soft power is about "shaping what others want," hard power "changes what others do."[10]

It should be noted that this is not the only established definition of soft power, nor is it purported to be an unequivocally superior definition

of soft power. Rather, this definition has been selected for its utility in shedding light on the "softer" elements of China's security strategy and hence best serves the objectives of this research. Narrower definitions generally define soft power according to the type of power involved rather than its effects. Particularly in the security domain, where certain types of power predominate, a restrictive definition would severely limit the number and variety of instances of soft power in the cases being studied and unnecessarily constrain the research. Broader definitions of soft power, however, blur the line between instances of power that are soft and those that are not. Without this distinction, the question this research seeks to answer becomes invalid.

Following from the definition of soft power, an analytical framework is needed to draw the link between observed instances of power and their intended effects. To this end, the research codes observations according to the three predetermined categories of "sources," "tools," and "modes." "Sources of power" or "sources" are the domains countries draw upon to exercise hard or soft power. Examples of sources of power include the economic, military, institutional, and cultural domains. Sources of power are neither hard nor soft when considered in isolation, as they do not prescribe the manner in which power is used. Nonetheless, an expanded military force or greater cultural cache, for example, means that a state's soft power (and hard power) potential is increased. "Tools of power" or "tools" refer to the specific forms in which sources of power manifest. For example, a financial loan is a tool, as is an art exhibition. A financial loan is likely to be derived from the economic domain; an art exhibition from the cultural domain. Tools need not be physical in nature. A speech by a political figure espousing a particular position is also a tool. Like sources of power, tools of power are also neither hard nor soft. A greater variety of tools provides a state with more avenues through which to draw on its potential power. "Modes of power" or "modes" refer to the ways in which tools of power are used. A mode comprises a multitude of factors, though it is described primarily by the intent of the actor exercising power and the audience that perceives the exercise of power. The mode of power is essentially the intended effect of a tool and therefore determines whether a tool of power is ultimately soft or hard—it is power in action.

Simply identifying the various forms of Chinese soft power at play in the security domain would fall short of the purpose of the research;

a final step in the analysis is necessary. Here, core concepts—potential aspects of China's soft power strategy, or "strategic aims"—are identified, abstracted, and synthesized to generate the desired product of this research: a hypothesis about the role of soft power in China's security strategy.

The South China Sea Disputes

The disputes center on unresolved claims by a handful of East Asian countries over a variety of land features in the SCS. Countries are reluctant to concede or agree to compromises in their claims for several reasons: (1) to gain exclusive access to resources in the waters and sea bed surrounding and beneath the features such as fisheries, oil, and natural gas; (2) to control major international shipping routes; and (3) because of the symbolic significance that is invariably attached to matters of national sovereignty.[11] Resolving these claims is made especially problematic because of the limitations of international maritime law, a sizeable part of which is based on international customary law. Even where countries have committed themselves to international agreements, gray areas remain. For example, the United Nations Convention on the Law of the Sea (UNCLOS) defines the territorial and economic rights that littoral states have with regard to the different types of land features (archipelagos, islands, reefs, rocks, etc.). However, it does not determine the rightful ownership of territory that is disputed or the appropriate status of land features in cases where countries disagree. Further complicating such agreements are the numerous caveats and reservations that countries attach to their participation.[12]

The claimants in the SCS disputes are China, Taiwan, Brunei, Malaysia, the Philippines, and Vietnam. China's extensive claims in the SCS, represented by the Nine-Dash Line, overlap with the claims made by all four Southeast Asia (SEA) countries. China and Taiwan's claims are effectively identical; however, China views Taiwan's claims in the SCS as complementary to its own, if not simply invalid. China and Taiwan base their SCS claims on the same map "issued in the late 1940s by China's then-Nationalist government."[13] Since Taiwan's claims are based on the same historical evidence as China's, Taiwan's claims only serve to lend credibility to China's. In addition, China believes that the territory of Taiwan will eventually be reunified with the mainland as a single political entity; hence Taiwan's claims are not viewed as competing with

China's.[14] Involvement in the disputes is not limited to claimant states.[15] The intensity of the disputes has risen and fallen repeatedly since the end of the Second World War. The most recent period began in 2009 with a new round of claims submitted by a number of states, including China with its Nine-Dash Line.[16] Since then, tensions in the SCS have continued to escalate steadily as a result of a series of actions and counteractions by both claimants and non-claimants.

Chinese Soft Power in the SCS

China's use of soft power in its handling of the SCS disputes has three strategic aims. First, it seeks to control the terms of discussion. China's goal is to strengthen the legitimacy of its claims in the SCS. This is done by redefining the legal basis upon which maritime boundary delimitation occurs, establishing the history of its claims, and controlling the manner in which disputes are managed and resolved. Controlling the terms of discussion allows China to increase the likelihood that the disputes will ultimately be resolved in its favor. The second strategic aim is to make China a preferred partner. By increasing its value to countries in the region, particularly among claimant states, and projecting an image of constructive participation in regional affairs, China hopes to soften opposition by other states to its activities in the SCS and encourage claimant states to work with China in resolving the disputes in a manner it deems appropriate. Finally, China wants to prevent interference. By reducing the extent to which non-claimant states influence developments in the SCS, China increases its leverage over claimant states. This pertains especially to the US, which possesses the economic, military, and political heft to both counter China unilaterally and maintain a tacit coalition of states that are able to work together to oppose China in the SCS. It also ensures China is able to isolate other claimant states through bilateral negotiations.

These strategic aims are inferred based on the observed application of sources, tools, and modes by China in its handling of the SCS disputes.[17] Specific components of soft power support each strategic aim, with links between the various components (refer to figure 1).

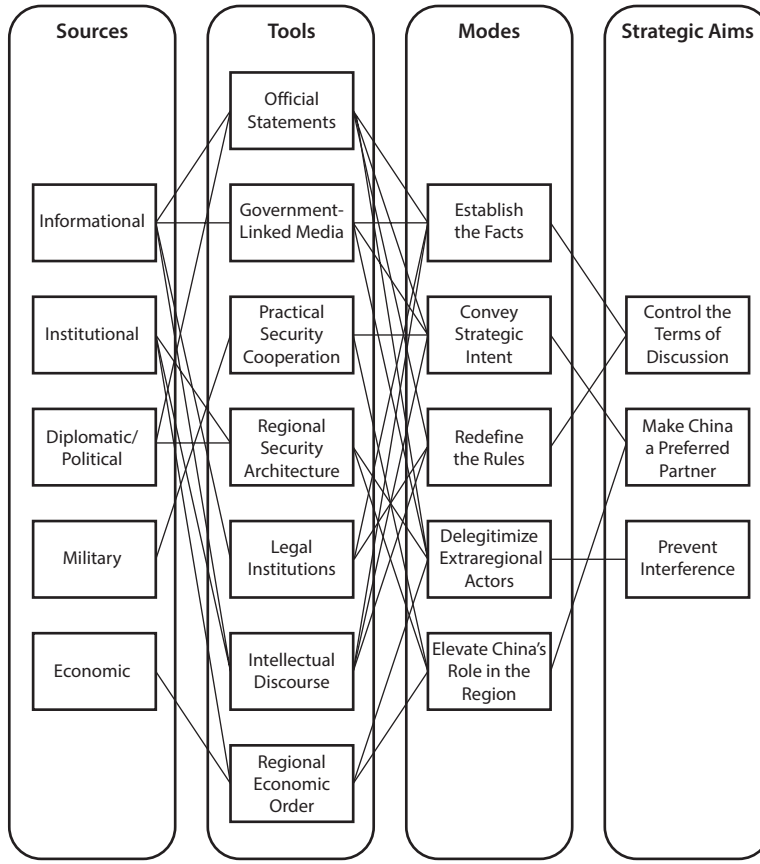

Figure 1. Depiction of soft power strategy—the SCS disputes

Control the Terms of Discussion

China's first strategic aim is to control the terms of discussion and by doing so increase the likelihood that the SCS disputes are managed and eventually resolved in its favor. This strategic aim draws on informational, institutional, and diplomatic sources of power to achieve two effects: (1) establish China's version of the facts and (2) redefine the rules to China's advantage.

Establish the facts. China's efforts in establishing the facts serve its goal of influencing what the facts are. Through a combination of official statements, products from official Chinese media, and participation by Chinese academics in the ongoing intellectual discourse on developments in the SCS, China seeks to convince the global public of the historical basis of its claims in the SCS. It argues that "the Chinese people

[were] the first to discover, name, develop and administer the Islands, and that the Chinese government was the first to peacefully and effectively exercise continuous sovereign jurisdiction on South China Sea Islands," citing both occidental and oriental historical maps as corroborating evidence.[18]

China has left no stone unturned in its efforts to "educate" the world. In 2016, China ran a video advertisement in New York City's Times Square, providing evidence for the validity of its claims in the SCS. The three-minute-long video ran 120 times a day for a period of 10 days and included soundbites from both Chinese and non-Chinese government officials.[19] Official Chinese media outlets like China Central Television (CCTV) and Xinhua have established dedicated online sites in English that reiterate China's position on the facts.[20] These sites supplement the official online repository maintained by the Chinese Ministry of Foreign Affairs (MoFA) that details the Chinese government's position on all SCS-related matters.[21] CCTV has also produced online videos that convey similar information but use an animated format that is likely to have greater appeal among online viewers.[22]

China's attempts at shaping intellectual discourse on the SCS go beyond the efforts of individual Chinese policy makers and academics. At the institutional level, China has established think tanks and institutions with a sole focus on the SCS. Among them are the Collaborative Innovation Center for South China Sea Studies (CICSCSS) established in 2012 and the National Institute for South China Sea Studies (NISCSS) established in 2013 as the successor to the Hainan Research Institute for the South China Sea. The NISCSS in turn sponsors the Institute of China-American Studies (ICAS) which is based in Washington, DC. ICAS "has a relatively low profile in Washington but has become [a] frequent contributor to American events discussing the South China Sea disputes."[23] These institutions provide China with the means to promulgate its version of the facts to non-Chinese academics and policy makers without drawing as much attention to China's underlying agenda.

Redefine the rules. China also seeks to redefine the rules by influencing which facts are relevant and how disputes should be resolved. By determining which facts are relevant, China hopes to redefine the legal basis by which international maritime boundaries are delimited and "shape international opinion in favor of a distorted interpretation of the UN Convention on the Law of the Sea."[24] Here again, official

statements frequently point to China's historical claim to territory in the SCS and reference "traditional fishing areas" as the basis on which China claims economic rights in various parts of the SCS. In terms of the manner in which disputes should be resolved, Chinese officials reference China's past successes in resolving boundary issues with its neighbors as an indication that bilateral negotiations are the best way forward in the SCS.[25] Institutions like the CICSCSS, NISCSS, and ICAS serve the dual purposes of providing China with a platform to share its interpretation of the rules among experts in the field and with a means by which to grow its own cadre of researchers and academic experts to bolster its institutional capacity to inform the intellectual discourse.

While China can easily establish think tanks and academic institutions to enhance its intellectual soft power, growing its influence in the area of maritime law poses a much greater challenge. Legal institutions, particularly those that function in the realm of international law, draw their legitimacy from the body of states that recognize their authority. This has not stopped China from trying to establish its own alternative legal institutions. In 2016, the chief justice of the Supreme People's Court announced that China would unilaterally establish an International Maritime Judicial Center (IMJC) that will adjudicate on maritime disputes.[26] By publicizing its judgments and judicial views, China hopes the IMJC will enable it to reshape legal norms in maritime disputes to its advantage—an approach informally termed by observers as "law fare."

Make China a Preferred Partner

China's second strategic aim is to present itself as a preferred partner to the member states of ASEAN and by so doing both soften their opposition to China's activities in the SCS and increase their receptivity to China's espoused approach to resolving the territorial disputes. This strategic aim draws on informational, institutional, diplomatic, military, and economic sources of power to achieve two effects: (1) conveying China's strategic intent and (2) elevating China's role in the region.

Convey strategic intent. China seeks to communicate a version of its strategic intent that will allay the fears of ASEAN member states and convince them of China's desire to work toward outcomes that are beneficial to all parties. At every opportunity, Chinese officials have reiterated their government's commitment to "rules and mechanisms

for management and control of differences of opinion," "realizing mutual benefits through cooperation," "safeguarding freedom of navigation in and flight over the South China Sea," and, more generally, "peace and stability in the South China Sea."[27] Official Chinese media outlets and Chinese academics from state-linked institutes present a similar refrain.

To back up its rhetoric, China has pointed to its support for ASEAN-China maritime cooperation, which includes a half-billion-dollar fund that it established in 2011, as well as to its proposals for confidence building measures (CBM) and "hotlines" to better manage potential conflicts in the SCS. It has also reiterated its support for the implementation of the Declaration on the Conduct of Parties in the South China Sea (DOC), and continued consultation on the ASEAN-China SCS Code of Conduct (COC). These efforts in practical security cooperation serve to demonstrate China's commitment to making its "dual-track" approach work—resolution of disputes through bilateral negotiations between claimant states, supported by a multilateral ASEAN-China effort to maintain peace and stability in the SCS.

China has also communicated its intent to maintain stability in the SCS through its willingness to work with the US. For example, China agreed to a Code for Unplanned Encounters at Sea (CUES) at the Western Pacific Naval Symposium in 2014.[28] It has since participated in bilateral CUES exercises with the US Navy and employed CUES during its encounters with the US naval vessels in the SCS. To allay concerns over its construction of dual-use facilities on its islands in the SCS, China has couched these developments as a way for China to "better perform [its] international responsibilities and obligations."[29]

Elevate China's role in the region. China has taken steps to increase its value and links with member states of ASEAN and in regional structures, in order to increase its attractiveness as a regional partner. In terms of the regional security architecture, China has continued to increase its participation in "multilateral dialogues and cooperation mechanisms such as the ASEAN Defense Ministers' Meeting Plus (ADMM+), ASEAN Regional Forum (ARF), Shangri-La Dialogue (SLD), Jakarta International Defence Dialogue (JIDD) and Western Pacific Naval Symposium (WPNS)."[30] It has also embarked on its own initiatives, such as the Xiangshan Forum—a track 1.5 regional security dialogue, which was inaugurated in 2009 but has significantly expanded in recent years—and the establishment of the China-ASEAN Defence Ministers'

Informal Meeting in 2015. China has also stated that it "resolutely supports ASEAN exhibiting a leading role in cooperation in the East Asia region" and has taken on a series of projects to demonstrate this support in a concrete manner.[31] China is an active participant in the ARF and has led more than 40 cooperation projects, constituting one-third of the total number of projects and the highest number among member states.[32]

Practical security cooperation is also a feature of China's soft power. It conducted humanitarian assistance and disaster relief (HADR) operations in support of the Philippines following Typhoon Haiyan in 2013 and in support of Malaysia following severe flooding in 2014. It also participated in the ARF Disaster Relief Exercise 2015 held in Malaysia. With Thailand, China has "numerous shared security interests, particularly regarding non-state threats in the Mekong River basin."[33]

From an economic perspective, China's value to the region has grown significantly. In addition to the large and growing volume of bilateral trade and investment with ASEAN member states, China's institutional influence has been enhanced by its establishment of the Asia Infrastructure Investment Bank (AIIB). The China-ASEAN Investment Cooperation Fund, which began its operations in 2010, serves as another symbol of China's commitment to economic development in SEA.

Prevent Interference

China's third strategic aim is to prevent interference from non-claimant states, particularly the US, and by doing so maintain its freedom of action in the SCS and increase its leverage in bilaterally negotiated dispute settlements. This strategic aim draws on informational, institutional, diplomatic, and economic sources of power to delegitimize extra-regional actors.

Unlike the first two strategic aims, which serve to enhance China's soft power, this third strategic aim focuses on reducing the soft power of extra-regional actors that pose a threat to China's achievement of its goals in the SCS. Statements by Chinese officials and the state-run media have sought to "[malign] the [US'] role in initiating and escalating tensions."[34] China's line of argument is that the militaristic nature of US involvement has introduced destabilizing elements in the SCS and points to "freedom-of-navigation operations in the South China Sea, flaunting its military force, and . . . pulling in help from cliques, supporting their allies in antagonizing China."[35] China has also sought to draw attention to

what it perceives as a history of "power politics and bullying by Western Powers."[36]

China argues that states in the region should be allowed to collectively develop their own approach to achieving peace and stability in the SCS without unwanted external interference. It has proposed the idea of a "security-governance method in keeping with the special characteristics of this region" or an "Asian way of comfort" that focuses on "non-aligned relationship routes," with the goal of excluding extra-regional actors.[37] China's extensive efforts in developing ASEAN-China initiatives also serve to limit the influence of actors like the US and Japan by reducing their role in the regional security architecture.

From an economic perspective, China has sought "to undermine U.S. dominance in established trade blocs while touting the benefits of a China-led order through its own initiatives."[38] Much like the AIIB, the Regional Comprehensive Economic Partnership (RCEP) offers the region an economic structure that has little in the way of a role for the US. The recent withdrawal of the US from the Trans-Pacific Partnership (TPP), which would have been an alternative, has only increased the attractiveness of realizing the RCEP.[39] This regional economic framework, along with the AIIB and the various funds operated by China for ASEAN and its member states, reinforces the perception of the US' waning economic relevance in the region.[40] This undercuts US soft power in the region and weakens its ability to maintain a grouping of countries, both claimants and non-claimants, are willing to work with the US to block China from achieving its designs for the SCS.[41]

Overall, China's soft power strategy appears to work hand-in-hand with its hard power goals in the SCS to "safeguard [China's] maritime rights and interests."[42] By controlling the terms of discussion, China is able to reshape not just the physical state of play in the SCS but also the legal and historical aspects of the disputes. It also increases the likelihood that its preferred method of resolving the disputes—bilateral negotiations—will eventually be agreed to by other claimant states. China's hard power goal of countering and fragmenting opposition to its claims is supported by soft power efforts to make China a preferred partner in the region and prevent interference by extra-regional actors. As the de facto leader of the loose grouping of countries opposed to China's actions in the SCS, the US will find itself hard-pressed to maintain the commitment of other states in resisting China, particularly as its soft power in the

region is diminished. China, on the other hand, will benefit from the growing desire of other states in the region to work with it as its status as a preferred partner rises.

Cross-Strait Relations

In 1949, China's Nationalist government, the Kuomingtang (KMT), was defeated by the Communist Party of China (CPC) and fled to the island of Taiwan, marking the end of the Chinese Civil War. Since then, China's fundamental position has remained essentially unchanged: it sees Taiwan as a rogue province that must eventually be reunified with China under the control of the CPC. Up until 2000, Taiwan's government also maintained the position that the territories of China and Taiwan would eventually be reunified, albeit under its control. The combination of these two political end states was captured in the 1992 Consensus that developed out of a meeting between representatives of the CPC and KMT and is the basis for the current interpretation of the "One China principle."[43]

The election of Chen Shui-bian from the pro-independence Democratic Progressive Party (DPP) as president of Taiwan in 2000 marked the beginning of a period of increased turbulence in cross-strait relations. Unlike the KMT, the DPP has not publicly accepted the 1992 Consensus, and while it has not attempted to make a formal declaration of Taiwanese independence, it is a strong proponent of a distinct Taiwanese identity. From 2000 to 2008, the Chinese government employed a host of coercive measures to dissuade the DPP from putting Taiwan on a path to independence, including the suspension of high-level interactions with the Taiwanese government, the passing of the Anti-Secession Law, and intensified diplomatic isolation of Taiwan.[44] During this eight-year period, no agreements were signed between China's Association for Relations across the Taiwan Straits (ARATS) and Taiwan's Straits Exchange Foundation (SEF), nor were there any formal interactions between the two organizations.[45]

The return to a KMT-led Taiwanese government in 2008 resulted in an immediate improvement in cross-strait relations and steadily increasing levels of cooperation between China and Taiwan in a variety of areas. However, the relatively healthy political situation is at odds with social trends among the Taiwanese population. "Since the 1992 consensus, the proportion of people on the island who identify themselves simply

as Taiwanese has more than tripled to almost 60%; the share of those who call themselves Chinese has plunged to just 3%."[46] This issue of identity is even more pronounced among Taiwanese youth and most notably manifested as student-led protests in the 2014 Sunflower Student Movement.[47]

In the 2016 round of elections in Taiwan, the DPP gained control of both the executive and legislative branches for the first time in Taiwan's history. While the current Taiwanese president, Tsai Ing-wen, has thus far taken a more conciliatory approach to cross-strait relations than former President Chen, China remains wary about her political goals and has made repeated calls for her to recognize the 1992 Consensus as a precursor to any further improvement in ties between China and Taiwan. The 2016 election also saw the emergence of the New Power Party, which has its roots in the Sunflower Student Movement and advocates independence for Taiwan. This points to trends in Taiwan's political landscape that will likely have an increasingly deleterious impact on cross-strait relations.

Chinese Soft Power in Cross-Strait Relations

The research indicates that China's use of soft power in handling cross-strait relations has two strategic aims. The first is to build robust social ties. China's goal is to undercut the emergence of a strong Taiwanese identity that is entirely separate from China. This is done by playing up the common historical identity that Taiwan shares with China and by creating an environment that promotes social reintegration between the Chinese and Taiwanese after decades of isolation from each other. Deep social ties serve as an anchor to prevent Taiwan drifting away from China toward independence. Next, China aims to engender a sense of shared prosperity. It seeks to convince the Taiwanese population that a close relationship is essential for Taiwan's continued prosperity. This involves developing a high level of economic interdependence between China and Taiwan as well as creating the perception that China is committed to supporting Taiwan's interests. By China having portrayed itself as a guarantor of Taiwan's continued prosperity, the Taiwanese will be less likely to support a political agenda that puts the stability of cross-strait relations at risk.

These strategic aims are inferred based on the observed application of sources, tools, and modes by China in its handling of cross-strait relations.[48] The components of soft power that support each strategic

aim, as well as the links between the various components, are shown in figure 2 below.

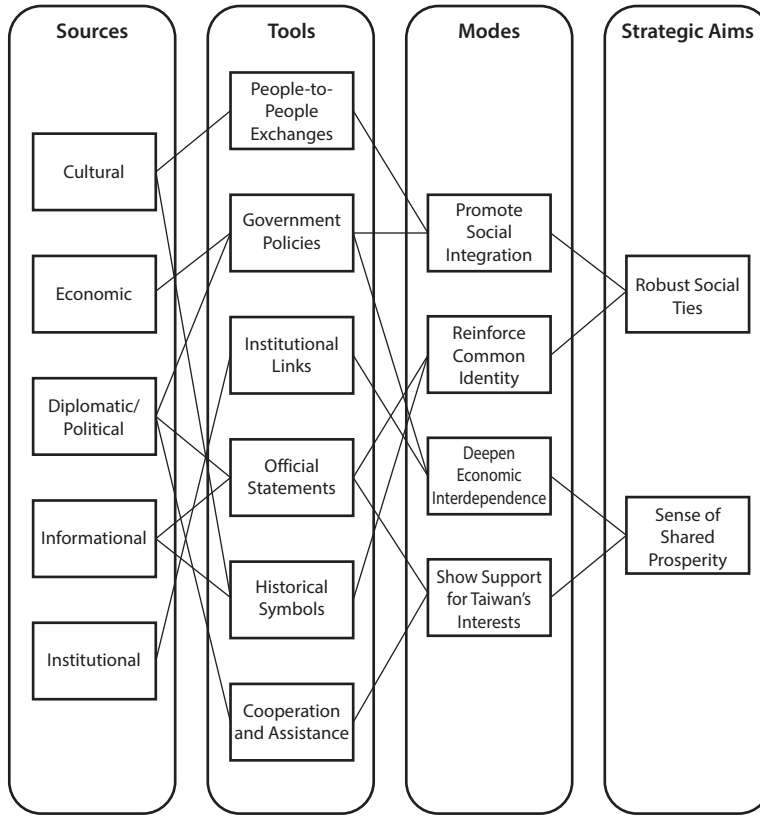

Figure 2. Depiction of soft power strategy—Taiwan

Build Robust Social Ties

China's first strategic aim is building robust social ties and by doing so provide a counter to the emergence of a Taiwanese identity that is entirely separate from China. This strategic aim draws on cultural, political, and informational sources of power to achieve two effects: (1) promote social integration and (2) reinforce a common identity.

Promote social integration. China seeks to promote the integration of the Taiwanese population into Chinese society through a combination of tools. The first of these has been to grow the number of people-to-people exchanges, "especially among ordinary citizens."[49] Cross-strait tourism appears to be one of the ways that this being achieved and is generally viewed as "a peace-building mechanism."[50] Beyond the rising

number of direct air routes and flights between China and Taiwan, entry requirements for Taiwanese to enter China have been eased. In 2015, per-visit entry permits were replaced with electronic travel passes that allow for multiple trips within a fixed duration.[51] China also is specifically targeting Taiwanese youth, as this segment of the Taiwanese population identifies very weakly with China and, consequently, serves as a strong base of support for the pro-independence agenda. Chinese officials have declared their intention to "boost the loyalty of young people from Taiwan . . . by organizing 'study trips' and exchanges for them to visit the mainland."[52] This proliferation of people-to-people exchanges also extends to the realm of academia. The number of Taiwanese students in Chinese universities has increased significantly over the past few years, from 928 in 2011 to 2,734 in 2014.[53] In 2016, a cross-strait think tank forum involving academics and experts was included for the first time in the annual Cross-Strait Forum, adding to a growing number of opportunities for exchanges between Chinese and Taiwanese academics.[54]

As evidenced by the suspension of high-level Taiwanese Affairs Office (TAO) and the Mainland Affairs Council (MAC) and ARATS-SEF interactions in May 2016, the DPP's control of the Taiwanese government may appear to constitute a major dampener on people-to-people exchanges between China and Taiwan. However, the reality is that this is largely political theater and only affects interactions between the top tiers of the two governments. In contrast, exchanges between city governments, professional associations, academic groups, and so forth have not been affected.

Policy measures have also been taken by the Chinese government to support the social integration of the Taiwanese into China. This includes preferential policies that "cover employment, social insurance and living needs" and "facilitate Taiwanese to live and work on the mainland."[55] China has made it easier for Taiwanese professionals to work in China. For example, Taiwanese law firms have been allowed to establish representative offices in China since 2011, and a sizeable number of Taiwanese are now qualified to practice law in China.[56] The number of intermarriages between Chinese and Taiwanese people has also grown significantly over time, increasing by more than 10,000 couples annually. In 2012, the Chinese government established an association specifically to provide assistance to these cross-strait couples across "a wide spectrum of

social services such as employment, social security, medical care, education and child bearing and raising."[57]

Reinforce a common identity. China has sought to reinforce the common historical identity that it shares with Taiwan. In their remarks, Chinese officials consistently refer to the Taiwanese in some form or other as "our own flesh and blood."[58] At the historic 2015 Xi-Ma meeting, Xi remarked that "we [Taiwanese and Chinese] are closely-knit kinsmen, and blood is thicker than water."[59] China has also couched this common identity in the form of a shared future by referencing the "Chinese dream" and the "great rejuvenation of the Chinese people" in the context of cross-strait relations.[60] Chinese officials have even gone as far as appealing to a sense of shared duty or national obligation by framing the disputes in the SCS and ECS as a responsibility to be borne by both Taiwan and China collectively.[61]

China has also leveraged historical symbols to emphasize the common identity between China and Taiwan. In 2011, a joint forum on Sun Yat-sen—the founder of the KMT—was held in Guangzhou and included high-level representation from the CPC. The forum coincided with the centennial of the 1911 revolution and focused on the "philosophy and ideas of Sun," "the rejuvenation of the Chinese nation," and Sun's role in the overthrowing of the Qing Dynasty.[62] In 2015, China commemorated the 70th anniversary of the end of the Second World War, which included a series of cross-strait events that drew attention to the contributions of the Communists and Nationalists in defeating the Japanese, with victory "only possible through the efforts of the entire nation."[63] Both KMT and CPC veterans were included at the front of the internationally televised and widely attended 2015 China Victory Day Parade. China's willingness to acknowledge and publicize the involvement of the Nationalists in modern Chinese history points to the increased emphasis it has placed on reinforcing a common Chinese identity among the Taiwanese.

Engender a Sense of Shared Prosperity

China's second strategic aim is to engender a sense of shared prosperity and use this to encourage Taiwan to pursue a political future where it remains hitched to China. This strategic aim draws on economic, political, informational, and institutional sources of power to achieve two

effects: (1) deepen economic interdependence between China and Taiwan and (2) show China's support for Taiwan's interests.

Deepen economic interdependence. China's goal is to develop a sufficiently deep level of economic integration with Taiwan such that the Taiwanese will consider a stable relationship with China essential to a prosperous future. Developing cross-strait economic links has long been a component of China's "embedded reunification" strategy; however, its potential has increased as China's economy has surged and Taiwan's has slowed.[64] China has pushed this economic integration through a combination of government policies and increased institutional links.

In terms of government policies, China and Taiwan signed the Economic Cooperation Framework Agreement (ECFA) in 2010—the first ever cross-strait trade agreement. The economic benefits of the agreement are generally tilted in Taiwan's favor. For example, "China eliminates tariffs on almost twice as many goods as Taiwan" and "opens up more of its service sector for Taiwanese entrepreneurs to invest in on the mainland."[65] This suggests that China's motivations for establishing the agreement lie beyond the apparent economic benefits. Since then, China and Taiwan have established a plethora of additional economic agreements, covering areas like taxation, finance, aviation, shipping, and services. This has continued even in Tsai's first term as president, with the launch of a preferential customs clearance program in the second half of 2016.[66]

In general, Chinese officials have made clear their intention to pursue economic policies that are preferential toward the Taiwanese.[67] For example, a comprehensive economic zone was established on Pingtan Island, in Fujian, China, as a pilot area for cross-strait cooperation. Businesses in the area can conduct banking in both Chinese and Taiwanese currencies and benefit from tax reductions. There are also preferential policies that make it easier for Taiwanese professionals to be employed within the zone.[68] More broadly, Chinese companies have invested approximately US $1.7 billion in Taiwan since being given the green light to do so in 2009, creating 11,400 Taiwanese jobs in the process.[69]

China has also increased its institutional links with Taiwan, which in turn support the growth of economic ties. In terms of financial institutions, Taiwan-based banks have been allowed to open branches in China since 2011, and a growing number of Taiwanese securities firms now have a presence in China.[70] A Cross-Strait Industrial Cooperation Forum has been established to "[strengthen] cooperation in hi-tech and

new industries."[71] This is in addition to numerous other economic forums that have for years been promoting cooperation across a wide variety of industries. China has also expressed a desire to have ARATS and SEF establish "cross-strait offices" in Taiwan and China respectively, though this has yet to come to fruition.[72]

Show support for Taiwan's interests. Simply establishing strong economic ties is unlikely to be sufficient to convince the Taiwanese that China is deeply invested in Taiwan's long-term future. To this end, China has made an effort to demonstrate its support for Taiwan's interests through its rhetoric and actions. Beyond references to the shared realization of the "Chinese dream" and the "great rejuvenation of the Chinese people," Chinese officials have explicitly stated that "the Chinese mainland will continue to strengthen the protection of the rights and interests of Taiwan compatriots."[73] In 2014, the TAO established an office specifically tasked to "manage public petitions related to Taiwan affairs" and "listen to the complaints and demands of Taiwan compatriots and Taiwanese spouses in the mainland and try to solve their problems."[74]

In terms of practical cooperation and assistance, China has offered humanitarian relief to Taiwan on a number of occasions. In 2012, China donated US $100,000 to Taiwan to assist with rainstorm-relief efforts.[75] In the aftermath of the 2015 earthquake in Nepal, China offered its assistance to Taiwanese in Nepal, saying that "both sides are of one family."[76] China has also cooperated with Taiwan on issues of cross-border crime since a mechanism for mutual assistance was established in 2009. In 2012, a joint China-Taiwan police operation resulted in a successful raid against a human-trafficking ring.[77] These actions are intended to convince the Taiwanese public that China's support for Taiwan extends beyond pure economic interest.

While the ultimate aim of all Chinese actions in regards to cross-strait relations is to prevent Taiwan from seeking independence and steer it towards eventual reunification, it appears that China's hard and soft power strategies are directed at different audiences. On the one hand, hard power has been primarily applied in a political context to influence the policies of the Taiwanese government—a combination of diplomatic strangulation as well as political tit-for-tat. On the other hand, soft power has focused on maintaining a favorable perception of China among the Taiwanese population—"to place hopes in the Taiwanese people," as the "slogan frequently uttered by Chinese leaders" goes.[78] This distinction

in the aims of China's hard and soft power strategies comports with the Taiwanese perception of "relatively low 'people-targeted' hostility" and comparably higher "'government-targeted' hostility" from China.[79]

Case Analysis and Observations

A series of meaningful observations can be made based on the results of these two case studies. First, the fundamental question of whether soft power has a distinct role in China's security strategy is answered in the affirmative. As was demonstrated in both case studies, varied combinations of sources, tools, and modes are employed by China to support a series of strategic aims. Consequently, any analysis of Chinese security strategy that deals with hard power alone or merely offers a superficial treatment of soft power should be questioned for its completeness.

Second, Chinese soft power draws on a wide range of sources, from commonly recognized sources of soft power such as culture and institutions to the traditionally "hard" domain of military power. That being said, not every source of soft power is present across all cases. The common social roots that the Chinese and Taiwanese share is unique to cross-strait relations, making culture a natural source of soft power. This is hardly applicable in the SCS disputes given the diverse range of players. On the other hand, the historical and political dynamics between China and Taiwan preclude the use of the military as a source of soft power. This differs markedly from the SCS disputes where militaries can simultaneously compete and cooperate with one another, enabling the PLA to be employed as hard and soft power.

Third, the relationship between soft and hard power varies depending on the specific issue. As highlighted in the analyses of the two cases, soft power and hard power are mutually reinforcing components of China's strategy in the SCS disputes. In the case of cross-strait relations, the purpose of exercising soft power is fundamentally different than that of hard power. It differs in time horizon (long-term rather than short-term), objective (promoting reunification rather than preventing independence), and target audience (people rather than politics). This suggests that the role of soft power is not limited to enhancing the effects of hard power; under certain circumstances, soft power may be employed to achieve aims that hard power simply cannot.

Implications for Policy Makers

The immediate implication for policy makers is self-evident: any strategy for dealing with Chinese actions that hopes to be effective must account for both the hard and soft power strategies employed by China. As an example, if the US' withdrawal from the TPP is considered solely from the perspective of hard power, it would appear to have little direct impact on the SCS disputes. Ostensibly, the withdrawal has implications for US influence in the Asia-Pacific in general, but it is difficult to identify how it might relate to China's strategy in the SCS disputes specifically. If, however, we consider the soft power strategic aim of "making China a preferred partner," then it becomes apparent that the withdrawal provides China with a strategic opportunity to advance this aim through a competing agreement like the RCEP, which advances China's agenda of substituting US leadership of the regional economic order with its own.

By understanding China's soft power strategy, policy makers can more accurately and comprehensively assess the impact of their decisions. With the SCS disputes, ignoring Chinese soft power may lead policy makers to underestimate the extent to which China can influence the various actors involved and shape the situation to its advantage. That being said, while a hard power–centric counterstrategy may fall short to some degree, it would not be misdirected in this particular case. With cross-strait relations, however, a lack of attention given to Chinese soft power is likely to have more serious consequences. A hard power analysis would fail to identify an entire aspect of China's strategy—Chinese actions directed at the people of Taiwan, rather than just the politics of Taiwan.

A second set of implications concerns the growth of China's soft power. Many major powers currently have more soft power at their disposal than China does. If this differential in soft power narrows or even flips in favor of China, these states may find that their existing strategies for managing China's rise are no longer as effective. Simply put, policy makers dealing with security issues involving China will need to pay careful attention to changes in Chinese soft power and be prepared to adjust their national strategies accordingly.

As was shown here, China's security strategy leverages multiple sources of power, presenting China with many avenues to enhance its soft power. China's economic power is huge and growing; its effects are particularly pronounced in Asia. Of all the sources of power, this is the

one that policy makers are probably most cognizant of and prepared to deal with. In terms of military power, China's growth potential is significant and involves more than just sheer size. The PLA is currently engaged in a massive modernization effort under Xi's leadership, shedding much of its antiquated doctrine and organization. As the PLA takes on new missions that involve it maintaining a greater external presence, China's ability to wield soft power through its military will grow both quantitatively and qualitatively. Considering the PLA held its first-ever exercise with a foreign military only as recently as in 2002, one can only assume that its untapped potential is significant.[80] The advancement of Chinese military technology is a possible game changer. Achieving parity with the US in military technology will have considerable hard power benefits for China, but the effect on Chinese soft power could be as large, if not greater. If countries are presented with a compelling reason to consider China as their primary technology partner, they may also be encouraged to fundamentally reconsider the centrality of their security relationships with the US.

China's institutional soft power deserves added attention. Compared with economic and military heft, institutional power takes time to cultivate. As China produces ever more scientists, academics, and professionals who operate at the cutting edge of their fields, increasing numbers of these individuals will take on positions of influence in institutions around the world and even create institutions of their own. China's ability to influence the regional and global discourse on a wide range of issues will increase correspondingly. In areas like cyber and space, where international norms have yet to be settled upon, this growth in institutional soft power will be particularly valuable.

One additional aspect of China's soft power growth policy makers should watch is the evolving role of Chinese nongovernmental entities—individuals, businesses, nongovernmental organizations (NGO), and so on. Unlike with hard power, governments do not hold a monopoly on soft power. The UK's *National Security Strategy and Strategic Defence and Security Review 2015* states explicitly that "much of the UK's soft power is completely independent of government, and this is what gives it its strength."[81] A common critique of China is that it is overreliant on the government as a generator of soft power. Nye points to China's overreliance on the government as a source of soft power in the sense that "the Chinese Communist Party has not bought into the idea that

soft power springs largely from individuals, the private sector, and civil society," and instead defaults to "tools of propaganda."[82] A change in China's soft power strategy, if it were to occur, that elevates the role of nongovernmental entities could catapult China up the global soft power standings. Admittedly, there are serious structural impediments to this, one example being "the absence of Chinese NGOs on the international stage."[83] At the same time, the sheer scale of China's economic growth has inadvertently thrust some of its citizens onto the world stage. Jack Ma, the billionaire founder and executive chairman of the Alibaba Group, regularly holds court with global audiences, helping to project a softer and more appealing image of China. This serves to highlight a secondary effect that a shift toward nongovernmental soft power would have: an enhancement of informational power through the higher credibility of nongovernmental entities.

If one considers China's dynastic history as an indicator of how China might approach strategy in the modern world, the appearance of soft power in China's security strategy should come as little surprise. For 2,000 years, Chinese emperors used the diverse cultural and economic products of the "middle kingdom" as a means to maintain the Imperial Chinese tributary system across Asia. During periods of dynastic weakness, when China was unable to secure its borders against foreign invaders, the Chinese strategy was to control the invading regime from within, through the institutional influence of the mandarins. Over time, the manner in which the invaders ruled would become effectively indistinguishable from that of the Chinese rulers they had sought to displace. In a sense, soft power has long been a major part of the Chinese security strategy—as China's most famous military strategist remarked, "To win without fighting is the acme of skill."[84] A modern corollary of this can be found in the well-known PLA publication *Unrestricted Warfare*: "Spaces in nature including the ground, the seas, the air, and outer space are battlefields, but social spaces such as the military, politics, economics, culture, and the psyche are also battlefields."[85] SSQ

Notes

1. This article is based on LTC Mikail Kalimuddin's master's thesis produced while attending the US Army Command and General Staff College. Dr. David A. Anderson was his thesis chair.

2. Bessma Momani, "Xi Jinping's Davos Speech Showed the World Has Turned Upside Down," *Newsweek*, 18 January 2017, http://www.newsweek.com/davos-2017-xi-jinping-economy-globalization-protectionism-donald-trump-543993.

3. Soft power, a term coined by the American political scientist Joseph Nye in 1990, refers to sources of state power that are complementary to traditional sources of power, or "hard power." Soft power is defined as the "ability to obtain desired outcomes through attraction rather than coercion or payment." Underpinning Nye's theoretical framework is the notion that any analysis of states that limits itself to traditional sources of power is fundamentally incomplete.

4. Examples of well-established soft power indices are the Pew Research Center Global Attitude Survey, Portland's The Soft Power 30, and Monocle's Soft Power Survey.

5. Mingjiang Li, "Soft Power in Chinese Discourse: Popularity and Prospect," in *Soft Power: China's Emerging Strategy in International Politics*, ed. Mingjiang Li (Plymouth, UK: Lexington Books, 2009), 23.

6. Xuequan Mu, "Xi: China to Promote Cultural Soft Power," Xinhua, 1 January 2014, http://news.xinhuanet.com/english/china/201401/01/c_125941955.htm.

7. Joseph S. Nye, *Understanding International Conflicts: An Introduction to Theory and History*, 6th ed. (New York: Pearson Longman, 2007), 289.

8. Joseph S. Nye, "Soft Power," *Foreign Policy*, no. 80 (Autumn 1990): 168, http://www.jstor.org/stable/1148580.

9. Joseph S. Nye, *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), 5.

10. Nye, *Soft Power.*

11. *See* Sean Mirski, "The South China Sea Dispute: A Brief History," *Lawfare*, 8 June 2015, https://www.lawfareblog.com/south-china-sea-dispute-brief-history.

12. See the by-country declarations for UNCLOS listed at http://www.un.org/depts/los/convention_agreements/convention_declarations.htm. As an example, China does not accept any of the dispute resolution mechanisms provided for in the Convention.

13. Austin Ramzy, "Taiwan, after Rejecting South China Sea Decision, Sends Patrol Ship," *New York Times,* 13 July 2016, https://www.nytimes.com/2016/07/14/world/asia/south-china-sea-taiwan.html?_r=0.

14. Taiwan Affairs Office of the State Council PRC (hereafter, Taiwan Affairs Office), "Mainland, Taiwan Responsible for S. China Sea Sovereignty: Spokeswoman," 25 April 2012, http://www.gwytb.gov.cn/en/SpokespersonRemarks/201204/t20120426_2493232.htm (article removed from site by 26 February 2017).

15. For example, Japan supplied or agreed to supply the Philippines and Vietnam with maritime patrol vessels in 2016.

16. Mirski, "South China Sea Dispute."

17. Overall, China's employment of hard power in the SCS is indicative of three components in its overarching strategy: (1) aggressively asserting its claims while reshaping the status quo to its advantage, (2) countering and fragmenting opposition to its claims, and (3) pushing for resolution mechanisms that provide it with the greatest leverage.

18. Bingguo Dai, "Speech by Dai Bingguo at China-US Dialogue on South China Sea Between Chinese and US Think Tanks" (address, China-US Dialogue on South China Sea Between Chinese and US Think Tanks, Washington, DC, 5 July 2016), http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1377747.shtml.

19. Angela Doland, "Watch the Chinese Propaganda Ad Playing 120 Times a Day in Times Square," *Advertising Age*, 27 July 2016, http://adage.com/article/global-news/a-mind-numbing-chinese-propaganda-ad-playing-times-square-120-times-a-day/305198/.

20. Examples of these sites are http://english.cctv.com/special/southchinasea/ and http://www.xinhuanet.com/english/special/SouthChinaSea/index.htm, accessed 26 February 2018.

21. "The South China Sea Issue," Ministry of Foreign Affairs, the People's Republic of China, http://www.fmprc.gov.cn/nanhai/eng/, accessed 26 February 2018.

22. China Central Television (CCTV), "Animated Videos Tell You Who Stirred the Waves in the South China Sea," posted to YouTube by "Listen to me" 19 June 2016, https://www.youtube.com/watch?v=PH7sOSmyalQ.

23. Bill Hayton, "Is China Getting Better at Charming Southeast Asia on the South China Sea?," *The Diplomat,* 17 November 2016, http://thediplomat.com/2016/11/is-china-getting-better-at-charming-southeast-asia-on-the-south-china-sea/.

24. US Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2007* (Washington, DC: Office of the Secretary of Defense, 2007), http://archive.defense.gov/pubs/pdfs/070523-China-Military-Power-final.pdf.

25. Jianguo Sun, "Strengthening Regional Order in the Asia-Pacific" (speech, International Institute for Strategic Studies [IISS] Shangri-La Dialogue 2015 Fourth Plenary Session, Singapore, 30 May 2015), http://www.iiss.org/en/events/shangri-la-dialogue/archive/shangri-la-dialogue-2015-862b/plenary4-b8e3/sun-0dfc.

26. Qiang Zhou, "Work Report of the Supreme People's Court" (speech, fourth session of the 12th National People's Congress, 13 March 2016), http://www.chinacourt.org/article/detail/2016/03/id/1825026.shtml.

27. Jianguo Sun, "The Challenges of Conflict Resolution" (speech, IISS Shangri-La Dialogue 2016 Fourth Plenary Session, Singapore, 5 June 2016), http://www.iiss.org/en/events/shangri-la-dialogue/archive/shangri-la-dialogue-2016-4a4b/plenary4-6c15/jianguo-6391.

28. CUES "offers safety measures and a means to limit mutual interference, to limit uncertainty, and to facilitate communication when naval ships or naval aircraft encounter each other in an unplanned manner." Western Pacific Naval Symposium (WPNS) Secretariat, *Code for Unplanned Encounters at Sea,* WPNS report (Qing Dao, China: WPNS, 22 April 2014), 5, http://www.jag.navy.mil/distrib/instructions/CUES_2014.pdf.

29. Sun, "Strengthening Regional Order in the Asia-Pacific."

30. The State Council Information Office of the People's Republic of China, *China's Military Strategy (M*ay 2015)**,** http://www.china.org.cn/china/2015-05/26/content_35661433.htm.

31. Sun, "The Challenges of Conflict Resolution."

32. Xia Hua, "China Supports Development of ASEAN Regional Forum with Practical Actions: FM," Xinhua, 27 July 2016, http://news.xinhuanet.com/english/2016-07/27/c_135542397.htm.

33. Stratfor, "The Limits of Soft Power in the South China Sea," 18 November 2015, https://www.stratfor.com/analysis/limits-soft-power-south-china-sea.

34. Jean-Marc F. Blanchard and Fujia Lu, "Thinking Hard about Soft Power: A Review and Critique of the Literature on China and Soft Power," *Asian Perspective* 36, no. 4 (2012): 574, http://www.jstor.org/stable/42704806.

35. Sun, "The Challenges of Conflict Resolution."

36. Dai, "Strengthening Regional Order in the Asia-Pacific."

37. Dai, "Strengthening Regional Order in the Asia-Pacific."

38. Stratfor, "The Limits of Soft Power in the South China Sea."

39. Takashi Terada, "South China Sea Dispute and Institutional Balancing: ASEAN, TPP and AIIB," Doshisha University, accessed 7 November 2017, http://web.isanet.org/Web/Conferences/HKU2017-s/Archive/253b3362-6522-494b-8b8c-a4afa3b722e2.pdf.

40. Ann Marie Murphy, "Great Power Rivalries, Domestic Politics and Southeast Asian Foreign Policy: Exploring the Linkages," *Journal of Asian Security* 13, no. 3 (Special Edition 2017): 165–82, http://doi.org/ckvs.

41. Jeremy Maxie, "The Elephant in the Room: US Needs a Geo-economic Strategy for Asia, Now," *The Diplomat,* 24 February 2017, https://thediplomat.com/2017/02/the-elephant-in-the-room-us-needs-a-geo-economic-strategy-for-asia-now/.

42. The State Council Information Office of the People's Republic of China, *China's Military Strategy.*

43. The "One China Principle," under the 1992 Consensus, is that both China and Taiwan are part of a single sovereign state, but there is disagreement over which political entity is the legitimate government of this state.

44. Article eight of the Anti-Secession Law authorizes China to use non-peaceful means to prevent Taiwan's secession from China.

45. Chien-Kai Chen, "China-Taiwan Relations Through the Lens of the Interaction Between China's Association for Relations Across the Taiwan Straits and Taiwan's Straits Exchange Foundation," *East Asia* 31, no. 3 (September 2014): 226, http://doi.org/ckvt.

46. "The Great Obfuscation of One-China," *The Economist*, 11 March 2017, http://www.economist.com/news/briefing/21718499-polite-fiction-there-only-one-china-has-kept-peace-east-asiabut-now-it.

47. The Sunflower Student Movement was a protest by students and civic groups in 2014 against the establishment of a trade agreement between Taiwan and China.

48. Overall, China's employment of hard power in its handling of cross-strait relations is indicative of two components in its overarching strategy: (1) delegitimizing Taiwan as a sovereign entity through diplomatic isolation, and (2) providing the Taiwanese government with disincentives for pursuing a path towards independence.

49. Taiwan Affairs Office, "More Efforts Urged in Cross-Strait Grassroots Communication," 28 June 2014, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201406/t20140630_6427961.htm.2014 (article removed from site by 26 February 2017).

50. Min-Hua Chiang, "Tourism Development Across the Taiwan Strait," *East Asia* 29, no. 3 (September 2012): 236, http://doi.org/cktc.

51. Taiwan Affairs Office, "Chinese Mainland to Issue Electronic Travel Passes to Taiwan Visitors," 15 September 2015, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201604/t20160408 _11429457.htm (article removed from site by 26 February 2017).

52. Jason Lee, "China to Target Young of Taiwan, Hong Kong to Boost Loyalty," Reuters, 3 March 2017, http://www.reuters.com/article/us-china-parliament-taiwan-hongkong-idUSKBN16A0ZU.

53. Taiwan Affairs Office, "Student Exchanges Double in Five Years," 8 November 2015, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201604/t20160408_11429652.htm (article removed from site by 26 February 2017).

54. Taiwan Affairs Office, "Eighth Cross-Strait Forum Sees Deepened Exchange," 17 June 2016, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201606/t20160623_11490003.htm (article removed from site by 26 February 2017).

55. Rui Zhang, "Chinese Mainland to Issue Preferential Policies for Taiwan Compatriots," CCTV.com, 2 September 2017, http://english.cctv.com/2017/02/09/ARTI4xXaowdbbQcchJdL0Htb170209.shtml. As of 2016, there are an estimated one million expatriate Taiwanese living in China.

56. Taiwan Affairs Office, "201 Taiwanese Qualified to Practice Law on Mainland," 25 September 2013, http://www.gwytb.gov.cn/en/SpokespersonRemarks/201309/t20130926_4938025.htm (article removed from site by 26 February 2017).

57. Taiwan Affairs Office, "Association Established to Serve Cross-Strait Couples," 28 August 2012, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201208/t20120829_3003246.htm (article removed from site by 26 February 2017).

58. Taiwan Affairs Office, "Mainland Welcomes all Taiwan Compatriots," 28 February 2014, http://www.gwytb.gov.cn/en/SpokespersonRemarks/201402/t20140228_5749151.htm (article removed from site by 26 February 2017).

59. "Xi-Ma Meeting: Transcript of China President Xi Jinping's Opening Remarks," *Today*, 7 November 2015, http://www. todayonline.com/singapore/transcript-china-president-xi-jinpings-speech-he-meets-taiwans-ma-jing-yeou.

60. "Xi-Ma Meeting."

61. Taiwan Affairs Office, "Mainland, Taiwan Responsible."

62. Taiwan Affairs Office, "Chinese Mainland, Taiwan to Hold Joint Forum on Sun Yat-Sen," 15 December 2011, http://www.gwytb.gov.cn/en/SpokespersonRemarks/201103/t20110316_1788618.htm (article removed from site by 26 February 2017).

63. Taiwan Affairs Office, "Commemoration of WWII Victory Promotes Cross-Strait Relations," 3 September 2015, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201604/t20160408_11429435.htm (article removed from site by 26 February 2017).

64. Christopher M. Dent, "Taiwan and the New Regional Political Economy of East Asia," *China Quarterly* 182 (June 2005): 400, http://doi.org/c5vnd9.

65. Min-Hua Chiang, "Cross-Strait Economic Integration in the Regional Political Economy," *International Journal of China Studies* 2, no. 3 (December 2011): 682, https://www.researchgate.net/publication/290573687_Cross-strait_economic_integration_in_the_regional_political_economy.

66. Straits Exchange Foundation, "Taiwan and Mainland Launch Preferential Customs Clearance Program," 1 October 2016, http://www.sef.org.tw/fp.asp?xItem=1010713&ctNode=4633&mp=300.

67. "China's Bottom Line," *The Economist*, 17 March 2015, http://www.economist.com/news/china/21646571-chinese-leaders-send-warnings-taiwans-opposition-party-ahead-elections-next-year-chinas-bottom.

68. Taiwan Affairs Office, "Chinese Mainland Island Seeks Taiwan Professionals," 14 February 2012, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201202/t20120215_2292610.htm (article removed from site by 26 February 2017).

69. Taiwan Affairs Office, "Mainland, Taiwan Acknowledge Progress of Cross-Strait Talk," 30 November 2015, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201604/t20160408_11429690.htm (article removed from site by 26 February 2017).

70. Taiwan Affairs Office, "6 Taiwan Banks Approved to Open Mainland Branches: Spokesman," 29 December 2010, http://www.gwytb.gov.cn/en/SpokespersonRemarks/201103/t20110316_1788623.htm (article removed from site by 26 February 2017).

71. Taiwan Affairs Office, "Mainland, Taiwan to Strengthen Hi-Tech Cooperation," 21 November 2012, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201211/t20121123_3386684.htm (article removed from site by 26 February 2017).

72. Taiwan Affairs Office, "Mainland Spokesman on ARATS, SEF Establishing Cross-Strait Offices," 16 January 2013, http://www.gwytb.gov.cn/en/SpokespersonRemarks/201301/t20130117_3554951.htm (article removed from site by 26 February 2017).

73. Taiwan Affairs Office, "Chinese Mainland to Strengthen Protection of Taiwanese Rights, Interests," 12 January 2011, http://www.gwytb.gov.cn/en/SpokespersonRemarks/201103/t20110316_1788626.htm (article removed from site by 26 February 2017).

74. Taiwan Affairs Office, "Mainland Opens Office to Handle Taiwan-Related Petitions," 15 August 2014, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201408/t20140819_7026283.htm (article removed from site by 26 February 2017).

75. Taiwan Affairs Office, "Mainland Sends Disaster-Relief Fund to Taiwan," 17 June 2012, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201206/t20120618_2749193.htm (article removed from site by 26 February 2017).

76. Taiwan Affairs Office, "Mainland Helping Taiwanese in Nepal," 29 April 2015, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201505/t20150514_9801140.htm (article removed from site by 26 February 2017).

77. Taiwan Affairs Office, "Mainland, Taiwan Jointly Bust Human-Trafficking Rings," 6 August 2012, http://www.gwytb.gov.cn/en/CrossstraitInteractionsandExchanges/201208/t20120809_2896898.htm (article removed from site by 26 February 2017).

78. Jing Sun, *Japan and China as Charm Rivals: Soft Power in Regional Diplomacy* (Ann Arbor, MI: University of Michigan Press, 2012), 124.

79. Sun, *Japan and China*, 128.

80. John W. Garver, "China's Influence in Central and South Asia," in *Power Shift: China and Asia's New Dynamics*, ed. David Shambaugh (Berkeley, CA: University of California Press, 2005), 213.

81. HM Government, *National Security Strategy and Strategic Defence and Security Review 2015* (London: UK Government, 2015), 49, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

82. Joseph S. Nye, "The Limits of Chinese Soft Power," Project Syndicate, 10 July 2015, https://www.project-syndicate.org/commentary/china-civil-society-nationalism-soft-power-by-joseph-s--nye-2015-07?barrier= accessreg.

83. Yiyi Lu, "Blind Spots in China's Soft Power," *The Straits Times*, 15 July 2007.

84. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 77.

85. Liang Qiao and Xiangsui Wang, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House Arts, 1999), 206.

Book Reviews

The China Questions: Critical Insights into a Rising Power, ed. Jennifer Rudolph and Michael Szonyi. Harvard University Press, 2018, 352 pp.

The China Questions is a compilation of 36 essays from academics affiliated with the Fairbank Center for Chinese Studies at Harvard University. Premised on the idea that "China matters, and therefore that understanding China matters" (p. 1), the editors, Jennifer Rudolph and Michael Szonyi, invited experts to pick a question Americans should ask about China and then provide a short, insightful answer. In organizing these answers, the book is divided into discussions of politics, international relations, economy, environment, and society as well as history and culture. Throughout each section, it is the intention of the authors to cumulatively show how China's past informs the present and how the present shapes the future. To this end, it is the hope of the editors that they will be able to lessen the "understanding deficit" America has with China.

Within the politics and international relations sections the authors ponder such questions as "Does Mao Still Matter?," discussing the continued influence of the Chinese Communist Party (CCP) founder Mao Zedong, especially as it relates to the rule of Xi Jinping and his desire to upend precedent and remove term limits from the office of the presidency. Also considered is the perennial question of Chinese Communism's legitimacy, which explores why the party continues to be viewed as legitimate by the Chinese people. Elizabeth Perry explores the idea that the CCP is reliant on its performance for legitimacy but is rapidly trying to transition to historical legitimacy to justify its rule in preparation for uncertain times. However, as the CCP looks to the past, it also inadvertently opens the door for criticism of Mao Zedong's policies such as the Anti-Rightist Campaigns, the Great Leap Forward, and the Cultural Revolution. To prevent undesirable narratives from undermining the CCP's efforts, in 2013 the party outlined the seven "speak-nots" (areas of liberal governance that might challenge CCP rule) including "historical nihilism," which Joseph Fewsmith describes as any historical writings or research that "conflicts with the Party's approved historiography" (p. 22). The urgency of the question of legitimacy gains increased relevance when, in a separate essay, Yuhua Wang asks what the CCP can learn from the various Chinese emperors' rise and fall. Wang's findings are disconcerting for the CCP as on average a Chinese dynasty lasted only 70 years, an age the CCP will reach in 2019, and were predominantly overthrown by societal elites and not external military powers.

With respect to the question of how strong the Chinese armed forces are, Andrew Erikson projects that despite China's near-term progress in developing and fielding military tech capable of targeting US vulnerabilities in the Yellow, East China, and South China Seas, propulsion, electronics, and other complex system-of-systems technologies will remain a key Chinese weakness. Furthermore, Erikson expects that the development of cutting-edge technology and mounting personnel costs, particularly with regard to supporting its growing retiree population, will place an increasing budgetary burden on the Chinese government and economy.

In asking if China's high growth will continue, Richard Cooper anticipates that the economy's rate of growth will likely begin to slow in the coming decade as many of the factors that previously bolstered growth rates above 10 percent diminish, potentially dropping to as low as 5 percent if China cannot spur innovation and further benefit from technological improvements. However, Dwight Perkins contends that while growth may be slowing, he sees little indication that the Chinese economy is in for a recession. Instead he suggests that the real danger to the Chinese economy is that continued low household consumption rates will be unable to offset the aggregate decrease in demand as China continues to taper off its massive national infrastruc-

ture and building projects. Perkins also points out that this excess production capacity, especially within the steel industry, has already resulted in anti-dumping actions in North America and Europe, making it unlikely that those markets will be willing to absorb additional capacity. Furthermore, in a study of urbanization in China, Meg Rithmire concludes that without significant reforms to the Chinese household registration (*hukou*) and land rights systems, China will be unable to successfully manage the rural-to-urban migration necessary to maintain a successful economy. While the outlook may look bleak, Nara Dillon is optimistic that China is capable of making the kind of data-driven developmental and welfare reforms appropriate to maintain the strong economy necessary for Xi Jinping to meet his goal of eliminating extreme poverty in China.

While the politics, international relations, and economy sections provide a relatively simplified, if not well trodden and direct, description of a complex and adaptive country, the essays on society, history, and culture that make up the second half of the book cover a much more varied and disjointed set of topics.

Through their writings on Confucius, religion, propaganda, education, law, and literature the authors try to delineate the boundaries and critical events that shape Chinese thinking and society. Of note is Paul Cohen's closing piece in which he catalogs several of the technological, political, and sociocultural factors which have changed the study of China over the years. Cohen describes how the open door policy of the 1970s combined with the growth of the internet and Chinese scholars' increasing willingness to study a broader array of questions have created a clearer picture of China—although, in the preceding piece, Stephen Owen cautions that while this picture may be clearer, we must always remain aware that the goals of Chinese scholarship are not the same as those of Western scholarship. Harkening back to the discussion of the seven speak-nots, he alludes to the chilling effect government censorship and official historiography have on critical scholarship, writing that a scholar's task is to secure "greater detail in the history of the people, and not to ask questions about it" (p. 285).

On a more critical note, as a book published in 2018 and purportedly focused on questions Americans should ask about China, it remains almost completely silent on China's continued support of North Korea and China's desired end state on the peninsula. This notable absence is possibly remedied by the inclusion of an extensive further reading list assembled by the authors and hosted on the Fairbank Center's website (http://fairbank.fas.harvard.edu/china_questions/). However, relying on the reader to seek out, identify, and decipher the scholarly material on such a critical matter misses the point of the book.

Overall, *China Questions* is a worthwhile read, and its short essays are perfect primers for quickly exposing the complexity of a specific subject without dwelling too deeply on the details. The individual essays may lack the depth and nuance of a published paper, but their ease of understanding opens the subject up to the uninitiated and encourages further research. I recommend this book as a starting place for anyone wanting to gain insight into the political, economic, social, and historical drivers shaping Chinese thinking and requiring solid ground from which to start.

Capt Sean E. Thompson, USAF

An Untaken Road: Strategy, Technology, and the Hidden History of America's Mobile ICBMs by Steven A. Pomeroy. Naval Institute Press, 2016, 304 pp.

The emerging field of Cold War history receives a new addition with *An Untaken Road,* an account of mobile intercontinental ballistic missiles (ICBM) in America. Steve Pomeroy, a history professor and former missileer himself, delves into one of least known areas of America's nuclear weapons history as he explores the Air Force's efforts to mobilize its ICBMs.

Pomeroy uses established historical theory of technological development to enlighten the reader as to how mobile ICBMs came about—and ultimately failed—in the context of the Cold War. Employing a modified version of historian Thomas Hughes's five-phase model of technological innovation, he shows how each succeeding mobile missile program ultimately did not garner the momentum required to become operational. Putting his subject in the context of the evolving politics of the time, Pomeroy makes a convincing case for why there are no trains with ICBMs currently traveling the railroads of the West.

An Untaken Road follows the early development and limitations of ICBMs—limitations that made static basing difficult (never mind the idea of moving them around). From here the divergence is well documented regarding how static ICBMs became the weapon of choice and various mobile options showed great promise but never achieved stability as programs. The author effectively uses his formal training as a historian to explain the shortcomings of rail-mobile, large-plane, superhard-shelter, and pool basing (even an underground tube-tunnel basing concept); he also documents why these approaches found sufficient favor to justify research but never enough to be deployed. Each proposal reached one of the stages of development but failed to proceed to the all-important final stage of stability—a status that would grant it funding and operational implementation.

The book facilitates a strong understanding of how military procurement works and thus influences today's multi-billion-dollar projects. The paradigm that Pomeroy generates is one of coalescing crucial factors at the right time to breathe life into a program. Many of the systems he describes were prototyped and tested but always lacked a key element to make them viable. So often political support was present, but the technology was not—or the technology was mature, but the driving Air Force leadership necessary to deploy a system failed to emerge. The text makes a strong argument that if a system of systems is to work, an entirely separate military-industrial-political system must be functioning efficiently.

Although written as a history, this study offers a lesson to current procurement teams. Its underlying theme is stability, and thus it rightly shines a bright light on Gen Bernard Schriever, the man responsible for the ICBM force. His systems approach to problems and dual focus on disruptive and sustaining innovations set the standard—one that slowly relaxed after his retirement. By contrasting the successful development and deployment of three ground-based ICBM systems with the repeated failures of mobile systems, *An Untaken Road* puts a stark spotlight on the degrading quality of systems engineering in military procurements. Without question, this is a book for any member of a program office.

By learning from our history, so well documented by Professor Pomeroy, we as a nation and military-industrial complex can make better decisions. The procurements he describes were often larger than those for the fighter jets, satellites, and ships we purchase today, and they suffered from the same shifting political tides and needs of the Department of Defense—so the lessons remain pertinent. We would do well to apply the book's paradigm of technological development and determine whether the big-ticket items we are buying today are still worth the cost. Too many times, historians admonish leaders for not learning the lessons of history and for repeating failures, but in this case the accusations are true. We can act on these lessons and apply them to things we do every day.

To make these arguments, the book uses open-source documentation on the political and public debates, as well as a wealth of newly declassified data, clearly showing why each proposal failed to gain the needed momentum. Pomeroy provides copious notes, although most of the technical details of these wondrous projects are from primary sources available only in archives.

Regrettably, the text contains only a fraction of the presentation slides and available pictures of the considered options for mobile basing. One of the areas for future research could involve

more indulgence in the technological aspects and a more detailed description of the massive ICBM carriers that never materialized. Some of the planes and tunnel-based ideas that Pomeroy describes deserve their own treatments, just to illustrate how bold and complex were the concepts that the Air Force seriously considered.

An Untaken Road establishes a solid foundation for the study of the service's truncated ICBM efforts, a subject that deserves more recognition than it receives because of its failings. The proposals and programs described all came to nothing because of inherent issues with their ability to advance through the developmental phases needed to sustain a program. Today's procurements are no different in terms of their cost and national security implications, making the book's lessons learned critical to the decision making of any officer tasked with procuring a new system.

Daniel Schwabe
Whittier, California

Understanding Cyber Conflict: 14 Analogies ed. George Perkovich and Ariel E. Levite. Georgetown University Press, 2017, 296 pp.

Recent cyber works frequently focus on uncovering new theories and observing technical developments, but George Perkovich and Ariel E. Levite follow a different path to better assimilate previously fielded material. The editors gathered 14 articles comparing cyber strategies to historic military events or developments such as Pearl Harbor, air defense, or drone warfare in an effort to inform those less familiar with cyberspace. This work owes credit to a 2014 Department of Defense–commissioned volume, *Cyber Analogies*, which aimed to assist US Cyber Command in educating senior leaders. Gathering all the conflict analogies together under a single cover is a novel concept and achieves their stated goal of stimulating discussion. Levite and Perkovich split their compilation into three sections: examining what cyber weapons are like, how a cyber war may appear, and how one would manage a cyber conflict. The book informs and educates the reader through using the 14 analogies to create new comparisons and pose questions about future paths.

The central goal emerges from earlier research suggesting human beings use analogies to communicate, especially for more complicated topics. The more complicated the topic, the more humans simplify the concepts through relating individual items to other structures. A common popular example is Aesop's fables, using the tortoise and the hare to illustrate a complicated thought process. Complicated ideas are initially simplified through analogy. As a technical example, an analogy common to many intelligence professionals is that of the "black swan" as proposed by Nicolas Taleb. Black swans did not appear in Europe, and so calling something a black swan indicated an impossibility, since all swans were white. However, black swans are common in Australia, so the analogy as related by Taleb really identifies not something impossible but one which has not occurred yet. The authors chosen by Perkovich and Levite all use similar but different examples to explain how cyber events could be understood or evaluated from a slightly different context.

The cyber weapons section investigates how digital munitions may appear in a future context. Four analogies were presented: intelligence, nonlethal weapons, precision-guided munitions (PGM), and drones. Although each was informative, especially for those new to cyber, none were significantly different than other cyber-focused works. In the information domain, intelligence approaches have appeared in multiple venues. Many writers have also discussed cyber's nonlethal aspects as the only two confirmed, physically destructive events being the 2008 Turkish pipeline incident and Stuxnet. The PGM article does advocate for either compellence or denial strategies against the broader target rather than looking for cyber panacea targets to avoid the mistakes of WWII's European air war. In discussing drones, the article highlights four areas where cyber differs from drones—worth noting as the same four capabilities are mentioned in several other chapters. Those drone to cyber effects are reversibility,

non-lethality, ability to strike repeatedly, and deniability. While none of this section's chapters offers unique analogies, all successfully explain a possible visualization of cyber effects.

The book's middle section includes five chapters that contemplate how cyber wars reveal themselves. The two most interesting chapters are the middle two, emphasizing technological development and economic warfare. Chapter seven, "Crisis Instability and Preemption," explores a comparison between cyber and railroad developments, circa 1914, as facilitating technologies. The unique attributes for rail are listed as open, linear, and fixed, while cyber is covert, flexible, and adaptable. Exploring how railroad technology developments shaped state strategy offers a valid perspective to cyber impacts as the two technologies encourage globalization through compressing time and space. Railroad technology shows a visible interdependent channel where cyber now creates the same connection except without any impact on the physical domain. The discussion suggests a perception of how technology affects warfare without reverting back to the popular 1990s concepts based on Revolution in Military Affairs theories.

The next excellent chapter was "Brits-Krieg," by Nicholas Lambert, discussing how England prepared strategies for economic warfare with Germany prior to World War I. The content walks through the development of international financial markets prior to the war while suggesting England's three strengths were its navy, intelligence gathering, and economy. States attempting to wage economic warfare relied on two vulnerable areas to create effective strategies: impacting the market system and understanding how politically aware industrial societies depend on smooth functioning system. The British, in Lambert's explanation, attempted to disrupt global communications (telegraph) to influence markets, and a wider impact could be achieved through modern cyber weapons. One can see smooth functioning system impacts in the Russian cyberattacks on Georgia (circa 2008), when disruptions to networks created secondary impacts in the cellular phone system and tertiary impacts to financial transactions like bill payment through those interdependent systems. (One reason I enjoyed this chapter was it strongly correlated with my own recent work, *Cashing In on Cyberpower* [2018], about how state and nonstate actors use cyber means to create economic effects.) Overall, several economic strategy questions for cyberspace employment are presented to suggest distinguishing public from private cyberspace, understanding interdependent data flows, and insulating collateral damage through the Global Cyber Commons. Any effective economic strategy considering cyber means should address the suggested questions before moving forward.

The final section, on managing cyber conflict, discusses shifting the primary WWII cyber analogy from Pearl Harbor to Harbor Lights. Harbor Lights references 1942 German attacks against shipping on the US's east coast. During the first three months of 1942, German submarines sank 2.5 million tons of shipping, 50 percent of the previous two years' raiding, largely because coastal cities refused to dim any lights at night. In the spring, President Franklin D. Roosevelt ordered a full coastal blackout extending miles inland, reducing attacks 73 percent in three months. The analogy suggests a comparison to those corporate agencies that fail to invest in proper security. Instead of Pearl Harbor as a single devastating event, extended commercial vulnerabilities will likely be more challenging in cyberspace. For example, when a nation-state can pillage intellectual property and hold infrastructure at risk, at what point should those private corporations' cybersecurity become a mandated matter for public involvement?

Overall, each of the 14 analogies provided some useful comparison between a noncyber domain event and a cyberspace consideration. Some of the analogies cover previously suggested comparisons, while others found new interactions to consider. Although suggested as a tool for the senior strategist, the book would serve best for those in an initial to intermediate standing regarding their cyberspace knowledge. The first two sections about cyber weapons and recognizing cyber conflict fit nicely into those company-grade roles, while the last section on managing cyber conflict addresses more field-grade concerns. *Understanding Cyber Conflict* nicely fills a gap between publicly accessible cyber considerations like Shane Harris's *@ War*

and more technical volumes such as Brandon Valeriano and Ryan C. Maness' *Cyber War versus Cyber Realities*. Reading this informative volume will definitely help the reader explore some existing perspectives and should stimulate new insights.

Lt Col Mark Peters, USAF

Russia's Dead End: An Insider's Testimony by Andrei A. Kovalev. Potomac Books, 2017, 247 pp.

A popular television documentary series follows several gold miners sifting through massive dirt and stone piles to find occasional gold. Similarly, *Russia's Dead End* delivers much generic Russian information with only the occasional insight into author Andrei Kovalev's individual experiences. The front cover and flap suggest Kovalev's work provides perceptive insights based on his long associations with Soviet and Russian regimes. Unique and perceptive insights are present, but the linkages to his own personal experiences are underdelivered. However, some remarkable Russian policy insight emerges, like the aforementioned gold nuggets, from unusual places. Kovalev superbly covers various challenges faced by post-Soviet society, exploring their historical basis and discussing future manifestations. He also analyzes why Russia's democratic reforms failed to take root.

Russia's Dead End argues transitioning from the Soviet Union to the Russian Republic offered the Russian people seeds of opportunity to become a great democratic republic. However, at every turn this growth was poisoned, sometimes literally, by active efforts from former KGB agents, the Russian people's nature, and outright paranoia. Chapter by chapter the book portrays different aspect of Russia's journey from the USSR's democratic steps under Gorbachev and subsequent coup, to the Russian people's challenges after those initial transitions, and then to how the KGB flourished as the new *Federalnaya Sluzhba Bezopasnosti* (Federal Security Service or FSB) in actively denying any further transitions. This central theme explains where the FSB motivation and control sparked Russia's revanchist strategic leanings and subsequent oppression of their populace. A revanchist strategy, first appearing in mid-nineteenth century France as derivative of the French verb *revenchier (revenge)*, expresses a return to previous national boundaries, particularly those lost to either war or diplomacy. Kovalev theorizes the FSB plan indicates a desire to return to Russia's historical boundaries as well as leadership practices espoused under Lenin and Stalin, except with more financial benefits for their hierarchy.

The USSR's transition from communism to democracy began as Kovalev worked for Gorbachev's Ministry of Foreign Affairs, and not surprisingly, the author sees that ministry, and his work therein, as a center for democratic reform. Kovalev's father, Anatoly Kovalev, was also heavily involved as the first deputy for Gorbachev's minister of foreign affairs, Eduard Shevardnadze. This division shaped the Final Act that clarified human rights conventions for the Helsinki Conference on Security and Cooperation in Europe through reforming criminal activity legislation in the criminal code of the Russian Soviet Federated Socialist Republic. The criminal code covered state use of punitive psychiatry that supposedly prevented felons from causing any further damage to the state. These punitive psychiatry practices, mandatory drug treatments, and involuntary hospitalization, thought discarded with the USSR's end, appear later with the FSB's recycled strategies. Much of the book continues in the same approach, moving rapidly between topics, lacking a consistent internal chapter timeline, and suggesting a shocking revelation about now-implemented antidemocratic practices. As an example of timeline difficulties, the first chapter ends with the completion of the August 1991 coup and the admission of Latvia, Estonia, and Lithuania to the Committee of European Foreign Ministers as independent countries, while the second returns to only cover previously completed coup events.

Chapters 3 and 4 next share the same 10-year period in exploring transitions to an almost democratic institution including how those organizations functioned until Vladimir Putin's 1999 election. Once Gorbachev left power, Russia's population expected a faster democratic transition and more immediate material payoffs than the government apparatus was equipped to handle. The text suggests supporting these payoffs to gain popular support resulted in a symbiosis of government, criminal, and business interests that each followed their own material interests while excluding all others, effectively abdicating national responsibilities once their gold was in hand. Kovalev suggests the high-level players used former Russian communist connections to KGB interests and individuals, such as Putin, as the basis for their success. The author even proposes Putin's most democratic recorded experience, working with the St. Petersburg mayor, was a KGB plot to bring about the mayor's downfall (p. 186). However, continued struggles with economic, environmental, and Islamic fundamentalist challenges demonstrate internal and external causes that helped prevent any democratic transition. The corruption endemic to the system, the personal politics required for even minor success, and the state agencies actions against their people's best interests caused these failures throughout Russia—but only because they were guided by the FSB.

Chapters 5, 6, and 7 move the remainder of the excess dirt away from Kovalev's core thesis, revealing where he believes the FSB now effectively controls Russia. The section begins with a reported Putin quote after his presidential appointment, "Order Number One for the complete seizure of power has been fulfilled. A group of FSB officers has successfully infiltrated the government" (p. 173). Unfortunately, like other controversial elements Kovalev espouses from several, apparently Russian sources, the text does not provide locations to confirm the material. The quote certainly makes one believe the FSB controls Russia, but outside confirmation remains important. FSB traditional practices, derived from the KGB, are suggested throughout and used for population control, to arrest or kill journalists challenging the state, and as a basis for Russia's imperialist military campaigns in Georgia, Crimea, and the Ukraine. Each item explores what occurred and where FSB influences were involved.

Overall, Andrei Kovalev offers a comprehensive, historical look at where Russian democratic transitions fail after the Cold War's end. From a national security perspective, he offers a chilling hypothesis for where the KGB-associated elements in the FSB are still running the Russian state. If his hypothesis proves true, those motivational changes could alter the decision calculus for any US or other policy makers hoping to interact with Russia democratically. However, other than Kovalev's personal claims, the details and the sourcing provided are simply insufficient to support similar conclusions. One cannot help comparing Kovalev's work to other KGB analysis and demonstrated sources, namely *The Sword and the Shield* and *The World was Going our Way*, which explore Cold War KGB practices using the Vasili Mitrokhin archive and Mitrokhin's personal testimony as the more useful evidence standard. Without solid background documentation, or at least endnotes, sifting through the surrounding material for an actual glimmer proves difficult. I found the book interesting but think a solid, detailed background in Russian affairs would prove extremely helpful prior to reading. Certainly not for the general public, and not as nugget filled as one might hope from an insider's testimony, *Russia's Dead End* offers an unusual look at cause and effect for that nations's problems over the past 30 years.

Lt Col Mark Peters, USAF

Mission Statement

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

Disclaimer

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

Comments and Contact

Send your comments, suggestions, or address change to:
StrategicStudiesQuarterly@us.af.mil.

Join the debate and like us on Facebook.com/AirUnivPress.

Follow us on Twitter.com/AirUnivPress.

Article Submission

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

Strategic Studies Quarterly (SSQ)
600 Chennault Circle, Building 1405, Room 143
Maxwell AFB, AL 36112–6026
Tel (334) 953–7311

Strategic Studies Quarterly online: **http://www.airuniversity.af.mil/ssq/**

Free Electronic Subscription

Strategic Studies Quarterly (*SSQ*) (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL.

A forum for critically examining, informing, and debating national and international security

"Aim High... Fly-Fight-Win"

http://www.airuniversity.af.mil/SSQ/