JULY 2019

A REPORT
OF THE CSIS
INTERNATIONAL
SECURITY
PROGRAM

BY OTHER MEANS

PART I: CAMPAIGNING IN THE GRAY ZONE

PROJECT DIRECTORS

Kathleen H. Hicks

Alice Hunt Friend

AUTHORS

Kathleen H. Hicks

Alice Hunt Friend

Joseph Federici

Hijab Shah

Megan Donahoe

Matthew Conklin

Asya Akca

Michael Matlaga

Lindsey Sheppard

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JULY 2019

A REPORT
OF THE CSIS
INTERNATIONAL
SECURITY
PROGRAM

BY OTHER MEANS

PART I: CAMPAIGNING IN THE GRAY ZONE

PROJECT DIRECTORS

Kathleen H. Hicks

Alice Hunt Friend

AUTHORS

Kathleen H. Hicks

Alice Hunt Friend

Joseph Federici

Hijab Shah

Megan Donahoe

Matthew Conklin

Asya Akca

Michael Matlaga

Lindsey Sheppard

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

About CSIS

Established in Washington, D.C., over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For the past eight years consecutively, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

ISBN: 978-1-4422-8118-9 (pb); 978-1-4422-8119-6 (eBook)

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com

Contents

Acknowledgments

The authors are grateful to Melissa Dalton, John Schaus, Seth Jones, Todd Harrison, and Suzanne Spaulding for their insights and feedback throughout the project. We would also like to thank Lorris Beverelli for his research contributions, as well as Rebecka Shirazi and Jeeah Lee for managing the publication process. Finally, the study team is indebted to those who took part in our working group discussions and senior leader dinner. Your insights and contributions were invaluable.

This report is made possible by the generous support from the Smith Richardson Foundation.

The content and recommendations presented, including any errors, are solely those of the authors.

BY OTHER MEANS

PART I: CAMPAIGN IN THE GRAY ZONE

The United States is being confronted with the liabilities of its strength. Competitors are contesting the rules of the international system and U.S. leadership. With the significant costs of engaging the United States in combat, and the growing range of indirect and non-military tools at their disposal, rivals are finding avenues for threatening U.S. interests without triggering escalation. Their coercive tools range the spectrum of fake news and online troll farms to terrorist financing and paramilitary provocations. Such approaches lie in the contested arena somewhere between routine statecraft and open warfare—the "gray zone."

Gray-Zone Challengers

Four countries conduct the lion's share of state-based gray-zone operations against the United States, its interests, and its allies and partners:

1. China
2. Russia
3. Iran
4. North Korea

Of these actors, China is the most concerning, followed by Russia, given the breadth and quality of each state's toolkit and their relative potential effects on U.S. interests.

The Gray Zone Toolkit

These challengers primarily use the following coercive tools in their gray zone toolkits:

1. Information operations and disinformation
2. Political coercion
3. Economic coercion
4. Cyber operations
5. Space operations
6. Proxy support
7. Provocation by state-controlled forces

Countering the Gray Zone Challenge: **Mission Objectives**

A dynamic campaign approach can drive competitive U.S. strategy in the face of gray zone challenges. The plan must incorporate the following mission objectives:

1. Gain advantages in gray zone competition that bolster U.S. national security interests.
2. Undermine competitors' tactics, from deterrence to effective campaigning to crisis response.

Principles and Priorities

Even as the United States campaigns in the gray zone, it should do so in accordance with its principles. U.S. laws and values are fundamentally strategic advantages in the competitions the country faces.

Campaign planning should focus on three priority lines of effort, defined by U.S. vital interests.

1. Protect U.S. constitutional tenets and the U.S. way of life;
2. Promote the nation's economic vitality; and
3. Advance U.S. influence

INTEGRATED FINDINGS AND RECOMMENDATIONS

The following imperatives be among those that shape the U.S. government's campaign plan for the gray zone:

Outpace Competitor Intelligence Capabilities

- Develop an intelligence-based understanding of foreign actors' motivations, psychologies, and societal and geopolitical contexts
- Maintain necessary inputs for innovation
- Deploy iterative feedback mechanisms for policymakers to keep up with competitors
- Leverage artificial intelligence to identify patterns and infer competitors' intent

Build and Synchronize Employment of Multidimensional U.S. Power

- Diversify strategic focus across public and private sectors in both domestic- and foreign-facing arenas
- Expedite decisionmaking processes to gain a critical advantage before and during crises
- Clearly signal foreign policy to facilitate assurance and deterrence and promote dialogue and de-escalation

Deploy Information and Narrative-Building in Service of Statecraft

- Promote a narrative of transparency, truthfulness, liberal values, and democracy
- Implement a compelling narrative via effective mechanisms of communication
- Continually reassess U.S. messages, mechanisms, and audiences over time
- Counteract efforts to manipulate media, undermine free markets, and suppress political freedoms via public diplomacy

Match Punitive Tools with Third Party Inducements

- Revitalize the Department of State to promote diplomacy
- Strengthen alliances
- Bring private sector and civil society into accord on U.S. interests
- Attract U.S. business and potential partners overseas using positive tools of economic statecraft

Develop Robust Anticipatory Repertoires of Conduct for Cyber Operations

- Establish a set of norms for cyber policy that accounts for the domain's evolving complexity
- Create a code of conduct for both offensive and defensive operations to avoid ad hoc decisionmaking
- Ensure that U.S. government authorities, policies, and organizations keep pace with rapidly evolving cyber capabilities

1 INTRODUCTION

The United States and its allies are being confronted with the liabilities of their strengths. Because U.S. supremacy at the conventional and strategic levels of military conflict remains unsurpassed, and the U.S.-led international state system still structures global diplomacy, law, and commerce, competitors are using alternative approaches to achieve their aims. Such approaches are somewhere between routine statecraft and open warfare. Some scholars and practitioners refer to this contested arena between peace and war as the "gray zone."[1]

The United States and its allies are being confronted with the liabilities of their strengths.

A range of actors are using gray zone approaches to achieve their strategic ends. Most worrisome for the United States are the actions of China and Russia, nuclear-armed competitors with the potential to substantially escalate violence.[2] To extend its regional dominance, China dredged the ocean floor and created artificial islands for use as military bases, asserting de facto, extra-legal control over the South China Sea.[3] To subvert post-Cold War transatlantic security, Russia engages in disinformation campaigns over social media platforms, sowing political and social division in rival states.[4] These are merely examples of some of the gray zone methods each employs.

The gray zone actions of Iran and North Korea also merit attention. Iran is determined to destabilize the Middle East to its own benefit and does so through the use of plausibly deniable proxy forces in countries including but not limited to Lebanon, Syria, and Iraq.[5] To ensure the continued dominance of the Kim family over domestic politics, the regime in North Korea has shown a willingness to conduct damaging cyber operations.[6]

Such tactics have galvanized significant attention from the U.S. public and political and military leadership. Both the 2017 National Security Strategy and 2018 National Defense Strategy call attention to the challenge set:

> *In addition, adversaries and competitors became adept at operating below the threshold of open military conflict and at the edges of international law . . . Such actions are calculated to achieve maximum effect without provoking a direct military response from the United States. And as these incremental gains are realized, over time, a new status quo emerges.*
>
> *-National Security Strategy, 27–28*
>
> *Both revisionist powers and rogue regimes are competing across all dimensions of power. They have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals.*
>
> *- National Defense Strategy, 2*

Adversaries' use of gray zone tactics has contributed to regional instability and a "weakening [of the] post-WWII international order."[7] Washington's failure to adapt has allowed competitors to exploit the order's benefits while undercutting its principles and rules.[8] Despite this high-level recognition of the gray zone challenge, U.S. policymakers have yet to articulate a comprehensive approach.

A concrete and actionable campaign plan is needed to deal with the gray zone challenge. Such a plan should: (1) develop a clear assessment of the global threats and opportunities posed by gray zone activities, (2) lay out specific actions the United States should take to compete in the gray zone when necessary, and (3) ultimately deter adversaries from using gray zone tactics.

Previous analyses have typically focused on individual challengers, such as China, Russia, or Iran, or particular functional challenges, such as paramilitary approaches or disinformation. Far less analysis exists to assess how the United States can more systematically address this broad challenge set. If the United States is to engage seriously in gray zone competition, it will need to identify and employ a broad spectrum of its considerable national power. It is time to identify the needed tools and concepts for their integrated employment—a campaign plan—that U.S. policymakers could use to deter and, if needed, to compete and win contestations in the gray zone.

Washington's failure to adapt [to gray zone approaches] has allowed competitors to exploit the order's benefits while undercutting its principles and rules.

DEFINITIONS

The CSIS study team has elected to represent the full scope of its inquiry in its use of the term "gray zone." National security practitioners, diplomats, military leaders, allies, and academics have used a host of terms to describe all or parts of the challenge set that exist below the threshold of conventional military conflict. A partial list of such terms includes irregular warfare, soft power and sharp power, hybrid warfare, active measures, political warfare, competition, strategic competition, and gray area or gray zone approaches.[9]

The lack of consensus around terminology is unsurprising: The strategies and operations present in the space between peace and war are intentionally ambiguous, meant to defy easy categorization and therefore also effective responses. Preferred terminology is ultimately a secondary issue, however, and extended labeling debates can delay needed action. Regardless of the lexicon, a growing body of work describes a similar set of phenomena, including the following:

"[A] deliberate policy choice to undermine a rival or achieve other explicitly political objectives by means other than routine diplomacy or all-out war" that "consists of the intentional use of one or more of the implements of power (diplomatic, information, military, and economic) to affect the political composition or decision-making within a state. Political warfare is often—but not necessarily—carried out covertly but must be carried out outside the context of traditional war." [10]

"A form of conflict that: Pursues political objectives through integrated campaigns; Employs mostly nonmilitary or nonkinetic tools; Strives to remain under key escalatory or red line thresholds to avoid outright conventional conflict, and; Moves gradually toward its objectives rather than seeking conclusive results in a relatively limited period of time."[11]

"[U]nique combinations of influence, intimidation, coercion, and aggression to incrementally crowd our effective resistance, establish local or regional advantages, and manipulate risk perceptions in their favor."[12]

"[A]n approach to international affairs that typically involves efforts at censorship or the use of manipulation to sap the integrity of independent institutions . . . allowing authoritarian regimes both to limit free expression and to distort political environments in democracies. . . ."[13]

The CSIS study team sees strong commonality across these definitions. Five common elements stand out:

1. **Bounded Thresholds**: There is an observable set of activities that are more threatening than statecraft but do not involve direct military combat between principal parties.[14] While precise and universal parameters are difficult to define, gray zone tactics seek primarily to avoid escalatory tripwires. The actor that uses gray zone tools might aim to accrue gains slowly, potentially accruing the kind of improved positions previously acquired only in battle. The actor might instead engage in violence but only through proxies or other means of obfuscation intended to remain below a rival's escalatory bar.
2. (**Veiled**) **Intentionality Toward a Security Objective**: An actor uses gray zone tactics in pursuit of security goals. Sometimes the security goal is clear, such as with China's militarization of reclaimed land in the South China Sea. Often, however, the link between the tactic and its security aim is veiled. This is particularly notable in the economic and information realms. Economic coercion, for example, might be intended to affect purely economic interests, or it may be used to undermine an adversary's international leverage.[15]
3. **Multidimensional Toolkits**: The means for undertaking gray zone activity spans a rival's capabilities and is limited only by the bounded thresholds outlined above, not by traditional legal and functional categories. Use of the full spectrum of state power also reinforces the ability to conceal intentions. For example, some rivals work with non-state or quasi-state entities that exhibit hybrid characteristics

that marry military capability with ambiguous legal connections to the government. Others pursue coercive energy and economic strategies.

4. (**Dis**)**Information Operations**: Notable in the multidimensional toolkit of gray zone efforts is the inclusion of information and disinformation operations. These types of operations are meant to both bolster the narrative of the state using these types of tools and foment social and political instability in target countries.
5. **Public- and Private-Sector Domains**: Boundaries between the public and private domain are blurred in the gray zone. States frequently use state-owned or state-affiliated enterprises as covers for activities, leverage private entities to evade state authority, or target private companies to undermine political processes and hold citizens at direct risk.

Accounting for these commonalities, and relying on its own research in this field, the study team at CSIS defines gray zone challenges as:

> *An effort or series of efforts intended to advance one's security objectives at the expense of a rival using means beyond those associated with routine statecraft and below means associated with direct military conflict between rivals. In engaging in a gray zone approach, an actor seeks to avoid crossing a threshold that results in open war.*

STUDY OVERVIEW

This project builds upon and synthesizes the extensive literature describing gray zone threats. It provides policymakers with a recommended campaign plan to compete against and counter gray zone challenges. By doing so, it provides a basis for the development of more detailed planning efforts against specific threat vectors and along traditional functional national security lines.

The CSIS study team analyzed the activities of four actors—China, Russia, Iran, and North Korea—across seven gray zone tools. Those tools were categorized as follows:

1. Information Operations and Disinformation;
2. Political Coercion;
3. Economic Coercion
4. Cyber Operations;
5. Space Operations;
6. Proxy Support; and
7. Provocation by State-Controlled Forces.

The study team then analyzed the effectiveness of U.S. responses to the threats posed under each tool as generated by the respective countries. The data collected was qualitative in nature and derived from print sources, including government documents, news items, histories, and academic studies. Country data for every tool was each ranked by two independent coders. Differences in coding were then adjudicated between coders and validated by the research group as a whole and the principal investigators. The gray zone competitor and U.S. response analysis helped develop a picture of current U.S. strengths, weaknesses, and gaps in the gray zone and informed the prioritization of issues for the culminating campaign plan.

The next chapter will report the findings of the CSIS study team's research on contemporary gray zone challenges and its expectations for gray zone competition over the next 10 years. The third chapter presents the campaign plan. The fourth chapter explores follow-on measures necessary for implementing the campaign plan.

2 THE CHALLENGE

To inform the design of a campaign plan for gray zone operations, CSIS conducted a 12-month study of contemporary trend lines in the use of gray zone tactics against the United States and its allies. The study group surfaced a variety of activities, measuring them by frequency and level of threat posed. Researchers also evaluated U.S. responses to date. This chapter describes the environment for gray zone activities and the range of those activities being conducted by challenger states and identifies significant gaps in the U.S. approach to the gray zone.

THE ENVIRONMENT

Gray zone challenges are not new. Their prevalence and importance to U.S. security, however, are more significant today than at any time since the end of the Cold War. Numerous trends in the international environment are contributing to the heightened status of gray zone tactics. Among the most salient trends are the disequilibrium in the international system and the discontinuities in domestic politics around the world, including in the United States.

Scholars see a drift away from democracy in many pivotal nations and warn especially of "executive aggrandizement and strategic electoral manipulation."[16] This more permissive environment has meant that authoritarian and mixed regimes are experiencing a kind of renaissance.[17] A vanguard of countries are also willing to challenge democratic values around the world, complicating cooperation on the international stage and opening avenues for exploitation of the gray zone.

The United States is one of the countries vulnerable to such exploitation. In its most recent annual index, Freedom House tracked a decline in U.S. "political rights and civil liberties" that began eight years ago, with a precipitous drop noted in 2017. It still assesses the United States as solidly free but notes the following:

> *The pillars of freedom have come under attack here in the United States. The United States has already been weakened by declines in the rule of law, the conduct of elections, and safeguards against corruption, among other important indicators measured by Freedom in the World. The current overall U.S. score puts American democracy closer to struggling counterparts like Croatia than to traditional peers such as Germany or the United Kingdom.*[18]

Rivals have the means, motive, and opportunity to use gray zone tactics to their advantage.

In this broad context, rivals have the means, motive, and opportunity to use gray zone tactics to their advantage.

Means: The diffusion of technology, especially relating to space, cyber, and information, has put the means of sub-threshold coercion into the hands of more actors in more regions.

Motive: Actors seeking security advantages over their rivals are generally deterred from escalating competition over known thresholds because of the significant conventional and nuclear power extant in key states, including the United States, Russia, and China.[19] Competitors also feel constrained by the U.S.-led order, perceiving limited relative gains from routine statecraft.

Opportunity: As power and resources are redistributed among global and regional actors, and as rules and norms are absent, contested, or unenforced, actors find opportunities to take advantage of the contemporary ambiguity in the international system. Domestic divisions and distractions in many contemporary democracies, including the United States, are ripe for sowing discord and inaction.

The increased saliency of gray zone tactics thus results from dynamism in the international strategic environment, which itself relates to the diffusion of technology and power and dissatisfaction with the constraints of the current order. For regimes that approach the status of major regional actors, the temptation of the gray zone is that it may help them vault into the club of globally pivotal states. The vulnerabilities inherent to open societies coupled with U.S. dependence on many modern technologies also give adversaries opportuni-

ties to make steady gains against the United States and its allies, partners, and interests.

GRAY ZONE CHALLENGES AND CHALLENGERS

In the course of surveying contemporary state-based gray zone challenges, the CSIS study group found that four countries conduct the lion's share of concerning activities. China, Russia, Iran, and North Korea all leverage gray zone tools, either directly against the United States or against U.S. allies, partners, and interests to varying degrees of success. Of these actors, China is the most concerning, followed by Russia, given the breadth and quality of each state's toolkit and their relative potential effects on U.S. interests. The coercive tools used by these gray zone competitors range the spectrum of fake news and online troll farms to terrorist financing and paramilitary provocations below the threshold of conventional war.

The gray zone toolkit analyzed in this study examines seven main areas of coercive activity.

The Gray Zone Toolkit[20]

Information Operations and Disinformation: Use of social media and other outlets, in addition to traditional efforts, to bolster the narrative of the state through propaganda and to sow doubt, dissent, and disinformation in foreign countries.

Political Coercion: Use of coercive instruments to affect the political composition or decisionmaking within a state. The tools to achieve such outcomes can be licit or illicit.

Economic Coercion: Use of coercive economic instruments (e.g., illicit finance or energy coercion) to achieve economic goals or cause economic harm to an adversary.

Cyber Operations: Use of hacking, viruses, or other methods to conduct information warfare, cause physical damage, disrupt political processes, punish economic competitors, or commit other malicious acts in cyberspace.

Space Operations: Disrupting competitors' normal space activities and space-enabled services by interfering with the equipment itself, communications to or from space, or the data or effects provided by space systems.

Proxy Support: Direct or indirect use of non-state and parastate groups to carry out militarized intimidation or control territory to exert influence or achieve specific security or political outcomes.

Provocation by State-Controlled Forces: Use of non-military or paramilitary forces with direct lines of funding or communication to the state to achieve state interest without the formal use of force. This category includes covert and clandestine activities.

The CSIS study team found that all four states it examined deploy these seven gray zone tools against the United States and its allies, partners, and interests in some form. As noted above, the countries pose different levels of threat across the range of tools, experiencing more success against the United States in areas where each has a competitive advantage or where the United States lacks the capability or will to counter the threat. In turn, the United States counters threats with varied intensity, leading to mixed results that highlight strengths, weaknesses, and gaps in the U.S. gray zone approach. The following sections provide a summary net assessment of the gray zone challenges from the four primary countries of interest, assessed against the capabilities and response to date from the United States.

China

China aggressively and effectively employs many gray zone tactics. Its most effective are provocation by state-controlled forces, economic coercion, cyber operations, and space operations.

The most prominent element of China's gray zone campaign is its island-building activities. Since 2013, China has engaged in the dredging and artificial island-building in the Spratly Islands—creating 3,200 acres of new land—and building outposts throughout the Paracel Islands.[21] The Chinese rely on both the Chinese Coast Guard and the People's Armed Forces Maritime Militia (PAFMM) to enforce such activities.[22] At least in regard to the Spratly Islands, China has turned some islands into military bases, "complete with radar domes, shelters for surface-to-air missiles and a runway long enough for fighter jets."[23] According to Admiral Philip S. Davidson, this militarization means that, "China is now capable of controlling the South China Sea in all scenarios short of war with the United States."[24] In recent years, the United States has stepped up its freedom of navigation operations in the region, alongside continued efforts to improve diplomatic and defense relationships with territorial claimants at odds with China.

China's economic coercion includes President Xi Jinping's signature economic and foreign policy project, the Belt and Road Initiative (BRI).[25] Although the BRI enhances China's trade connectivity and reduces China's surplus domestic industrial capacity, China uses its economic leverage to shape other counties' interests and to "deter confrontation or criticism of China's approach to or stance on sensitive issues."[26] Moreover, there are questions as to whether BRI's "debt-trap diplomacy" creates opportunities for China to introduce military forces into their acquired assets.[27]

Alongside the development of BRI has been China's Digital Silk Road initiative, which involves bringing technological advances and digital infrastructure to developing economies. Like BRI, the Digital Silk Road can create economic benefits for China, but there are warranted concerns that the initiative has unstated security purposes.[28] For instance, through the installation of fiber optic cables, Chinese state-owned or state-affiliated enterprises will control vast amounts of data, which could ultimately be used by the Chinese government for leverage beyond the economic realm.[29] In the race for 5G, there is a similar fear that once a company like Huawei installs its network, it will be used for Chinese state espionage and intelligence gathering purposes and could create coercive influence. For instance, just as China cut off Japanese access to rare earth metals in the midst of an unrelated 2010 maritime dispute, the Chinese government could seek to punish or alter the policy of a hosting nation by turning off its 5G access, even if briefly.[30]

Additionally, China uses economic coercion to acquire intellectual property and otherwise conduct industrial espionage. This is done through cyber operations or by Chinese companies at the direction of the Chinese government, which includes acquiring "companies and technology based on their government's interests—not on commercial objectives."[31] As an example, from 2013 to 2016, Chinese companies sought to acquire a number of businesses in the semiconductor industry. The potential Chinese domination of the industry could play a role in altering the future global military balance, seeing as semiconductors are essential to advanced military systems.[32]

China relies on cyber operations in the gray zone for more than economic purposes. Cyber is a prime route to conduct espionage and intelligence gathering but also to target other states' critical infrastructure and disrupt political processes abroad. In all, Chinese cyber operations have targeted U.S. government entities, personnel, allies, and defense contracting companies.[33]

Since 2014, the most consistently-focused U.S. response to Chinese gray zone activity has been in cyberspace. With presidential-level attention, the United States undertook a public "naming and shaming" campaign and threatened the use of economic sanctions. Although the causal relationship between U.S. action and decreased Chinese activity is not clear-cut, the number of Chinese cyber incursions against U.S. private- and public-sector networks significantly declined thereafter.[34]

Currently, a number of high-level strategy documents, such as the 2018 National Cyber Strategy and the Department of Defense Cyber Strategy, appropriately highlight the challenges posed by Chinese cyber activities.[35] Additionally, the former seeks to build a "cyber deterrence initiative," which will work with "like-minded states to coordinate and support each other's responses to significant malicious cyber incidents."[36] In 2018, U.S. Cyber Command was elevated to a combatant command and in their subsequent "Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command" not only acknowledged gray zone competition at the strategic level but also named China explicitly as a cyber threat.[37] The highest levels of the U.S. government, including Vice President Mike Pence and acting Secretary of Defense Patrick Shanahan, have highlighted the threat posed by China's cyber activity.[38]

Despite this high-level attention, there is evidence that Chinese cyberattacks may be increasing in response to U.S. trade pressure, suggesting that the Chinese government continues to view cyber operations as a viable horizontal escalation tool it can employ as needed.[39] This accords with a more general assessment that the U.S. approach to Chinese gray zone tactics seems to be consistently several steps behind the threat. As in the Russia case, this is likely due in large part to the absence of a coherent strategic approach, leading to ad hoc U.S. responses from one crisis point or domain of interaction to the next. U.S. policymakers can be reassured that many Chinese gray zone tactics seem to be backfiring, as more countries and businesses become wary of China's motives and deny it desired leverage points. However, there is ample evidence to suggest that, absent more coordinated U.S. strategy, China is effectively controlling the pace and timing of interactions that concern vested U.S. interests.

There is evidence that Chinese cyberattacks may be increasing in response to U.S. trade pressure.

Understanding space to be a "new warfighting domain," China's well-financed space program engages in a host of gray zone activity.[40] Kinetically, China has frequently tested the technologies needed to develop a co-orbital anti-satellite weapon, including developing satellites capable of on-orbit rendezvous and proximity operations. China is also most likely pursuing non-kinetic weapons that result in physical damage to objects in space using directed-energy technology. This includes the utilization of laser weapons, which can temporarily or permanently damage satellites' sensors. According to the Defense Intelligence Agency, China is developing jamming technologies to target U.S. satellite communications and Global Positioning Systems (GPS) through the use of electronic attacks.[41] Commercial satellite imagery has shown military-grade Chinese jamming equipment on islands in the South China Sea, which can be used to target communications, PNT signals, or any other satellites in the region.[42] China has also been implicated in using their cyber capabilities target space systems. This includes conducting cyberattacks directly against U.S. satellites as well as hacking the computers of companies and government contractors that control satellites.[43]

Importantly, although China has the greatest capability to exploit the gray zone, it has chosen not to take action in some areas. This seeming restraint necessitates further investigation to understand whether China feels deterred by U.S. actions or is simply self-regulating for other reasons. If the latter is true and those reasons can be discovered and understood, they may offer a set of incentives to dissuade China from relying on gray zone tactics in the future.

Russia

Russia's most effective gray zone tactics are information operations and cyber operations, followed by political coercion and space operations.

Russian information operations from the Internet Research Agency (whose owner, Yevgeny Prigozhin, has close ties to Russian President Vladimir Putin) continue to be well-funded, relentless, and prolific.[44] Russia's political coercion in Europe has gotten bolder over time, coinciding with Putin's attempts to block the expansion of NATO. Moscow's deepened ties with Serbia, Serbian-majority Bosnia, and a failed covert operation to block the Prespa Agreement are all increasing calls for concern.[45] Russia has increasingly used gray zone tactics in space to jam GPS signals during NATO military exercises, conduct provocative rendezvous and proximity operations against U.S. commercial and allied military satellites, and has even lasered the sensors on a Japanese satellite.[46]

The United States has responded most effectively to Russian gray zone activity in the cyber sphere. The United States has a heightened awareness of the Russian threat, taken significant steps to improve its cyber defenses, and increased funding for cyber defense capability.[47] The National Cyber Strategy and the Presidential Policy Directive-41 of 2016 have been especially useful in highlighting policy priorities and improving cyber incident coordination. Most U.S. responses to other tools have been tepid.[48] Notable gaps in U.S. efforts are to counter Russian information campaigns and political coercion, particularly against European allies and partners. Though DoS's Global Engagement Center has

Russia's political coercion in Europe has gotten bolder over time, coinciding with Putin's attempts to block the expansion of NATO.

legislative authority to defend allies and partners from foreign information operations, it is not authorized to defend the United States from information operations targeting the United States, like those Russia deployed during the 2016 presidential elections.[49]

The most concerning shortcomings in U.S. responses to Russian gray zone activity are the poor clarification and coordination of efforts. The National Security Strategy, National Defense Strategy, and National Intelligence Strategy identify a wide range of Russian gray zone tactics as national security threats, yet they do not translate these concerns into clear policies and strategies. In that absence, agencies are forced to respond to Russia's gray zone tactics with few legislative authorities and ad hoc coordination. One notable example is DHS's Countering Foreign Influence Task Force (CFITF), which is the sole U.S. agency team actively combatting disinformation campaigns in the United States. Because the CFITF lacks legislative authority to combat information operations, it suffers from impermanent staffing and budgets and unclear objectives. Likewise, the Department of State's Energy Bureau (ENR) suffers from a lack of direction and authority to combat Russian energy dominance in Europe. Experts have expressed frustration that ENR's authorities are too slow and too hindered by legal structures and funding to quickly respond if and when a country requires emergency energy supplies. Though DOE has the capacity to aid this security concern, it has too insufficient a budget and legal authority to provide meaningful assistance and relies heavily on ENR. This lack of direction has driven some agency-led innovations, like the Russian Influence Group, an interagency coordinating body. However, most U.S. agencies struggle without clear authorities and responsibilities.

Iran

The preferred Iranian gray zone tools against U.S. interests include support for proxies, provocation by state-backed military forces, and cyber and information operations.

Iran's support for proxy groups across Lebanon, Syria, Iraq, and Yemen is one of its most effective tools in the gray zone and poses a significant threat to U.S. interests.[50] The Islamic Revolutionary Guard Corps (IRGC) is the paramilitary "executor of Iranian proxy policies," with close ties to groups such as Hezbollah in Lebanon, the Houthis in Yemen, the National Defense Forces militia in Syria, and the Badr Corps in Iraq, among others.[51] Through its special forces unit known as the Quds Force, the IRGC is able to train and advise its proxy forces—an "axis of resistance" estimated at over a quarter of a million fighters—outside of its borders through illicit funding streams, thereby threatening U.S. allies and partners in the broader Middle East region.[52]

The IRGC is able to train and advise its proxy forces—an "axis of resistance" estimated at over a quarter of a million fighters—outside of its borders.

As a state-backed force, the IRGC also actively participates in provocations such as close-encounter naval maneuvers in the Gulf and the Strait of Hormuz against U.S. and partner vessels. This involves using the IRGC Navy in parallel with the conventional Islamic Republic of Iran Navy (IRIN) to carry out low-level, threshold-testing provocations such as "approaching in very close proximity to U.S. ships with weapons uncovered, engaging in dangerous maneuvers that could have caused a collision, and conducting live fire exercises unannounced near U.S. ships."[53] These sorts of provocations—in addition to incidents such as the 2016 Iranian arrest of U.S. sailors who accidentally entered Iranian waters—have been a particular source of U.S. concern, leading to fears of inadvertent maritime escalation between the two countries.[54]

Iranian cyber threats and information operations threats are both swiftly increasing as more Iranian hackers work to target people, companies, and government entities around the world, focusing primarily on the Middle East region (e.g., Saudi Arabia and Israel)

but also on the United States directly.[55] Most notably, Iran carried out a data deletion attack on dozens of Saudi government and private-sector networks in 2016 to 2017.[56] The United States has acknowledged that Iran has been employing "increasingly sophisticated cyber techniques to conduct espionage."[57]

The regime in Tehran has a tight control over the domestic consumption of information by restricting television broadcasts, social media, and internet access, which prevents foreign influence and promotes pro-regime narratives.[58] Internationally, information operations have helped Iran perpetuate its image as a regional powerhouse, particularly as a challenger to Saudi Arabia and Israel, while simultaneously presenting itself as a reliable international partner, particularly during Joint Comprehensive Plan of Action (JCPOA) negotiations and in its continued adherence to the deal post-U.S. withdrawal.[59]

Iran's information operations also incorporate space as a gray zone arena. It has repeatedly jammed satellite communications broadcasts without major repercussions. As examples of this practice, Tehran has jammed Voice of America, the British Broadcasting Corporation, and others. The timing seems to correspond with when Iran is under pressure domestically or internationally. Given the recent escalations in tensions between the United States and Iran in the wake of the United States backing away from the JCPOA, Iran is likely to turn again to these forms of gray zone action.[60]

Overall, the U.S. response to most Iranian coercive activity has been moderately effective, with the exception of the Iranian cyber and information operations. The United States does not perceive the Iranian cyber threat to be as high as that of Russia and China; as a result, Iran is treated as a lower priority, and the United States inadvertently falls short against Iran's highly sophisticated information operations.

Although the Trump administration designated the IRGC as a terrorist group in April 2019, the act has done little to deter the IRGC's activities and may in fact have emboldened the group.[61] Although U.S. force posture contributed to the reduction of Iranian maritime provocation from mid-2017 onward, the effect was apparently temporary: recent attacks on two Saudi oil tankers, an Emirati vessel, and a Norwegian vessel in the vicinity of the Strait of Hormuz point toward an Iranian return to coercive maritime activity.[62]

U.S. economic sanctions on Iran have been the most effective responses to Iranian gray zone activity. The United States has carried out 17 rounds of Iran-related sanctions on 147 Iran-related individuals and entities. It has pursued a "maximum pressure" campaign against Iran, designed to "choke off revenues" of the regime that might otherwise go to support proxy forces, cyber activities, and similar activities.[63] The impact of unilateral U.S. sanctions on Iran is significant. Since the Trump administration pulled out of the JCPOA: Iran's GDP declined by 3.9 percent in 2018 and is projected to decline another 6 percent by the end of 2019; the Iranian rial has depreciated by 60 percent; and the country's oil revenues have suffered losses of over $10 billion, predicted to worsen further after the expiry of U.S. sanctions waivers to Iranian oil importers.[64]

The National Security Strategy and National Defense Strategy both explicitly call out Iran for engaging in gray zone tactics against the United States, its allies, and its partners.[65] Consequent U.S. policy decisions regarding Iran in 2019—including terrorist designation of the IRGC, deploying the USS Abraham Lincoln carrier strike group, pulling personnel out of Iraq, and rhetoric around sending 120,000 troops to Iran—has led to the rapid deterioration of U.S.-Iranian relations, portending a potentially dangerous escalation between the two countries.[66]

North Korea

North Korea's most salient gray zone activities include cyber operations, political coercion, and military provocations.

North Korea maintains a skilled and sophisticated cyber force capable of executing disruptive operations worldwide.[67] Notable cyber operations attributed to North Korea include the 2014 Sony attack, the 2016 Bangladesh Bank heist, and the 2017 WannaCry malware worm.[68] More recently, a wave of cyberattacks targeting U.S. based oil and gas companies is cause for concern.[69]

North Korea's political coercion is aimed at strengthening the regime's position by exploiting U.S. efforts to coordinate with its regional allies and partners.[70] For example, the ongoing trade war between the United States and China has forced the Trump administration to balance its commitment to the maximum pressure campaign against Pyongyang with its efforts to strike a credible bargain with Beijing over tariffs.[71] The trade war has inadvertently strengthened North Korea's

political position by pushing U.S. regional allies—principally South Korea and Japan—further into China's regional economic sphere of influence. "The trade war could have been an opportunity to drive a wedge between China and its regional trading partners," writes Bloomberg columnist Daniel Moss, "Yet the Trump administration's irreverence for the collateral damage of its actions might end up drawing China's neighbors closer into its orbit."[72]

Meanwhile, the Kim regime stands to benefit from the Trump administration's nebulous diplomatic strategy as the uncertainty relaxes Pyongyang's ability to play the rival states off one another to support struggling economy. The recent announcement by the South Korean government of a $8 million food aid package to North Korea—a decision supported by President Trump—is one such example of Kim's cunning ability to accrue relative political advantage without any comparable gains to Washington and its regional allies.[73] As Brookings expert Jung Pak wrote in 2018, "At a minimum, North Korea is attempting to sow division within South Korea and shape Seoul's policies toward ones that are favorable to Pyongyang."[74]

With 70 percent of its ground forces deployed within 60 miles of the DMZ, the threat posed by North Korean conventional military forces is clearly illustrated.[75] Experts find that military and other malign provocations follow a long-term cycle correlated with South Korea's elections and U.S.-North Korea negotiations.[76] North Korean gray zone military tactics also manifest in space, where the country is arguably the most prolific space-based systems jammer in the world. North Korea routinely jams GPS signals into South Korea, disrupting air travel and seaports near the DMZ.[77]

Malign provocations follow a long-term cycle correlated with South Korea's elections and U.S.-North Korea negotiations.

DPRK's May 4, 2019 and May 9, 2019 short-range ballistic missile (SRBM) tests put the success of alliance decoupling on global display, in addition to fracturing within the Trump administration itself.[78] Following the tests, a first since 2017, U.S. president Donald Trump and South Korean defense minister Jeong Kyeong-doo dismissed the missile tests along with calls to increase pressure on DPRK as a result.[79] The dismissal of DPRK testing was at odds with the Japanese defense minister Takeshi Iwaya, as U.S. acting secretary of defense Patrick Shanahan and national security advisor John Bolton who strongly asserted the tests were a violation of U.N.S.C. resolutions. Defense Minister Iwaya went further to call for the implementation of sanctions as required when violating the resolutions.[80] The fracturing within the Trump administration went further when Press Secretary Sarah Huckabee Sanders stated that "President Trump and the North Korean leader, Kim Jong-un, "agree" in their negative assessment of former Vice President Joseph R. Biden Jr."[81]

In response, the United States has coordinated a multinational "maximum pressure" campaign intended to deter North Korea's future nuclear development, bring regime leaders to the negotiating table, and ultimately denuclearize the Korean peninsula.[82] To that end, the United States continues to issue trade advisory warnings, bring attention to illegal ship-to-ship transfers, and maintain sanctions against entities doing business with the regime.[83] Moreover, the federal government has partnered with private-sector companies and foreign governments to attribute cyber operations to North Korean cyber agents as part of a name and shame strategy to increase international pressure on the regime.[84]

For the foreseeable future, two developments are likely to influence the U.S. response to North Korea gray zone activities. First, diplomatic grievances between North Korean and U.S. officials threaten to prolong the stalled negotiations.[85] For example, North Korean officials have publicly blamed the lack of progress on Secretary of State Pompeo and National Security Advisor Bolton. While President Trump maintains that he and Kim share a positive relationship, differing interpretations about who is responsible for the breakdown in talks at Hanoi, in addition to internal tensions within the executive branch leadership, raises doubts about the possibility of another summit.[86] Meanwhile, President Trump has postponed

EXAMPLES FROM THE GRAY ZONE TOOLKIT

U.S.-South Korea military exercises which observers say could be detrimental to U.S. regional influence.[87] That is, the reduction in joint drills benefits the strategic aims of North Korea, Russia, and China at the expense of weakened multilateral coordination between the United States, South Korea, and Japan.[88] According to one recent report, "Any such drawdown would face strong pushback from Congress and Japan, whose conservative government is deeply wary of North Korea's intentions."[89]

North Korean behavior since the Hanoi summit also suggests that Kim is determined to find "a new way" to strengthen his international position absent a U.S. agreement. To that end, Kim's April 2019 visit to Russia and his continued outreach to China for economic assistance can be interpreted as a strategy to divide the United States and its regional allies while by finding ways to evade the international sanctions regime.[90] Russian investment in North Korean infrastructure and mineral resources, for instance, would strengthen Kim's strategic posture by reducing his dependence on a U.S. brokered agreement.[91] Put simply, North Korea's gray zone activities will likely be geared toward exploiting the perceived U.S. ambivalence toward its regional commitments.[92]

FINDINGS

The summaries above illustrate the range of actions and actors operating in the gray zone in ways potentially damaging to U.S. interests. At the same time, they illustrate the degree to which various departments and agencies of the U.S. government are active in efforts to combat these threats. Nevertheless, the collective U.S. approach has generally been less than the sum of its parts. The result is a largely reactive and ad hoc U.S. strategy: actions taken by the United States react to specific incidents or threats and are either poorly integrated across tools of power or not integrated at all.

Figure I illustrates how the basic tools of power are optimized for the "high end" and "low end" of the spectrum of U.S. national security policy.[93] Both are important, but as the CSIS study team has found, the gap that has developed in between—the gray zone—raises critical strategy and policy questions that also require answers.

Four significant pain points stand out within the current U.S. "action-reaction" approach to gray zone com-

SPECTRUM OF U.S. FOREIGN POLICY ACTIVITY

Statecraft ⟷ Major Conflict

U.S. TOOLKIT				
	Diplomacy	• Negotiate access agreements • Conduct arms control • Routines of interaction on behalf of U.S. citizens and the U.S. government, especially via embassies	• What more should the United States do to hedge against Chinese 5G technology in Europe? • How should the United States assist allies being subjected to adverse economic and political coercion?	• Sue for peace and/or terms of surrender • Invoke collective defense (Article V) • Build warfighting coalition
	Informational	• "Free and Open Indo-Pacific" narrative • NATO Article V messaging • Watching conflict indicators	• How can the U.S. federal government incentivize media literacy and civics at home? • Should social media platforms be regulated?	• Distribute images of adversary troops crossing international border • Issue joint statement of allied resolve • Public and backchannel messaging to known adversary
	Military	• Exercise freedom of navigation • Build allied interoperability	• How can the United States dissuade the use of disguised state-backed forces? • What assistance to allies facing "unconventional" coercion is effective?	• Execute military operations to deny, defeat, or otherwise achieve established objectives
	Economic	• Negotiate trade agreement • International development assistance	• Is the defense industrial base secure? • What can the United States do to assist the private sector in preventing economic coercion? Report cyber intrusion?	• Blockade • Wartime lend/lease-style support to allies

petition:

Indications and Warning: The CSIS study team finds that the United States has not adequately adapted its information indicators and thresholds for warning policymakers to account for gray zone tactics. Competitors have undertaken a marked shift to slow-burn, deceptive, non-military, and indirect challenges to U.S. interests. Relative to traditional security indicators and warnings, these are more numerous and harder to detect and make it difficult for analysts to infer intent.

Decisionmaking Speed and Quality: Even when appropriate warning is given, such as with China's land reclamation and subsequent militarization in the South China Sea, the United States can struggle with deciding to act on information, particularly in a timely manner. Savvy actors present gray zone tactics as one-off incidents that on their own do not seem to warrant a significant response. Many actors pursue gray zone tools precisely for their utility in testing or circumventing U.S. redlines. The approach has at times lured the United States into complacency, at least to the point at which a broader campaign is discerned. The time delay has a compounding effect. Additionally, the nature of most gray zone threats is such that they are difficult to attribute to a specific actor, which can confuse and delay U.S. re-

A campaign plan for the gray zone must account for U.S. vulnerabilities and strengths and must take care not to over-rely on any one tool of statecraft or line of effort.

sponses.[94] Given the high threshold of confidence for attributions inherent in U.S. norms and values, current U.S. gray zone responses are slow and comparatively weaker than attacks. Because the campaign of gray zone tactics is designed to shift the status quo in an actor's favor, it becomes increasingly difficult—and requires greater investment—to shift it back.

Public-Private Collaboration: Most of the competitive U.S. strengths lie outside the confines of the U.S. government. U.S. cultural suasion, economic reach, and information tools come largely from the private sector and civil society. The United States has struggled to bring these tools to bare in the face of gray zone tactics. The failure to successfully rally its sources of soft power (e.g., U.S. social media companies, private investors, the public at large) to serve as invested allies has hampered U.S. government efforts to compete against states using gray zone tactics, especially economic, political, and informational ones.

Campaign Mindset: Reactivity and ad hocery are symptoms of a more general U.S. tendency to manage national security from crisis to crisis. This approach falls short in the sort of competitive global landscape the United States faces today. Early in the Cold War, George Kennan warned of U.S. "popular attachment to the concept of a basic difference between peace and war . . . and by a reluctance to recognize . . . the perpetual rhythm of struggle" in international relations.[95] Add to this tendency the practically ceaseless pressure of business and it is easy to see how gray zone tactics can be so successful as part of a longer-term strategy that undermines U.S. interests. Without a campaign mindset and associated toolbox, it is difficult to advance objectives in the face of gray zone tactics.

A campaign plan for the gray zone must account for U.S. vulnerabilities and strengths and must take care not to over-rely on any one tool of statecraft or line of effort. If the United States is to engage seriously in gray zone competition, it will need to identify and employ a broad spectrum of its national power to deter, compete, and counter (where necessary) other countries' approaches. Furthermore, gray zone threats are inherently adaptive and thus dynamic because they work around U.S. strengths. It is therefore critical that the United States understands its own capabilities, the capabilities of its adversaries, and international standards of conduct to compete in, shrink the size, and ultimately deter use of the gray zone.

3 THE CAMPAIGN PLAN

CSIS DEFINITION

Gray Zone Approaches

An effort or series of efforts intended to advance one's security objectives at the expense of a rival using means beyond those associated with routine statecraft and below means associated with direct military conflict between rivals. In engaging in a gray zone approach, an actor seeks to avoid crossing a threshold that results in open war.

Adversaries and competitors use gray zone tactics as part of a larger strategy. Like countering terrorism, gray zone campaigning should be thought of as a major strategic component within a broader U.S. national strategy. Because of the prevalence of gray zone tactics, and the expectation of continuing challenges and opportunities presented in the spectrum between routine diplomacy and major military operations, the CSIS study team concludes that the United States would be advantaged by using a campaign planning framework specifically focused on gray zone operations. This will not substitute for a well-crafted national security strategy, nor for discrete purpose-built strategies regarding U.S. policy toward China or Russia or to advance, for instance, cyber or space operations. It should, however, better position the United States to gain advantage as a gray zone competitor, which will be integral to its success in virtually all national security pursuits.

This campaign plan capitalizes on U.S. strategic advantages, lays out the key lines of effort in pursuit of core national interests, and describes ways to outpace the dynamism of gray zone threats.

WHY CAMPAIGN PLANNING?

The terminology of campaign plans is unfamiliar to many outside the military. It is thus reasonable to question whether it is a useful approach to the interagency and international approach that gray zone challenges inherently demand. The diplomatic community, for instance, thinks most naturally in terms of country strategies, given the embassy-centric nature of its mission. The National Security Council staff is used to issuing summaries of conclusions that delineate lines of agency responsibility. These and other similar approaches have a valuable role in implementing a strategy or campaign approach, but they are not substitutes for it. As presented in more detail in the next chapter, the lack of an interagency planning culture is a long-acknowledged shortcoming. This deficiency should be addressed rather than accepted and ignored. The international environment is seldom forgiving enough to ensure its challenges match preferred U.S. solutions.

U.S. STRATEGIC ADVANTAGES

The United States brings considerable strategic advantages to the gray zone problem set. The following factors, comprising a mix of soft and hard power, are potential asymmetric assets in the U.S. portfolio.

U.S. Constitutional Tenets

Too often seen as a source of vulnerability, the commitment of the United States to its constitutional principles, including respect for individual freedoms, a layered system for government accountability, and adherence to transparency and rule of law, is its greatest potential strength in combatting gray zone tactics. The more attractive the U.S. model of governance, the less susceptible its citizens and foreign populations are to tactics aimed at corroding the nation from within and without. A vibrant U.S. democracy lessens the exploitative potential of many authoritarian gray zone tactics and simultaneously erodes the power of those whose governance compares poorly to it. In the words of CSIS Senior Adviser Suzanne Spaulding, U.S. strategy should be grounded in forcing others to "fight in the light."[96]

Business, Media, and Civil Society

Closely related to the strength of the U.S. democratic governance model is the vibrancy and reach of the U.S. non-governmental sectors. In the economic realm, the United States has traditionally been able to thwart economic coercion against it—and advance its own interests—because others' desire to work with U.S. busi-

Gray zone campaigning should be thought of as a major strategic component within a broader U.S. national strategy.

nesses, attract U.S. tourists and investors, and reach the U.S. market with their own goods and services. U.S. cultural suasion is further propelled by its leadership in the arts, entertainment, and media. To the frustration of those who might seek an alternative to the U.S. way of life, its companies, academic and scientific communities, personalities, and philanthropies carry U.S. soft power far and wide.

The United States faces serious challenges in defending itself from efforts to exploit the openness of its society, but it will be most successful in advancing its interests if it builds on, rather than erodes, fundamental tenets of its democracy. Harvard's Joe Nye explains, "As democracies respond to sharp power, we have to be careful not to undercut our own soft power by imitating the authoritarian model . . . Authoritarian countries such as China and Russia have trouble generating their own soft power precisely because of their unwillingness to free the potential talents in their civil societies."[97]

Alliances and Partner Networks

Strong alliances and international partner networks are another asymmetric advantage on which the United States should capitalize. The competitors most intent on undermining U.S. interests in pursuit of their own—including China, Russia, Iran, and North Korea—lack America's track record of galvanizing international action to advance common security interests. They are seen by many other nations as spoilers, rather than creators, of international order. In a survey spanning people from 25 other nations, 63 percent of respondents, including Russians, preferred having the United States as "the world's leading power." Only 19 percent preferred Chinese global leadership.[98]

Some scholars have theorized that alliances bring greater risk of entanglement than reward in achieving desired U.S. outcomes.[99] Other recent scholarship disputes the view that alliances have the propensity to drag the United States into conflict, and evidence of the strategic value of alliances is significant.[100] In the past several years alone, the United States has reaped dividends when it has mobilized international support in the face of adversarial gray zone tactics. A United Nations tribunal ruled against China on its land reclamation activity at Scarborough Shoal, helping to deepen solidarity among Asian nations opposing its land-grabbing policies in the region. European nations and multilateral organizations have played a vital role in raising the costs on Russia for its gray zone tactics, including substantial economic sanctions for its invasion of Crimea and the expulsion of Russian intelligence officials in the wake of the attempted Skripal assassinations. On Iran and North Korea policy, the United States has also gained leverage when it has shown an ability to bring international sanctions to bear. Such actions do not always immediately reverse gray zone gains, but in these early years of establishing new boundaries (and re-establishing traditional ones), raising the costs of gray zone actions will help to diminish their appeal.

Breadth and Depth of Government Means

For at least the last 70 years, the United States has made it a priority to invest in the tools of statecraft and international leadership. It has the world's largest economy, most capable—albeit challenged—military, a storied diplomatic and development corps, and expansive, professionalized law enforcement and intelligence communities. When able leadership orchestrates these capabilities with sustained unity of effort, and in alignment with the other strengths described above, the United States has been able to advance the interests of the American people. Perhaps the most notable of such times includes the aftermath of World War II, when the United States worked with like-minded nations to establish an international system of governance disposed toward individual freedom, democratic norms, and the rule of law among nations.

Campaign planning should seek first to shore up the strategic advantages above. The reader can readily think of deficiencies in how the United States is currently tapping its potential in these areas. Recommendations on specific areas for improvement are included in the priority lines of effort described later in this chapter. A second priority is to improve America's operational approach to deterring harmful gray zone tactics, campaigning in the face of them, and responding effectively in crises below the threshold of war. In the preceding chapter, the CSIS study team concluded that the United States government is currently undertaking action in response to all the gray zone threat vectors it identified. However, too often the U.S. approach has been reactive and ad hoc. In particular, the United States lags in necessary capabilities in indications and warning; decisionmaking quality and speed; public-private collaboration; and transitioning to a campaign mindset for competing against gray zone challenges.

MISSION AND PRIORITIES

Mission Statement

Given the environment described in the prior chapters and the assumptions laid out in the report's introduction, the United States should work in close collaboration with a range of international and domestic partners to employ a campaign planning model with two primary objectives. First, it should seek advantages in gray zone competition that bolster its national security interests. Second, it should seek to undermine competitors' gray zone tactics, from deterrence to effective campaigning to crisis response. Concepts such as "winning" and "losing" will have less salience to these objectives than measures of relative gain and loss assessed over time.

As it pursues its objectives, the United States should not lose sight that its laws, principles, and values are strategic *advantages* in gray zone competition. Competitors' autocratic, deceptive, and extra-legal gray zone tactics can create significant challenges for U.S. foreign policy but responding in like manner will change the character of the United States, diminishing its appeal not only to its allies but to its own citizens. Thus, even as the United States engages in gray zone tactics, it should do so in accordance with its principles.

Interest-Based Priorities

In pursuit of the above campaign planning mission, the United States should prioritize its gray zone approach according to the importance of the U.S. interests at stake. Threats wax and wane, but a bipartisan sentiment about vital U.S. interests is more enduring. Every published national security strategy, spanning Republican and Democratic administrations, has framed four driving U.S. interests: securing U.S. territory and citizens; meeting treaty commitments; promoting prosperity; and upholding the rule of law, including respect for human rights.[101] The Trump administration is the latest to use an interest formulation along these lines:

- Protect the U.S. people, homeland, and way of life;
- Promote U.S. prosperity;
- Preserve peace through strength, with an acknowledgment that "allies and partners magnify our power"; and
- Advance U.S. influence, including through "a commitment to liberty, democracy, and the rule of law."[102]

The United States should not lose sight that its laws, principles, and values are strategic *advantages* in gray zone competition.

This relative constancy of vital interests is a firm, strategy-based foundation on which to ground campaign planning. Requiring multiple instruments of statecraft to achieve, an interest-based framework also helps propel bureaucracies past their inclination to devolve all problems into severable organizational stovepipes. Clear roles and responsibilities for execution are important, but as the CSIS study team finds, beginning from and routinely returning to an integrated campaign design is imperative.

Given the tactics and targets of known and expected gray zone competition, three priorities stand out as pillars—or, in campaign parlance, lines of operation—for planning:

- Protect U.S. constitutional tenets and the U.S. way of life;
- Promote the nation's economic vitality; and
- Advance U.S. influence.

Each line of effort is described in further detail below.

LINES OF EFFORT

1. Protect U.S. Constitutional Tenets

America's first line of effort in deterring, campaigning in, and responding to gray zone challenges is strengthening the underpinnings of the U.S. system of governance. The U.S. public is as divided as it has been in a generation. These divisions span many dimensions: political, socioeconomic, geographic, gender, and age, to name some of the most pronounced. What unites the country at present is perhaps equally troubling: a steady drop in confidence in governing institutions and a growing sentiment that "the system is rigged."[103] These socio-political trends can be exploited by a wide range of opportunists, including foreign nations and non-state actors.

Gray zone tactics, with the prospect of skirting U.S. thresholds for action, are a preferred means of such ex-

ploitation. Speaking to the example of Russian interference in U.S. elections, David Brooks wrote in the New York Times, "It may not be bombing buildings or shooting at people, but if a foreign government is attacking the factual record on which democracy runs, it is still a sort of warfare. The Russians are trying to undermine the information we use to converse, and the trust that makes conversation possible."[104]

The system's commitments to the rule of law, individual rights and freedoms, protections of minorities, and promotion of prosperity underwrite the U.S. way of life as well as domestic political stability. Three priorities for U.S. government action to reinvigorate this system to withstand gray zone attacks are: securing the co-equal branches of the U.S. federal government; fostering civil society, including through greater public-private collaboration; and advancing a free and fair press.

Democratic Institutions

The democratic pillars of U.S. society are desirable targets for gray zone tactics. When vibrant, they are the greatest source of U.S. soft power, and weakening them directly undermines U.S. interests. There is widespread attention to the threats facing the U.S. electoral system. Russian interference in the 2016 presidential election called into question the vulnerability not only of electoral institutions but also the U.S. voter. Cyberattacks on both the media environment around elections and on elections systems themselves are a concern.[105]

As CSIS's Defending Democratic Institutions project highlights, there is evidence that Russian information operations also target the U.S. justice system, exploiting fissures in U.S. society for their own gain and in some cases inventing foundationless narratives.[106] In one salient 2016 example, a Facebook group calling itself "Secure Borders" accused a prosecutor and a judge in a municipal criminal case of corruption. Though presenting itself as a group of local citizens, the group was actually a creature of Russian disinformation operations and weaved in fears about Syrian immigration unrelated to the case.[107]

Although Russia has been the most brazen, other actors may be, or may become, emboldened to use gray zone tactics to erode or disrupt U.S. democratic institutions. All three branches of the federal government and the electoral and legal processes that support them must be legitimate in the eyes of the U.S. citizenry as well as those the United States seeks to sway abroad. Efforts should

Protecting the U.S. Constitutional Tenets

- Protect U.S. electoral processes, its judicial systems, and the legitimacy of its governance model
- Invest in educating U.S. citizens in civics and media literacy
- Strengthen social media regulation, respecting precedent on U.S. citizens' First Amendment rights

focus on ensuring equal treatment for U.S. citizens, enforcing existing anti-corruption and foreign interference and investment laws, and capable defending electoral and judicial processes from cyber and disinformation attacks.

Civil Society

In the nineteenth century, visiting Frenchman and political scientist Alexis de Tocqueville observed that "the spirit of association" was a foundational element of democracy and social resilience in the United States.[108] A vibrant civil society builds public resilience against disinformation and political and economic coercion. The National Center for Charitable Statistics at the Urban Institute reports that the United States had somewhere around 1.5 million nonprofits registered with the Internal Revenue Service in 2015.[109] In 2018, a record-high 77 million U.S. citizens—30 percent of adults—performed volunteer service.[110] The U.S. drive to join together to secure interests and solve problems remains strong.

Nevertheless, numerous trends are combining to weaken U.S. civil society and disconnect that society from its government, making it more prone to exploitation by gray zone tactics. A declining percentage of the U.S. population has public service experience, including military experience. The information age and especially social media have created silos of virtual connectivity that have the potential to separate people as much as they bring them together. The federal government has significantly reduced grants to support civics education in U.S. schools over the last decade, and the quality of existing civics education—which is not even required in eight states—is uneven.[111] In 2017, only 24 percent of high school seniors—the next generation of voters—scored as proficient or higher on a national civics exam; only 12 percent were proficient or higher in U.S. history.[112]

The business community is a vital segment of U.S. civil society. Although a frequent target of economic coercion, evidence is strong that U.S. businesses have historically been reluctant to report cyber breaches.[113] Moreover, there is little evidence that the private sector appreciates the degree to which it is in the crosshairs of state-based gray zone activity and relevant national security implications. A recent report on U.S. businesses demonstrates a lack of willingness on the part of U.S. companies to report or thwart Chinese cyber intrusions.[114] The 2018 National Cyber Security Strategy encourages strong dialogue between the federal government and private sector to encourage better reporting.[115] This is a good start. The importance of building trust between the private sector and the federal government extends beyond cyber security to include a range of economic coercion that happens in the gray zone, including through foreign investment and compromised intellectual property rights. Bringing the business community onboard as partners in combating gray zone threats and ensuring adequate reporting and enforcement mechanisms will greatly assist civic resilience.

Free and Fair Press

One of the main conduits of the information necessary for public policy debates and democratic oversight of government action is a free and fair press, independent from government control and intimidation and manipulation by those with an interest in promoting or suppressing certain stories. A long tradition of objective journalism in the United States is today suffering from a credibility gap, in part because of active gray zone efforts by U.S. adversaries. Disinformation is frequently designed to prey upon existing divisions, including partisan controversies. Using fabricated identities on social media sites, foreign troll farms have added energy to fierce public debates over issues as disparate as protests at National Football League games, security at America's southern border, mass shootings, policing, and the Mueller Report. Reporters themselves can fall into the trap of sensationalism stoked by foreign efforts.[116]

Yet again, this is an area where domestic conditions are already self-harming. According to Nielsen, the average U.S. citizen spends 11 hours a day consuming media, some 34 percent of it from the internet, where stories designed to stoke outrage can snowball.[117] Meanwhile, prominent politicians, notably including the president of the United States, have engaged in persistent attacks against the news media, undermining the credibility of outlets that print or air stories unfavorable to them and praising those who express admiration.[118] Succinctly summing up the challenge, CSIS's James Andrew Lewis notes: "The internet allows people to have their own facts. Social media amplifies this trend."[119]

Press freedom requires a bipartisan, patriotic commitment. First, elected officials must lead in pulling America back toward First Amendment norms that embrace free and fair media as central to U.S. democracy. Elites stoking widespread distrust in the media—calling them enemies of the public—are playing into the hands of those seeking to undermine the United States. Second, media literacy, like civics, should be a core element of twenty-first century public education. Third, the reg-

ulatory framework for media must better capture the role of social media. The European Union created significant new regulations in 2018; the U.S. approach will need to be carefully crafted to protect First Amendment principles, create needed transparency, ensure liability, and impose costs for noncompliance.

2. PROMOTE ECONOMIC VITALITY

Much of U.S. power is derived from its economy. The ability to sustain a prosperous way of life at home and promote it abroad is a direct result of the U.S. economic system. Those who wish to weaken the United States have taken aim at that system, including both the U.S. domestic organs and the system of international institutions the United States helped to build over the course of the twentieth century. Defending against gray zone threats to these institutions implies preserving three things in particular: reliance on the dollar as a reserve currency; U.S. access to global markets; and the health of the private sector.

Role of the Dollar as the Global Reserve Currency

Approximately 60 percent of all international reserves are currently held in dollar denominated assets, making the U.S. dollar the global reserve currency. This status is a market outcome and not the decision of an international body or an international treaty, but it is bolstered by careful U.S. policy management. Former Federal Reserve Chairman Ben Bernanke highlights this point, writing: "investors and governments freely choose to hold dollars . . . because of the quality of U.S. financial regulation; because the Federal Reserve has kept inflation low and stable for the past thirty years; and because the United States is large, prosperous, and politically stable."[120] This "enhanced prestige and status" provides the United States with, perhaps, the strongest soft power tool in the already robust U.S. arsenal.[121]

Because of the dollar's status, the United States remains the most influential voice in institutions such as the International Monetary Fund and the World Bank. Although these institutions do not reflexively adopt U.S. preferences, "most of the fingerprints on important outcomes are still American."[122] The dollar is therefore also a potential tool in punishing or deterring gray zone activity. Through sanctions, the dollar's centrality to international finance allows the United States to constrain malign actors and, at the extreme, employ comprehensive sanctions.[123]

Strengthen U.S. Economic Vitality

- Maintain a healthy and stable U.S. economy and ensure sufficient financial regulation to protect the dollar's global role
- Expand U.S. free trade agreements, both bilateral and regional, especially for Europe and Asia
- Help U.S. businesses defend against cyber and economic coercion and ignite their soft power, including through investments in U.S. innovation

Sanctions work best when they are multilateral in scope.[124] Imposing unilateral sanctions jeopardizes relationships with U.S. allies which are impacted by secondary sanctions. Additionally, the more the United States uses sanctions, the more targeted countries look for and invest in permanent workarounds, which could impact the strength of the dollar.[125] To ensure sanctions remain effective and do not isolate allies, and that the dollar remains essential, the United States should broaden its approach to economic statecraft (see next section) rather than over-rely on sanctions.

Increased Market Access

Growing the U.S. economy—a vital interest of U.S. security policy—requires gaining access to the 95 percent of the world's population that lives outside of the United States.[126] Gaining increased market access through both trade and U.S. foreign aid not only promotes U.S. economic growth but also provides alternatives to economic gray zone activity.

Free trade agreements (FTAs) have been particularly effective in opening foreign markets to U.S. exports.[127] The United States is currently party to 20 bilateral trade agreements, which accounted for $720.3 billion in U.S. goods exported in 2017.[128] The United States is also party to over 50 Trade and Investment Framework Agreements (TIFAs), which can serve as foundations for eventual FTAs.

Economic gains aside, bilateral and regional FTAs can be used as inducements that present alternatives to competitors' coercive economic activity, such as China's Belt and Road Initiative (BRI). Unlike the "debt-trap" agreements negotiated via China's BRI, FTAs negotiated by the United States are comprehensive and address issues such as: "rules on foreign investment, intellectual property rights protection, commitments on opening government procurement markets, and enforceable provisions on labor standards and the environment" that benefit the partner and the United States.[129] Through these agreements, the United States is also able to promote its values and continue to shape global trade rules. Other countries either adopt the rules that reflect U.S. values or watch their investment in a trading bloc shrink.[130]

In any economy, there will be some sectors that gain more than others from an FTA. Typically, some sectors even lose. Because FTAs leverage where a country has a comparative advantage, the U.S. service sector has seen net gains from FTAs.[131] For U.S. manufacturing, the picture is more complicated due to the nation's "relative abundance of high-skilled labor and a relative scarcity of low-skilled labor. As such, the United States' comparative advantage will be in goods produced using high-skilled labor intensively."[132] The U.S. government and private sector must mitigate these disparities by investing in education and retraining programs for people in sectors disadvantaged by FTAs.

Foreign aid is another form of inducement that can increase market access for U.S. business.[133] In 2016, the United States exported more than $2 trillion in goods and services. Eleven of the top 15 U.S. export markets were former recipients of U.S. foreign assistance, like South Korea.[134] As with trade, U.S. foreign aid challenges adversaries that deploy gray zone tools by creating an alternative for targeted third-party countries. In October 2018, the U.S. Congress passed the Better Utilization of Investment Leading to Development (BUILD Act), in part as a counter to growing Chinese overseas investment.[135] The act created a new U.S. development agency: the U.S. International Development Finance Corporation (USIDFC).[136] The USIDFC is a development finance institution which "will seek to 'crowd-in' vitally needed private-sector investment in low and lower-middle income countries."[137] The BUILD Act has pledged $60 billion in funding for the USIDFC. U.S. foreign aid alone is unlikely to compete with China's current level of foreign investment—China has pledged $60 billion to Africa alone—but it is a critical element in a comprehensive economic strategy for advancing U.S. economic and geopolitical interests in the face of others' gray zone tactics.[138]

Support to the Private Sector and U.S. Industry

A critical category of action within the economic line of effort is U.S. government leadership in igniting business efforts to sustain America's technological edge, even as others use gray zone tactics to erode it.

The U.S. government must lead a public-private campaign to advance technologies relevant to security. Ensuring sufficient and appropriately targeted government research, development, and capability is critical. Facilitating technology innovation in the commercial sector is similarly important. Doing so will require a mix of grants and other investments, such as in STEM education, new and strengthened research and development partnerships (domestic and international), regulatory changes, and senior leader attention. The

The United States must also have an immigration strategy that supports its competitiveness in critical innovation fields.

details are important and will require careful planning. A National Innovation Strategy may be a helpful first step for determining the most beneficial focus areas for U.S. government action, along with proposals for the mix of incentives and regulations (or deregulation initiatives) to deploy. [139]

The United States must also have an immigration strategy that supports its competitiveness in critical innovation fields. Immigration has been a major element of U.S. technological dominance: between 1995 and 2005, more than half of Silicon Valley's new companies were founded by immigrants.[140] There are valid concerns to be addressed pertaining to graduate students from competitor nations gaining skills in the United States only to return home. Those concerns should be mitigated, but U.S. policy must be careful to consider the facets of immigration that contribute to U.S. economic power.

Additionally, the United States must help the private sector protect its intellectual property and limit cybertheft. There must be stronger cyber defense regulation and enforcement, especially for national critical infrastructure, known gray zone targets. Incentivizing private-sector transparency when attacks do occur, including damage assessment and, where possible, attribution, will also help.[141] The government should also consider maintaining—and making public—a list of state-owned or affiliated companies that have been determined to have stolen intellectual property.[142]

The private sector may also leverage energy as a tool, as technological improvements such as hydraulic fracturing and directional drilling help bolster the U.S. economy, battle the narratives of "American 'declinism'" domestically and internationally, and take on energy-reliant gray zone challengers.[143] The United States can leverage its energy sector to combat gray zone activity. In carrying out trade negotiations and increasing market access, having the ability to ship liquified natural gas (LNG) provides U.S. trade negotiators with a new means of leverage. With an abundance of oil, organizing an international oil embargo against a country that is energy reliant, such as Russia or Iran, becomes much easier.[144] The United States can potentially assist other countries, such as Ukraine, in accessing untapped shale gas, which makes it less dependent on Russia for supplies.[145] And while the United States will not replace Russia anytime soon as the primary provider to Europe, the United States could be of critical assistance in relieving pressure on allies in times when Russia might seek to use energy coercion as a gray zone tactic.[146]

3. ADVANCE U.S. INFLUENCE

A successful campaign to counter and deter gray zone coercion will be international in scope and require a renewal of the U.S. commitment to international engagement based on law, cooperation, and shared values, alongside investments in a diverse set of offensive and defensive means to support it. These components of the campaign are not just rhetorical devices; they constitute the foundations of U.S. action and leadership and will mobilize global efforts to steer international relations away from the gray zone.

Rule of Law

At the international level, rule of law is built on a system of multilateral institutions forming and reinforcing standards and norms and promoting collaboration to tackle transnational challenges. Gray zone tactics are almost entirely transnational by their nature; they rarely affect just one country and often target the norms and institutions used to regulate international life. Thus, maintaining the rule of law, and international institutions by association, must be a key element of a strategy to defend against and neutralize gray zone threats.

Doing so will require reinforcing norms in some places and creating new norms and adapting institutions in others. The United States must send clear and consistent signals regarding the norms of conduct it expects international actors to adhere to in the context of gray zone tactics. This includes placing a foreign policy priority on establishing norms in largely ungoverned domains like disinformation, cyberspace, and space, and

practicing and enforcing established laws and norms around well-settled questions of territorial sovereignty and air and maritime law.

The information operations, political coercion, and proxy support activities in the gray zone will especially require international mobilization. International standards for governance transparency and accountability should be foremost in this re-examination of norms and institutions and will have implications for internet-based surveillance, press and media freedoms, financial transactions, and—most importantly—the financial relationships governments have with private-sector and non-state actors.[147] International cooperation on "governance gaps in key markets and institutions" that adversaries who use gray zone tools can exploit to undermine democratic states is of critical importance.[148] The United States should avail itself of existing international institutions to broker new arrangements and help form new incentives to bolster transparency and accountability between and within states.

This project will be challenged by the surge in authoritarianism around the world and the domestic challenges facing some of the staunchest democracies. Cooperation on developing new norms and standards for transparency with regimes undertaking authoritarian practices will need to be coupled with incentives for participation. Wherever possible, norm-setting should be done with the adversaries of greatest concern. This creates the greatest legitimacy and thus the highest potential for a resilient and proactive international community when violations occur. Where it is not possible to reach true agreement with potential adversaries, either because they will not participate in negotiations or cannot be trusted to adhere to the established norms, the United States should seek instead to develop multilateral coalitions of the willing that can work with U.S. citizens to credibly deter or respond in times of crisis.

Above all, U.S. approaches to gray zone threats must encourage international standards that update concepts of noncombatant immunity. Holding civilian electrical grids at risk, threatening the safety and privacy of individuals by selling and exploiting personal data, perpetrating intellectual theft, and exacerbating social cleavages with the intention of triggering political violence should all be unacceptable activities under international norms and law. Revisiting the definition of a combatant, in an era when countries increasingly use proxies and "little green men" to conduct gray zone

Reinforce International Engagement

- Strengthen international norms and their enforcement
- Improve alliances, America's greatest international strength
- Diversify and grow America's foreign policy toolkit beyond conventional military capability and economic sanctions

activities, will also be important. In all cases, the United States must lead the way in drawing ethical, not just operational, lines in the gray zone.

Healthy and Reliable Alliance System

The alliance structure that formed the backbone of twentieth century statecraft has been under enormous pressure in the second decade of the twenty-first century. This condition is directly tied to gray zone challenges, as undermining that alliance structure is a major goal of adversaries wielding gray zone tactics. The United States must not fall into the trap of helping adversaries dismantle the positive elements of alliances like NATO. Instead, it should focus on sustaining, strengthening, and adapting them for gray zone threats and other shifts in the international landscape. This will mean both preparing alliances themselves for deterring and responding to gray zone threats and building resilience among allies.

Fighting gray zone challenges requires access and cooperation, and access and cooperation require trust. A major element of America's ability to sustain international leadership is its commitment to recognizing the interests of others and where U.S. and others' enduring interests meet. To the extent that Russia and China are the main adversaries using gray zone tactics, traditional alliances in Europe and Asia are as relevant as ever.

In the European context, the revitalization of alliances will take place against a backdrop of long-standing tensions in the area of burden-sharing. As CSIS has argued elsewhere, security contributions happen along a variety of lines of effort, including measures of resilience not typically captured in purely fiscal terms.[149] In Asia, stressors include differences between the United States and its allies in their diplomatic approaches to the region, Japan's advancing military capability, and Chinese competition for military access. The United States will need to meet these challenges head on, including by adjusting its own expectations about contributions to common alliance activities and capacities.

Above all, allies must develop common appreciation of and approaches to gray zone threats, sharing information about adversary lines of effort and formulating joint priorities and responses. The cyber domain and tools to monitor and operate within it constitute the front line in allied adaptation to gray zone efforts, and interoperability among allies along these lines should be as important as conventional military operations have been in the past. Moreover, public-private cooperation and connections between external security measures and domestic measures will need to become more fluid. The security of the transatlantic financial system should be a major line of effort for NATO. This, in turn, demands new awareness and oversight regimes to maintain democratic accountability and prevent the kind of corrupt exploitation on which adversaries that deploy gray zone tools thrive.[150]

Multidimensional Power

Achieving U.S. security interests in the face of gray zone challenges puts a premium on appropriately leveraging a range of foreign policy tools. From military and covert direct action to diplomacy and economic statecraft, a capably employed suite of tools will advantage the United States for both defense and offense. Honed and ready, such tools can be used to deter actors seeking to exploit perceived vulnerabilities or wielded at a time and place of America's choosing to campaign for advantage.

Multidimensional power is always valuable in international affairs. For competing in the gray zone, it is vital. It enables approaches to conflict and conflict resolution beyond traditional vertical escalation to direct military conflict, a key advantage in a campaign of gray zone tactics. In recent years, the U.S. national security enterprise has relied heavily on demonstrations of conventional military power and economic sanctions to compete in the gray zone. Both are critical instruments for U.S. success, but they are insufficient. A brief review of deterrence theory and its applications to the specific dynamics at play in gray zone campaigning is instructive.

From military and covert direct action to diplomacy and economic statecraft, a capably employed suite of tools will advantage the United States for both defense and offense.

Even when it is using offensive means to pursue the three core interests in its National Security Strategy, the basic U.S. approach to international conflict accords with the general tenets of deterrence. The United States can deter by directly denying a rival its objective, including denying the ability to prevent the United States from achieving U.S. objectives (denial) or by punishing an opponent (punishment) until it reverses course, agrees to acceptable terms, or is simply convinced to forego further objectives, whichever may be the U.S. aim. To achieve its objectives through denial or punishment, the United States can seek vertical escalation of a conflict, such as with the employment of conventional or nuclear military power. Since the end of the Cold War, this has been the preferred U.S. form of deterrence, which has contributed to limiting conventional or nuclear actions against it.

As discussed in Chapter 2, U.S. success at deterrence by credible threat of escalation to military conflict has increased incentives for rivals to use gray zone tactics, which are attractive precisely because they make the risk of vertical escalation appear too great.[151] This is where the need for more diversity in the U.S. toolkit becomes critical for both offensive and defensive purposes. As China, Russia, and others have demonstrated, it creates the means for credibly threatening or employing horizontal escalation. Horizonal escalation might seek to challenge a rival in the same domain of conflict it has used, move horizontally to another domain, or expand the geographic area of conflict.[152] Horizontal escalation is an especially attractive option if one is willing to pursue one's objectives through deterrence by punishment rather than denial.[153]

Presumably for these reasons, the 2018 National Defense Strategy hints at a renewed U.S. military emphasis on greater use of horizontal escalation options.[154] In light of the growth in gray zone challenges, there is undeniable wisdom in this emphasis. As argued by the Commission on the National Defense Strategy, even as it seeks to outpace advanced capabilities, the U.S. military must itself deepen its dimensionality to campaign below the threshold of war.[155] This requires operational concepts that build on military capabilities in space and cyberspace, the information domain, foreign internal defense, and other smaller-scale campaigning techniques in the air, at sea, and on land.

Of course, many credible options will not involve the use of military force at all. At first, they will depend instead on the effective employment of U.S. soft power. Diplomatic and development influence are critical in deterrence as well as offensive campaigning. Economic statecraft—through both inducements and sanctions—could play a major role. As underscored in the first line of effort, priority must be placed on investing in the tools of public diplomacy as well as information operations. Covert action and U.S. gray zone activity will play a critical, albeit supporting, role. In the face of gray zone tactics, the United States will gain advantage by demonstrating the breadth and depth of its power across these areas. In its forthcoming, *By Other Means—Part II: Adapting to Compete in the Gray Zone*, the CSIS study team will provide specific design recommendations aimed at reducing the most glaring deficiencies in the national security enterprise that impede execution of this campaign plan.

Horizontal escalation is not without risks, including to other pillars of this campaign plan. It requires a tight coupling of operational choices and desired strategic effects to avoid self-defeating approaches. The United States will need to carefully consider how it creates desired effects without triggering unintended consequences, such as weakening political cohesion or finding oneself on the wrong side of a cost-imposing calculus. The ability to synchronize power and integrated strategic and operational lenses will be vital.

FOLLOW-ON PLANNING FOCUS

In all, the CSIS study team identified nine priority planning areas within the campaign's three lines of effort:

1. Protect U.S. electoral processes, its judicial systems, and the legitimacy of its governance model;
2. Invest in national service models, civics education, and media literacy;
3. Strengthen social media regulation, respecting precedent on U.S. citizens' First Amendment rights;
4. Maintain a healthy U.S. economy and ensure sufficient financial regulation to protect the dollar's global role;
5. Expand bilateral and regional U.S. free trade agreements
6. Help U.S. businesses defend against cyber and economic coercion and rally their soft power, including through investments in U.S. innovation;
7. Strengthen international norms and their enforcement; develop new norms for constraining and

SPECTRUM OF U.S. FOREIGN POLICY ACTIVITY

U.S. TOOLKIT	Statecraft ⟷ Major Conflict		
Diplomacy	• Negotiate access agreements • Conduct arms control • Routines of interaction on behalf of U.S. citizens and the U.S. government, especially via embassies	• Persuade European countries to purchase alternative to Chinese 5G • Strengthen cohesion of alliances against economic and political coercion	• Sue for peace and/or terms of surrender • Invoke collective defense (Article V) • Build warfighting coalition
Informational	• "Free and Open Indo-Pacific" narrative • NATO Article V messaging • Watching conflict indicators	• Overt support to democracy movements and free press abroad • Engagement, including regulatory, with US press and social media platforms on foreign influence • Putting up safeguards around U.S. electoral processes to protect against interference	• Distribute images of adversary troops crossing international border • Issue joint statement of allied resolve • Public and backchannel messaging to known adversary
Military	• Exercise freedom of navigation • Build allied interoperability	• Flexible deterrent options against "little green men" • Stepped-up efforts at foreign internal defense	• Execute military operations to deny, defeat, or otherwise achieve established objectives
Economic	• Negotiate trade agreement • International development assistance	• Cyber defense regulations • Mechanisms to facilitate private sector reporting on foreign economic coercion to law enforcement	• Blockade • Wartime lend/lease-style support to allies

regulating gray zone competition;

8. Ensure a healthy and reliable system of alliances; and
9. Diversify and grow America's foreign policy toolkit beyond conventional military power and economic sanctions.

Each requires detailed follow-on planning, with leadership and direction orchestrated by national security leaders in the U.S. government. Downstream efforts would begin with the creation of key milestones for execution, many of which can be derived from the analysis provided in this chapter. Responsible departments or agencies would be assigned, and measures of effectiveness would be established against which progress can be monitored and assessed. Figure II incorporates these priority areas into specific steps the United States could potentially take to counter the gray zone threat.

Unfortunately, the CSIS study team assesses that the U.S. government today is unlikely to implement this or any other strategic framework for achieving U.S. aims in the face of gray zone tactics. The report's concluding chapter reviews the reasons for this assessment. It also sets forth the foundations for *By Other Means: Part II*, which will provide recommendations on U.S. government design changes aimed at making campaign planning for the gray zone a reality.

4 FROM PLAN TO PLANNING

Campaign planning cannot be effective if it is rigid. Elements of the preceding campaign framework are likely to grow stale as the United States and other actors in the gray zone learn and adapt their techniques and adjust related strategies. For instance, should the United States improve its warning systems and agility to respond, it may lessen China's incentives to pursue quasi-military approaches to territorial expansion in the air and maritime domains. At the same time, other actors will themselves be adapting to U.S. behavior, to lessons learned by others, and to evolving opportunities in methods and means. The possibility also exists for interactive opportunism, or even coordination and collaboration among other states, which may so profoundly challenge the international influence line of effort as to require a wholesale rethinking of how the United States engages the rest of the world.

In its findings on the U.S. approach to gray zone planning (Chapter 2), the CSIS study team identified the lack of a campaign mindset as a major deficiency. The United States must therefore ensure a dynamic and enduring approach to the gray zone. Doing so will require effective continual assessment and feedback and an adjusted action loop. As an Army campaign planning handbook cautions, "The operational design effort never ceases in a dynamic environment."[156] A campaign mindset is needed to continually reassess the plan's assumptions and approaches, searching for shifts within and among them that would argue for an altered course.

It is here—in moving from *plan* to *planning*—that the U.S. government is likely to encounter its greatest challenge. Strategic planning has long posed a serious challenge for the United States national security enterprise, as has been observed in multiple independent assessments. The *9/11 Commission Report* found that "throughout the government, nothing has been harder for officials—executive or legislative—than to set priorities, making hard choices in allocating limited resources."[157] Similarly, CSIS found in its 2005 *Beyond Goldwater-Nichols* report that differences in institutional culture and language is a hinderance to strategic planning: "When the same words and ideas mean different things to different agencies, coordination and cooperation are difficult at best."[158] The official 2012 *3D Planning Guidebook* for coordinating policy between the State Department, the Department of Defense, and the U.S. Agency for International Development (USAID) found that difficulties arose in part because there was no framework "for interagency communication and collaboration in planning."[159] Effective adaptation to the contemporary strategic environment demands that the United States stop admiring its planning deficiencies and instead begin to address them. If U.S. adversaries are able to conduct campaigns in the gray zone, surely Washington can rise to the challenge.

CAMPAIGNING: REFORM IMPERATIVES

CSIS's forthcoming *Beyond Other Means: Part II* report will provide recommendations for priority adjustments to government organization, policies, authorities, and tools needed to implement the campaign planning framework above and better position it to anticipate and respond to competitors' gray zone tactics through a virtuous campaign planning cycle. The study team's analysis to date suggests the following reform imperatives:

Intelligence

The United States must do a better job recognizing competitive campaigns from the weak signals of many gray zone tactics. It must not just pace competitors but outpace them. For the intelligence community, this requires deep understanding of foreign leaders' motives and psychologies, societal and international dynamics, and the technologies underpinning the modern digital era. For the private sector, this means maintaining the inputs necessary for innovation while remaining cognizant of the risks posed by gray zone activity in an interconnected, global economy. For policymakers, this necessitates setting strategic priorities to focus intelligence collection, with iterative feedback mechanisms to adjust focus as gray zone competitors adapt. With more information accessible than ever before, human analysts must be augmented through algorithmic techniques. There are simply not enough humans to analyze the vast amounts of data returned through intelligence collection. Further, while mechanisms to confound and deceive have always existed, new techniques, such as deep fake technology, may not be recognizable to the naked human eye and require machine assistance. Successful employment of secure artificial intelligence and machine learning systems can help analysts in quickly identifying new patterns in data and inferring intent through synthesis with the traditional intelligence disciplines. The interactive effects of various actors' tactics, especially how they are learning from and perhaps collaborating with one another, is another area for improved warning.

Moreover, the ways that rivals learn from their own uses of gray zone tactics is an important area for U.S. intelligence gathering.

Strategic Campaigning

Warning is fruitless in the absence of effective policy. The United States can best improve its gray zone campaigning by systematically building and synchronizing the employment of U.S. power across its many dimensions, including public and private and domestic- and foreign-facing. Moreover, clarifying responsibilities and speeding quality decisionmaking—even a decision for inaction—would provide the United States a critical advantage prior to and during crises. It creates a window for clear assurance and deterrence signaling, a second attribute of effective decisionmaking processes. Clarity of signals can in turn promote dialogue and, in the event of miscalculation, de-escalation dynamics, including by a third party.

A compelling narrative, timely communication, and effective mediums . . . are vital to deterring and responding to gray zone tactics, as well as campaigning effectively in the space between peace and war.

Narrative

The United States must treat information as a critical domain of statecraft. Such a shift is long overdue. In the Cold War, the United States wrestled with an ideological challenge to the tenets of world order established in the wake of World War II. During the so-called Global War on Terror, U.S. leaders spoke of the "war of ideas" that pitted the ideology of al Qaida against the notion of individual freedom inherent in the U.S. model of democracy. Today, the ties that bind U.S. citizens to each other and the community of nations together are under threat, from autocratic states and transnational movements as well as weaknesses in U.S. societies. Gray zone misinformation and information exploitation tactics are particularly insidious in fraying these ties. A compelling narrative, timely communication, and effective mediums—public and private; governmental and civil society; and for domestic and international audiences—are vital to deterring and responding to gray zone tactics, as well as campaigning effectively in the space between peace and war. Overseas, public diplomacy must include programs aimed at undermining competitors' efforts to manipulate and control media, undermine free markets, and suppress political freedoms. Though the overarching narrative based on U.S. strengths and value should be enduring, the United States will need to continually reassess supporting messages, mechanisms, and domestic and international audiences. The centerpiece of any such communications strategy should be U.S. transparency and truthfulness, reinforcing the model of governance and international conduct it espouses.

Inducements

U.S. national security investments are heavily weighted toward punitive tools, especially traditional military capabilities and sanctions. These capabilities are important, and improved deterrence and coercion mechanisms are needed. Nevertheless, the United States can advantage itself in gray zone interactions as much from its ability to attract third parties as to directly thwart competitors. The U.S. government must revitalize its tools of suasion. This centers around a revitalized State Department but also includes alliances and efforts to bring the private sector and civil society into accord on U.S. interests and the strategy to defeat gray zone threats to them. Positive tools of economic statecraft will be critical, particularly the ability to attract U.S. business and potential partners overseas with effective development and trade inducements.

Cyber

Cyber is a particularly pernicious source of gray zone activity, given the lack of norms, the high number of ac-

tors, and the mix of public and private, domestic and foreign, and national and international elements. Both defensive and offensive in nature, cyber operations move far beyond the speed of human decisionmaking and thus require robust anticipatory repertoires of conduct and attribution. Keeping pace with rapidly-evolving capabilities in the cyber domain must be a central concern for adapting U.S. government authorities, policies, and organizations if the United States is to advance its interests in the presence of gray zone tactics.

CONCLUSION

Improving the U.S. gray zone game may only address a portion of the strategic competition challenge, but it is an important one. Although competition is spanning the spectrum of international interactions, from routine statecraft to nuclear deterrence, it is in the gray zone where the United States has adapted the least, despite ample demonstration by others that they are adapting and in ways that could have lasting strategic effect. Failing to attend to the strategic importance of these tactics imperils U.S. ability to advance its citizens' safety, security, and prosperity. Using a campaign framework, the CSIS study team has created a foundation for deeper planning along particular threat vectors, whether regionally or functionally derived. The campaign plan design also helps highlight the architecture and ways in which the U.S. government will need to adapt its approach to strategy if it is to succeed.

The campaign planning framework presented above should not be considered a "unified field theory" for strategic competition or even an immutable set of principles and priorities for gray zone action. Nor is the campaign plan a substitute for further in-depth planning related to the use of various tools, such as economic policy and information operations, or against various competitors, be it China or Iran. Rather, its intent is to prioritize and synchronize current U.S. efforts to exploit opportunities in the space between peace and war and minimize risk from gray zone tactics present today and projected in the near-future.

ABOUT THE AUTHORS

Kathleen Hicks is senior vice president, Henry A. Kissinger Chair, and director of the International Security Program at CSIS. Dr. Hicks is a frequent writer and lecturer on U.S. foreign and security policy; defense strategy, forces and budget; and strategic futures. She previously served in the Obama administration as the principal deputy under secretary of defense for Policy and the deputy under secretary of Defense for Strategy, Plans, and Forces. She led the development of the 2012 Defense Strategic Guidance and the 2010 Quadrennial Defense Review. She also oversaw Department of Defense contingency and theater campaign planning. From 2006 to 2009, Dr. Hicks was a senior fellow in CSIS's International Security Program. Prior to that, she spent almost thirteen years as a career official in the Office of the Secretary of Defense, rising from Presidential Management intern to the Senior Executive Service. She holds a PhD in political science from the Massachusetts Institute of Technology, an MPA from the University of Maryland, and an AB magna cum laude from Mount Holyoke College. Dr. Hicks is concurrently the Donald Marron Scholar at the Kissinger Center for Global Affairs, Johns Hopkins School of Advanced International Studies and is a member of the Council on Foreign Relations. Dr. Hicks served on the National Commission on the Future of the Army and the Commission on the National Defense Strategy and currently serves on the board of advisors for the Truman Center and SoldierStrong. She is the recipient of distinguished service awards from three secretaries of defense and a chairman of the Joint Chiefs of Staff, the 2011 DOD Senior Professional Women's Association Excellence in Leadership Award, and the National Capital-Area Political Science Association's 2018 Walter Beach Award, for strengthening the relationship between the worlds of political science and public service.

Alice Hunt Friend is a senior fellow in the International Security Program at the Center for Strategic and International Studies (CSIS), where she focuses on African security issues and American civil-military relations. From 2012 to 2014, she was the principal director for African affairs in the Office of the Under Secretary of Defense for Policy, where she focused primarily on North and West African counterterrorism policy. She joined the Department of Defense in 2009 as special assistant to the under secretary of defense for Policy and also served as the senior adviser to the deputy under secretary of defense for Strategy, Plans, and Forces and as country director for Pakistan. She has held previous research positions at CSIS and the Center for a New American Security in Washington, D.C. and has worked at the International Labor Organization in Geneva and with the Senegalese Association for Research, Study, and Aid to Development. Ms. Friend is a doctoral candidate at American University's School of International Service, where she focuses on the civil-military relations of special operations, unmanned systems, and cyber warfare. She is a term member of the Council on Foreign Relations and holds a master's degree in international relations from American University and a bachelor's degree in government from Smith College.

Joseph Federici is a research associate and program manager with the International Security Program at the Center for Strategic and International Studies (CSIS), where he works on a variety of project pertaining to geopolitics, national security, and defense matters. Mr. Federici also assists in coordinating the CSIS Military Fellows program. He holds a JD from Rutgers University School of Law and a BA in history and political science from Rutgers University. Most recently, he graduated, with distinction, from Georgetown University with an MS in foreign service.

Hijab Shah is a research associate with the International Security Program at CSIS. She graduated from Georgetown University's School of Foreign Service with a master's degree in security studies in 2016 and a bachelor's degree in culture and politics in 2011. She was a postgraduate exchange student at the Center for the Study of Terrorism and Political Violence at the University of St. Andrews.

Megan Donahoe is a research assistant with the International Security Program at CSIS, where she supports a variety of projects pertaining to geopolitics, U.S. security and defense matters, and gray zone competition. She holds a master's degree in Eastern European history and a bachelor's degree in international relations, with specializations in international security and Europe and Russia, both from Stanford University.

Matthew Conklin is a research intern with the International Security Program at the Center for Strategic and International Studies (CSIS), where he provides research assistance on projects relating to national security and defense issues. He holds a master's degree in international relations from the University of Chicago and a bachelor's degree in history from Wichita State

University. Following his internship at CSIS, Mr. Conklin will return to the University of Chicago to pursue a PhD in political science with a concentration in international relations.

Asya Akca is a program manager with the Defense-Industrial Initiatives Group at CSIS. She was previously an intern with the International Security Program. Prior to joining CSIS, she worked as a research assistant at the Chicago Project on Security and Threats from 2015 to 2017. She holds a master's degree in international relations and a bachelor's degree in political science both from the University of Chicago.

Michael Matlaga was a research associate with the International Security Program at CSIS, where he specialized in NATO and European defense policy issues. He received his master's degree in security policy studies from the George Washington University's Elliott School of International Affairs and his bachelor's degree in public policy from the University of Chicago.

Lindsey Sheppard is an associate fellow with the International Security Program at CSIS, where she supports various projects in emerging technology, including artificial intelligence and machine learning, and in security applications, ranging from strategic to tactical. Ms. Sheppard contributes expertise in modeling and simulation, system architecture, electronic warfare, and radar from five years of experience in defense research and development. Before joining CSIS, she was a member of the technical staff at the Charles Stark Draper Laboratory and the Georgia Tech Research Institute, during which time she served as the systems engineering lead on multiyear efforts building simulation capabilities to evaluate technology and deployment solutions to support military operations. She holds an MS and a BS in aerospace engineering from the Georgia Institute of Technology.

Endnotes

1 Kathleen Hicks, John Schaus, and Michael Matlaga, *Zone Defense: Countering Competition in the Space between War and Peace* (Washington, DC: Center for Strategic and International Studies, 2018), 1, https://csis-prod.s3.amazonaws.com/s3fs-public/181126_Gray_Zone_Defense.pdf?eWmJQKXLsrQcRT0Y.JIO2mJKkASbfGdX.

2 Department of Defense, *National Defense Strategy* (Washington, DC: 2017), 2, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

3 Hannah Beech, "China's Sea Control Is a done Deal, 'Short of War With the U.S.'," *New York Times*, September 20, 2018, https://www.nytimes.com/2018/09/20/world/asia/south-china-sea-navy.html.

4 Sheera Frenkel, Kate Conger, and Kevin Rose, "Russia's Playbook for Social Media Disinformation Has Gone Global," *New York Times*, January 31, 2019, https://www.nytimes.com/2019/01/31/technology/twitter-disinformation-united-states-russia.html.

5 Kathleen Hicks et al., *Deterring Iran after the Nuclear Deal* (New York, NY: Rowman & Littlefield, 2017), IX, 26, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170313_Hicks_DeterringIran_Web.pdf?GwRM-1vOIS4wvH67bb359MogE8MWl2DJg.

6 Leekyung Ko, "North Korea as a Geopolitical and Cyber Actor," New America, June 6, 2019, https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/north-korea-geopolitical-cyber-incidents-timeline/; Jung Pak, "Regime insecurity or regime resilience?" Brookings Institute, January 17, 2018, https://www.brookings.edu/research/regime-insecurity-or-regime-resilience-north-koreas-grand-strategy-in-the-context-of-nuclear-and-missile-development/.

7 DoD, *National Defense Strategy*, 2.

8 Ibid.

9 "Sharp Power: Rising Authoritarian Influence," National Endowment for Democracy, December 5, 2017, https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/.

10 Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018), 6, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf.

11 Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: United States Army War College Press, 2015), 58, https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1303.

12 Nathan Freier et al., *Outplayed: Regaining Strategic Initiative in the Gray Zone* (Carlisle, PA: United States Army War College Press, 2016), xiii, https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1325.

13 Christopher Walker, "What is 'Sharp Power'?" *Journal of Democracy* 29, no. 3 (2018): 9-23.

14 Hicks, Schaus, and Matlaga, *Zone Defense*, 2.

15 Ibid.

16 Nancy Bermeo, "On Democratic Backsliding," *Journal of Democracy* 27, no. 1 (January 2016), 5–19; See also Steven Levitsky and Daniel Ziblatt, *How Democracies Die* (New York: Crown, 2018).

17 Steven Levitsky and Lucan Way, *Competitive Authoritarianism: Hybrid Regimes After the Cold War* (New York: Cambridge University Press, 2010).

18 "Freedom in the World 2019: Democracy in Retreat," Freedom House, 2019, 18-19, https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.

19 Although not the focus of this report, the CSIS study team assesses that the United States will need to improve its conventional and strategic capabilities if it is to continue deterring modernizing competitors from risking war against it.

20 The definitions for the gray zone toolkit are derived from previous CSIS work. Please see Schaus et al., "What Works: Countering Gray Zone Coercion," CSIS, *CSIS Briefs*, July 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180716_Schaus_WhatWorks.pdf?_2N5GlQNzTKzXCXELkLmjNOhXI8fyMSg.

21 Asia Maritime Transparency Initiative, "China Island Tracker," Center for Strategic and International Studies, https://amti.csis.org/island-tracker/china/#Spratly%20Islands.

22 .S. Library of Congress, Congressional Research Service, *China's Actions in South and East China Seas: Implications for U.S. Interests – Background and Issues for Congress*, by Ronald O'Rourke, R42784 (2019), https://fas.org/sgp/crs/row/R42784.pdf.

23 Beech, "China's Sea Control Is a Done Deal, 'Short of War With the U.S'."

24 Ibid.

25 U.S.–China Economic and Security Review Commission, *2018 Report to Congress* (Washington, DC: November 2018), https://www.uscc.gov/sites/default/files/annual_reports/2018%20Annual%20Report%20to%20Congress.pdf.

26 Department of Defense, *Assessment on U.S. Defense Implications of China's Expanding Global Access* (Washington, DC: December 2018), https://media.defense.gov/2019/Jan/14/2002079292/-1/-1/1/EXPANDING-GLOBAL-ACCESS-REPORT-FINAL.PDF.

27 William Pacatte, *Be Afraid? Be Very Afraid? – Why the United States Needs a Counterstrategy to China's Belt and Road initiative* (Washington, DC: CSIS, October 2018), https://defense360.csis.org/be-afraid-be-very-afraid-why-the-united-states-needs-a-counterstrategy-to-chinas-belt-and-road-initiative/.

28 DoD, *Assessment on U.S. Defense Implications of China's Expanding Global Access*.

29 Brian Harding, "China's Digital Silk Road and Southeast Asia," CSIS, *Commentary*, February 15, 2019, https://www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia.

30 James Andrew Lewis, "Issue the Executive Order," CSIS, *Commentary*, March 29, 2019, https://www.csis.org/analysis/issue-executive-order.

31 Zack Cooper, *Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare* (Washington, DC: Foundation for Defense of Democracies, September 2018), https://www.fdd.org/wp-content/uploads/2018/09/REPORT_China_CEEW.pdf.

32 Ibid.

33 See, e.g., Harold, Scott, Martin Libicki, and Astrid Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica, CA: RAND, 2016), https://www.rand.org/pubs/research_reports/RR1335.html; Ellen Nakashima, "Chinese breach data of 4 million federal workers," Washington Post, June 4, 2015, https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html?noredirect=on&utm_term=.728218fe5b48; Jonathan Cheng and Josh Chin, "China Hacked South Korea Over Missile Defense, U.S. Firm Says," Wall Street Journal, April 21, 2017, https://www.wsj.com/articles/chinas-secret-weapon-in-south-korea-missile-fight-hackers-1492766403?mod=article_inline; Catherine Theohary, "Information warfare: Issues for Congress," Congressional Research Service, March 5, 2018, https://fas.org/sgp/crs/natsec/R45142.pdf.

34 Fireeye iSight Intelligence, *Redline Drawn: China Recalculates Its Use of Cyber Espionage* (Milpitas, CA: June 2016), https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf. Importantly, this study also concludes that internal initiatives by President Xi Jinping also contributed to the downturn in cyber activity. It states: "We attribute the changes we have observed among China-based groups to factors including President Xi's military and political initiatives, widespread exposure of Chinese cyber operations, and mounting pressure from the U.S. Government."

35 The White House, National Cyber Strategy (Washington, DC: 2018),https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; DoD, *Summary: Department of Defense Cyber Strategy* (Washington, DC: 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

36 The White House, National Cyber Strategy.

37 U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Washington, DC: 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

38 Mike Pence, "Vice President Mike Pence's Remarks on the Administration's Policy Toward China," Hudson Institute, October 4, 2018, https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018; Aaron Mehta, "In testimony, Shanahan underlines it's 'China, China, China'," DefenseNews, March 14, 2019, https://www.defensenews.com/pentagon/2019/03/14/in-testimony-shanahan-underlines-its-china-china-china/.

39 Nicole Perlroth, "Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies," *New York Times*, February 18, 2019, https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html.

40 Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2019* (Washington, DC: CSIS, April 2019), 11, https://www.csis.org/analysis/space-threat-assessment-2019.

41 Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC: January 2019), https://www.dia.mil/

Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

42 Michael R. Gordon and Jeremy Page, "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says," *The Wall Street Journal*, April 9, 2018, https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320.

43 Ibid.

44 Neil MacFarquhar, "Inside the Russian Troll Factory: Zombies and Breakneck Pace," *New York Times*, February 18, 2018, https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html.

45 Barbara Surk, "Serb Nationalist Claims Victory in Bosnia in Early Vote Count," *New York Times*, October 7, 2018, https://www.nytimes.com/2018/10/07/world/europe/bosnia-elections-dodik.html; Helen Cooper and Eric Schmitt, "U.S. Spycraft and Stealthy Diplomacy Expose Russian Subversion in a Key Balkans Vote," *New York Times*, October 9, 2018, https://www.nytimes.com/2018/10/09/us/politics/russia-macedonia-greece.html; Michael Birnbaum, "Russia's Low Cost Influence Strategy Finds Success in Serbia," *Washington Post*, October 3, 2018, https://www.washingtonpost.com/world/europe/russias-low-cost-influence-strategy-finds-success-in-serbia--with-the-help-of-fighter-jets-media-conspiracies-and-a-biker-gang/2018/10/03/49dbf48e-8f47-11e8-ae59-01880eac5f1d_story.html?utm_term=.2f2b10e6a1b5.

46 Harrison, Johnson, and Roberts, *Space Threat Assessment 2019*, 11–24.

47 Ellen Nakashima, "U.S. Cyber Force Credited with Helping Stop Russia from Undermining Midterms," *Washington Post*, February 14, 2018, https://www.washingtonpost.com/world/national-security/us-cyber-force-credited-with-helping-stop-russia-from-undermining-midterms/2019/02/14/ceef46ae-3086-11e9-813a-0ab2f17e305b_story.html?utm_term=.7442be99689e.

48 The White House, *National Cyber Strategy*; The White House, "Presidential Policy Directive – United States Cyber Incident Coordination," July 26, 2016, https://fas.org/irp/offdocs/ppd/ppd-41.html.

49 "Global Engagement Center," U.S. Department of State, https://www.state.gov/r/gec/.

50 Nathan A. Sales, "Countering Iran's Global Terrorism," U.S. Department of State, November 13, 2018, https://www.state.gov/countering-irans-global-terrorism/; Brian Katz, "Axis Rising: Iran's Evolving Regional Strategy and Non-State Partnerships in the Middle East," CSIS, *CSIS Briefs*, December 05, 2018, https://www.csis.org/analysis/axis-rising-irans-evolving-regional-strategy-and-non-state-partnerships-middle-east.

51 J. Matthew McInniss, "Proxies: Iran's Global Arm and Frontline Deterrent," in Hicks et al., *Deterring Iran After the Nuclear Deal*.

52 Ibid.; Babak Dehghanpisheh, "The Secretive Commander of Iran's Elite Quds Force Is Flexing His Muscle at Home," Business Insider, March 5, 2019, www.businessinsider.com/revolutionary-guards-commander-flexes-political-muscle-2019-3; Seth G. Jones, "War by Proxy: Iran's Growing Footprint in the Middle East," CSIS, *CSIS Briefs*, March 2019, 4-5, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190312_IranProxyWar_FINAL.pdf.

53 Michael Connell, "Close Quarters Provocations: Iran's Naval Strategy in the Gulf," in Hicks et al., *Deterring Iran After the Nuclear Deal*.

54 Michael S. Schmidt, "9 in Navy Disciplined Over Iran's Capture of Sailors," *New York Times*, June 30, 2016, https://www.nytimes.com/2016/07/01/world/middleeast/us-navy-iran.html.

55 Jack Stubbs, "Special Report: How Iran Spreads Disinformation around the World," Reuters, November 30, 2018, www.reuters.com/article/us-cyber-iran-specialreport-idUSKCN1NZ1FT; FireEye Intelligence, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East," August 21, 2018, https://www.fireeye.com/blog/threat-research/2018/08/suspected-iranian-influence-operation.html.

56 Daniel R. Coats, "2019 Worldwide Threat Assessment," ODNI Home, January 29, 2019, www.odni.gov/index.php/newsroom/congressional-testimonies/item/1947-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

57 Ibid.

58 Michael Eisenstadt, "Information Warfare: Centerpiece of Iran's Way of War," in Hicks et al., *Deterring Iran After the Nuclear Deal*.

59 Ibid.

60 Harrison, Johnson, and Roberts, *Space Threat Assessment 2019*, 25–29.

61 Kayhan Barzegar, "The Trump Administration's Terrorist Label Is Strengthening the IRGC," Atlantic Council, April 15, 2019, https://www.atlanticcouncil.org/blogs/iransource/the-trump-administration-s-terrorist-label-is-strengthening-the-irgc; Suzanne Maloney, "What both Trump and his critics get wrong about the IRGC terrorist designation," Brookings Institution, April 11, 2019, https://www.brookings.edu/blog/order-from-chaos/2019/04/11/what-both-trump-and-his-critics-get-wrong-about-the-irgc-terrorist-designation/; Afshon Ostovar, "Designating Iranian military unit a 'terrorist organization' will make U.S. relations with Iran more difficult. Here's how." *Washington Post*, April 8, 2019, https://www.washingtonpost.com/politics/2019/04/08/designating-irgc-terrorist-organization-will-make-us-relations-with-iran-more-difficult-heres-how/.

62 Michael Connell, "Close Quarters Provocations: Iran's Naval Strategy in the Gulf," in Hicks et al., *Deterring Iran After the Nuclear Deal*; Nicole Bauke, "Why Did Iran Stop Harassing U.S. Navy Ships?" *Navy Times*, January 31, 2018, www.navytimes.com/news/your-navy/2018/01/31/why-did-iran-stop-harassing-us-navy-ships/; Gordon Lubold, and Nancy A. Youssef, "Iran's Fast Boats Stop Harassing U.S. Navy, Baffling Military," *Wall Street Journal*, January 26, 2018, https://www.wsj.com/articles/irans-fast-boats-stop-harassing-u-s-navy-baffling-military-1516897301; DoD, "Department of Defense Press Briefing on the Navy," May 2, 2018, dod.defense.gov/News/Transcripts/Transcript-View/Article/1511123/department-of-defense-press-briefing-on-the-navy/; Summer Said, Nancy A. Youssef, and Benoit Faucon, "U.S. Says Iran Likely Behind Ship Attacks," Wall Street Journal, May 13, 2019, https://www.wsj.com/articles/saudi-oil-tankers-attacked-before-entering-persian-gulf-11557725971.

63 Michael R. Pompeo, "Confronting Iran: The Trump Administration's Strategy," U.S. Department of State, October 15, 2018, www.state.gov/secretary/remarks/2018/10/286751.htm; Iran Action Group, "Outlaw Regime: A Chronicle of Iran's Destructive Activities," U.S. Department of State, 2018, https://www.state.gov/documents/organization/286410.pdf.

64 Hijab Shah and Sarah Minot, "The Art of Unraveling the Deal," CSIS, *Commentary*, May 10, 2019, https://www.csis.org/analysis/art-unraveling-deal; "Six Charts That Show How Hard US Sanctions Have Hit Iran," BBC News, May 2, 2019, https://www.bbc.com/news/world-middle-east-48119109.

65 Katie Lange, "What Is the National Defense Strategy?" DoD, October 8, 2018, https://www.defense.gov/explore/story/Article/1656414/what-is-the-national-defense-strategy/.

66 Shah and Minot, "The Art of Unraveling the Deal"; Ghassan Adnan, "U.S. Embassy Staff to Leave Iraq as Iran Tensions Mount," *Wall Street Journal*, May 15, 2019, https://www.wsj.com/articles/u-s-embassy-staff-told-to-leave-iraq-amid-iran-tensions-11557910345.

67 James Andrew Lewis et al., *North Korea's Cyber Operations: Strategy and Responses* (Washington, DC: CSIS, November 2015), https://www.csis.org/analysis/ executive-summary-north-koreas-cyber-operations-strategy-and-responses; Emma Chanlett-Avery et al., "North Korean Cyber Capabilities: In Brief," Congressional Research Service, August 3, 2017, https://fas.org/sgp/crs/row/R44912.pdf.

68 Chanlett-Avery et al., "North Korean Cyber Capabilities."

69 Nicole Perlroth, "As Trump and Kim Met, North Korean Hackers Hit Over 100 Targets in U.S. and Ally Nations," *New York Times*, March 3, 2019, https://www.nytimes.com/2019/03/03/technology/north-korea-hackers-trump.html?rref=collection%2Ftimestopic%2FNorth%20Korea.

70 Keith Bradsher and Choe Sang-Hun, "With Kim's Visit, China Shows U.S. It Has Leverage on Trade," *New York Times*, January 8, 2019, https://www.nytimes.com/2019/01/08/business/china-north-korea-kim-trade.html; Jung Pak, "Kim Jong-un's tools of coercion," Brookings Institution, June 21, 2018, https://www.brookings.edu/blog/order-from-chaos/2018/06/21/kim-jong-uns-tools-of-coercion/.

71 Keith Bradsher and Choe Sang-Hun, "With Kim's Visit, China Shows US It Has Leverage on Trade," *New York Times*, January 8, 2019, https://www.nytimes.com/2019/01/08/business/china-north-korea-kim-trade.html.

72 Daniel Moss, "With Friends Like the U.S., Who Needs Economic Foes?" Bloomberg Opinion, May 22, 2019, https://www.bloomberg.com/opinion/articles/2019-05-23/japan-south-korea-get-reminder-of-how-powerful-china-s-economy-is.

73 Choe Sang-Hun, "Trump Supports Food Aid for North Korea, South Says," *New York Times*, May 7, 2019, https://www.nytimes.com/2019/05/07/world/asia/trump-north-korea-food-aid.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

74 Jung Pak, "Kim Jong-un's tools of coercion," Brookings Institution, June 21, 2018, https://www.brookings.edu/blog/order-from-chaos/2018/06/21/kim-jong-uns-tools-of-coercion/.

75 U.S. Department of Defense, *A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year*

2012: Military and Security Developments Involving the Democratic People's Republic of Korea 2017 (Arlington, VA: DOD, 2017), 9.

76 Lisa Collins, "25 Years of Negotiations and Provocations: North Korea and the United States," CSIS Beyond Parallel, https://beyondparallel.csis.org/25-years-of-negotiations-provocations/.

77 Harrison, Johnson, and Roberts, *Space Threat Assessment 2019*, p. 33.

78 Missile Defense Project, "North Korean Missile Launches & Nuclear Tests: 1984-Present," Missile Threat, Center for Strategic and International Studies, April 20, 2017, last modified May 10, 2019, https://missilethreat.csis.org/north-korea-missile-launches-1984-present/.

79 Anabelle Liang, "South Korea Urges Restraint After Recent North Korea Missile Tests," *TIME*, June 1, 2019, http://time.com/5599415/south-korea-north-korea-missile-test/.; Donald Trump, Twitter post, May 4, 2019, 6:42 a.m., https://twitter.com/realDonaldTrump/status/1124670603179565056.

80 Liang, "South Korea Urges Restraint After Recent North Korea Missile Tests."; Zachary Cohen, "Shanahan breaks with Trump over North Korea missile test," CNN, May 29, 2019, https://www.cnn.com/2019/05/29/politics/shanahan-north-korea-missile-test-un-violation/index.html.

81 Maggie Haberman, "Sarah Sanders Says Trump and Kim 'Agree in Their Assessment' of Biden," May 26, 2019, https://www.nytimes.com/2019/05/26/us/politics/sarah-sanders-meet-the-press.html?searchResultPosition=17.

82 Victor Cha and Katrin Fraser Katz, "The Right Way to Coerce North Korea: Ending the Threat Without Going to War," *Foreign Affairs* 97, no. 3 (May-June 2018), https://www.foreignaffairs.com/articles/north-korea/2018-04-01/right-way-coerce-north-korea.

83 Cho Yi-jun, "U.S. Treasury Issues Alert on Financial Dealings with N. Korea," *Chosun Ilbo*, March 13, 2019, http://english.chosun.com/site/data/html_dir/2019/03/13/2019031301218.html; Choe Sang-Hun, "Sanctions Are Hurting North Korea. Can They Make Kim Give In?" *New York Times*, April 20, 2018, https://www.nytimes.com/2018/04/20/world/asia/north-korea-trump-sanctions-kim-jong-un.html; Sangmin Lee, Leejin Jun, and Eugene Whong, "Russian Shipping Company Accused of Doing Business With North Korea Hard-Hit by U.S. Sanctions," Radio Free Asia, December 13, 2018, https://www.rfa.org/english/news/korea/gudzon-sanctions-12132018160613.html.

84 Thomas P. Bossert, "It's Official" North Korea is Behind WannaCry," *Wall Street Journal*, December 19, 2017, https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

85 Choe Sang-Hun, "North Korea Hits a Man With Glasses," New York Times, April 20, 2019, https://www.nytimes.com/2019/04/20/world/asia/north-korea-john-bolton.html?rref=collection%2Ftimestopic%2FNorth%20Korea.

86 Koh Byung-joon, "N. Korea calls for replacing Pompeo with 'more careful and mature' negotiator," Yonhap News Agency, April 18, 2019, https://en.yna.co.kr/view/AEN20190418008851325?section=nk/nk; John Walcott, "Trump's Go-It-Alone Strategy on North Korea Led to a White House Fight," TIME, April 25, 2019, http://time.com/5576489/kim-jong-un-vladimir-putin-donald-trump/.

87 Sue Mi Terry and Lisa Collins, "Assessment of the Trump-Kim Hanoi Summit," CSIS, *Critical Questions*, February 28, 2019, https://www.csis.org/analysis/assessment-trump-kim-hanoi-summit; Phil Stewart and Idrees Ali, "U.S., South Korea suspend more drills to bolster North Korea diplomacy," Reuters, October 19, 2018, https://www.reuters.com/article/us-usa-northkorea-wargames/u-s-south-korea-suspend-more-drills-to-bolster-north-korea-diplomacy-idUSKCN1MT25Y.

88 "U.S., South Korea to scale back large-scale spring military exercises," *Japan Times*, March 2, 2019, https://www.japantimes.co.jp/news/2019/03/02/asia-pacific/u-s-south-korea-scale-back-large-scale-spring-military-exercises/#.XMG1g2hKjcs.

89 Ibid.

90 Lee Min-hyung, "Kim Jong-un arrives in Vladivostok for summit with Putin," *Korea Times*, April 24, 2019, http://www.koreatimes.co.kr/www/nation/2019/04/356_267718.html; Jon Herskovitz and Dandan Li, "China, North Korea Open New Border Crossing Despite Sanctions," Bloomberg, April 8, 2019, https://www.bloomberg.com/news/articles/2019-04-08/china-north-korea-open-new-border-crossing-despite-sanctions; See also Eleanor Albert, "The China-North Korea Relationship," Council on Foreign Relations, March 13, 2019, https://www.cfr.org/backgrounder/china-north-korea-relationship.

91 Vladimir Isachenkov, "Russian President Putin Hosts Kim Jong Un for Talks on North Korean Nuclear Standoff," *TIME*, April 25, 2019, http://time.com/5577801/vladimir-putin-kim-jong-un-meeting-russia/.

92 Timothy W. Martin and Na-Young Kim, "North Korea's New Strategy: Be Passive-Aggressive," *Wall Street Journal*,

April 20, 2019, https://www.wsj.com/articles/north-koreas-new-strategy-be-passive-aggressive-11555690033.

93 Although a useful illustration for this report's purposes, the authors believe representing international relations along a two-dimensional spectrum oversimplifies how actors employ various means—often across a range of intensities—in support of their objectives.

94 Office of the Director of National Intelligence, "A Guide to Cyber Attribution," September 14, 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

95 "Policy Planning Staff Memorandum," National Archives and Records Administration, May 4, 1948, https://www.archives.gov/research/guide-fed-records/groups/273.html.

96 "Prospects and Priorities for U.S. Gray Zone Competition," CSIS, November 27, 2018, https://www.csis.org/events/2018-global-security-forum-prospects-and-priorities-us-gray-zone-competition.

97 Joseph S. Nye, "Protecting Democracy in an Era of Cyber Information War," Belfer Center Paper, Belfer Center for Science and International Affairs, January 2019, 7, https://www.belfercenter.org/sites/default/files/files/publication/ProtectingDemocracy.pdf.

98 , "How the World Sees the U.S. and its President in 9 Charts," Pew Research Center, October 9, 2018, graph 9, https://www.pewresearch.org/fact-tank/2018/10/09/how-the-world-views-the-u-s-and-its-president-in-9-charts/.

99 See, for example, Barry R. Posen, "Pull Back: The Case for a Less Activist Foreign Policy," *Foreign Affairs* 92, no. 1 (January/February 2013), 116-128.

100 Michael Beckley, "The Myth of Entangling Alliances," *International Security* 39, no. 4 (Spring 2013); See Hal Brands and Peter D. Feaver, "What are America's Alliances Good For?" *Parameters* 47, no. 2 (Summer 2017), 16-30.

101 Kathleen Hicks, "Now What? The American Citizen, World Order, and Building a New Foreign Policy Consensus," *Texas National Security Journal* 1, no. 2 (November 2017), https://tnsr.org/2017/11/now-american-citizen-world-order-building-new-foreign-policy-consensus/.

102 The White House, *National Security Strategy of the United States*, 4.

103 Donald Trump popularized this phrasing during the 2016 election, but many politicians and analysts across the political spectrum have picked up on its viral appeal in the intervening years, applying the sentiment to everything from the Electoral College to college admissions. One analyst wrote, "The anger is bipartisan, although the lists of suspected villains differ"; Steve Denning, "Why 'The System' is Rigged and the U.S. Electorate is Angry," Forbes, January 23, 2016, https://www.forbes.com/sites/stevedenning/2016/01/23/why-the-system-is-rigged/#20d14593feac. Denning's piece was triggered by a 2016 *Esquire*/NBC News survey entitled, "American Rage," that found that 78 percent of surveyed Americans believed "elected officials generally enact policies that favor the interests of the wealthy," https://www.esquire.com/news-politics/a40693/american-rage-nbc-survey/; See also Joseph E. Stiglitz, "The American Economy is Rigged: And What we Can Do About It," *Scientific American*, November 1, 2018, https://www.scientificamerican.com/article/the-american-economy-is-rigged/?redirect=1.

104 David Brooks, "It's Not the Collusion, It's the Corruption," *New York Times*, April 18, 2019, https://www.nytimes.com/2019/04/18/opinion/mueller-report-corruption.html.

105 Suzanne E. Spaulding, *Countering Adversary Threats to Democratic Institutions* (Washington, DC: CSIS, February 2018), https://www.csis.org/analysis/countering-adversary-threats-democratic-institutions.

106 For more on the Defending Democratic Institutions Project, see https://www.csis.org/programs/international-security-program/defending-democratic-institutions.

107 Suzanne E. Spaulding and Harvey Rishikof, "How Putin Works to Weaken Faith in the Rule of Law and Our Justice System," Lawfare Blog, September 17, 2018, https://www.lawfareblog.com/how-putin-works-weaken-faith-rule-law-and-our-justice-system.

108 Alexis De Tocqueville, *Democracy in America* (London: Saunders and Otley, 1835).

109 Brice McKeever, "The Nonprofit Sector," National Center for Charitable Statistics, January 3, 2019, https://nccs.urban.org/project/nonprofit-sector-brief.

110 "Volunteering in U.S. Hits Record High; Worth $167 Billion," The Corporation for National and Community Service, November 13, 2018, https://www.nationalservice.gov/newsroom/press-releases/2018/volunteering-us-hits-record-high-worth-167-billion.

111 National Commission on Military, National, and Public Service, *Interim Report* (Washington, DC: January 2019), p. 13, https://www.inspire2serve.gov/NCOS%20Interim%20Report.pdf.

112 "How Did U.S. Students Perform on the Most Recent Assessments?" The Nation's Report Card, 2017, https://www.nationsreportcard.gov.

113 On suspected underreporting in SEC filings, see Eamon Javers, "Cyberattacks: Why Companies Keep Quiet," CNBC, February 25, 2013, https://www.cnbc.com/id/100491610.

114 Laura Sullivan, "As China Hacked, U.S. Businesses Turned a Blind Eye," National Public Radio, April 12, 2019, https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye.

115 The White House, *National Cyber Strategy of the United States*, 10–11.

116 Scott Shane and Mark Mazzetti, "The Plot to Subvert an Election: Unraveling the Russia Story So Far," *New York Times*, September 20, 2018, https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html.

117 "Time Flies: U.S. Adults Now Spend Nearly Half a Day Interacting with Media," Nielsen Media, July 31, 2018, https://www.nielsen.com/us/en/insights/news/2018/time-flies-us-adults-now-spend-nearly-half-a-day-interacting-with-media.html.

118 John T. Bennett, "Trump attacks media, says N.Y. Times should 'beg for forgiveness'," *Roll Call*, April 23, 2019, https://www.rollcall.com/news/whitehouse/trump-attacks-media-says-n-y-times-should-beg-for-forgiveness; David Siders and Stephanie Murray, "Nunes declares war on the media," Politico, July 18, 2018, https://www.politico.com/story/2018/07/18/devin-nunes-fresno-bee-newspaper-attacks-731032; Morgan Gstalter, Morgan, "Trump labels New York Times report on business losses a 'highly inaccurate Fake News hit job'," *Politico*, May 8, 2019, https://thehill.com/homenews/administration/442640-trump-labels-new-york-times-report-on-business-losses-a-highly.

119 James Andrew Lewis, "Cognitive Effect and State Conflict in Cyberspace," CSIS, *Commentary*, September 26, 2018, https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace.

120 Ben Bernanke, "China's gold star," Brookings Institution, December 1, 2015, https://www.brookings.edu/blog/ben-bernanke/2015/12/01/chinas-gold-star/.

121 Benjamin Cohen, "The Future of Reserve Currencies," International Monetary Fund, September 2009, https://www.imf.org/external/pubs/ft/fandd/2009/09/pdf/cohen.pdf; Judy Shelton, "The Case for a New International Monetary System," CATO Journal (Spring/Summer 2018), https://www.cato.org/cato-journal/springsummer-2018/case-new-international-monetary-system.

122 Christopher Smart, "The Future of the Dollar – and Its Role in Financial Diplomacy," Carnegie Endowment for International Peace, December 16, 2018, https://carnegieendowment.org/2018/12/16/future-of-dollar-and-its-role-in-financial-diplomacy-pub-77986.

123 Jonathan Masters, "What are Economics Sanctions?" Council on Foreign Relations, August 7, 2017, https://www.cfr.org/backgrounder/what-are-economic-sanctions; Alex Capri, "Why U.S. Sanctions Are So Lethal," *The Diplomat*, February 23, 2018, https://thediplomat.com/2018/02/why-us-sanctions-are-so-lethal/.

124 Neil Bhatiya and Edoardo Saravalle, "America Is Addicted to Sanctions. Time for an Intervention," *Atlantic*, August 5, 2018, https://www.theatlantic.com/international/archive/2018/08/when-sanctions-go-too-far/566771/.

125 Ibid.

126 "The Benefits of International Trade," U.S. Chamber of Commerce, https://www.uschamber.com/international/international-policy/benefits-international-trade.

127 "Free Trade Agreements," Department of Commerce, https://www.trade.gov/fta/.

128 Andrew Schwarzenberg, "U.S. Trade with Major Trading Partners," Congressional Research Service, December 18, 2018, https://fas.org/sgp/crs/row/R45434.pdf.

129 Congressional Research Service, "U.S. Trade Policy Primer: Frequently Asked Questions," January 29, 2019, 34, https://fas.org/sgp/crs/row/R45148.pdf.

130 Edward Alden, "Trump and the TPP: Giving Away Something for Nothing," Council on Foreign Relations, January 23, 2017, https://www.cfr.org/blog/trump-and-tpp-giving-away-something-nothing.

131 The White House, *The Economic Benefits of U.S. Trade* (Washington, DC: May 2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/cea_trade_report_final_non-embargoed_v2.pdf.

132 Congressional Research Service, "U.S. Trade Policy Primer: Frequently Asked Questions," January 29, 2019, 2, https://fas.org/sgp/crs/row/R45148.pdf.

133 Congressional Research Service, "Foreign Aid: An Introduction to U.S. Programs and Policy," April 16, 2019, https://fas.org/sgp/crs/row/R40213.pdf.

134 U.S. Global Leadership Coalition, *America's Global Economic Leadership* (Washington, DC: July 2017), https://www.usglc.org/downloads/2017/07/USGLC-Americas-Global-Economic-Leadership-July-2017.pdf.

135 Daniel Runde and Romina Bandura, "The BUILD Act Has Passed: What's Next?" CSIS, *Critical Questions*, October 12, 2018, https://www.csis.org/analysis/build-act-has-passed-whats-next.

136 Ibid.

137 Ibid.

138 Ibid.

139 Samuel Brannen, "Bad Idea: Expecting the Private Sector to Drive Innovation in National Security," Defense 360, November 30, 2018, https://defense360.csis.org/bad-idea-expecting-the-private-sector-to-drive-innovation-in-national-security/.

140 Michele Flournoy and Gabrielle Chefitz, "Here's How the United States Can Keep Its Technological Edge," Foreign Policy, February 25, 2019, https://foreignpolicy.com/2019/02/25/heres-how-the-united-states-can-keep-its-technological-edge-trump/#.

141 Zack Cooper, "Understanding the Chinese Communist Party's Approach to Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, September 2018, https://www.fdd.org/wp-content/uploads/2018/09/REPORT_China_CEEW.pdf.

142 Ibid.

143 Michael Ratner et al., "21st Century U.S. Energy Sources: A Primer," Congressional Research Service, November 5, 2018, https://fas.org/sgp/crs/misc/R44854.pdf; Robert Blackwill and Jennifer Harris, *War by Other Means: Geoeconomics and Statecraft* (Cambridge, MA: The Belknap Press of Harvard University Press, 2016), 214.

144 Blackwill and Harris, *War by Other Means*, 216.

145 Ibid., 217.

146 Ibid., 217; Peter Ford "U.S. seeks energy 'dominance.' But is that a shield against geopolitical risks?" *Christian Science Monitor*, February 22, 2018, https://www.csmonitor.com/World/2018/0222/U.S.-seeks-energy-dominance.-But-is-that-a-shield-against-geopolitical-risks.

147 Ronald Deibert, "The Road to Digital Unfreedom: Three Painful Truths about Social Media," *Journal of Democracy* 30, no, 1 (January 2019): 25-39.

148 Heather A. Conley et al., *The Kremlin Playbook 2: The Enablers* (Washington, DC: CSIS, 2019).

149 Kathleen Hicks et al., *Counting Dollars or Measuring Value: Assessing NATO and Partner Burden Sharing* (Washington, DC: CSIS, 2018), https://www.csis.org/analysis/counting-dollars-or-measuring-value.

150 See Conley, *Kremlin Playbook 2* for detailed recommendations on how to shore up Russian exploitation of gaps in European and American finance.

151 Although not the focus of this study, it is important to note that U.S. advantages in vertical escalation to warfighting are also eroding and must be improved.

152 Traditionally horizontal escalation was defined only in this last way—an approach that expands geographic scope. The broader definition provided here is more useful in understanding modern conflict.

153 For a detailed discussion of escalation and deterrence, see Michael Green et al., "Countering Coercion in Maritime Asia: The Theory and Practice of the Gray Zone," (Washington DC: Center for Strategic and International Studies, 2017).

154 Department of Defense, *National Defense Strategy* (Washington, DC: 2017), 5, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

155 National Defense Strategy Commission, *Providing for the Common Defense* (Washington, DC: September 2018), 19, 22-23, 44, https://media.defense.gov/2018/Oct/03/2002047941/-1/-1/1/PROVIDING-FOR-THe-COMMON-DEFENSE-SEPT-2018.PDF.

156 Col, Mark Haseman ed., *Campaign Planning Handbook: Academic Year 2016* (Carlisle Barracks, PA: Army War College, 2019), p. 28, https://ssi.armywarcollege.edu/PDFfiles/PCorner/CampaignPlanningHandbook.pdf.

157 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: July 2004), https://www.9-11commission.gov/report/911Report.pdf.

158 Clark A. Murdock and Michele A. Flournoy, *Beyond Goldwater Nichols: U.S. Government and Defense Reform for a New Strategic Era* (Washington, DC: CSIS, 2005).

159 DoD, DoS, and USAID, *3D Planning Guide: Diplomacy, Development, Defense* (Washington, DC: July 2012), https://www.usaid.gov/sites/default/files/documents/1866/3D%20Planning%20Guide_Update_FINAL%20%2831%20Jul%2012%29.pdf.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.csis.org

ROWMAN & LITTLEFIELD

Lanham • Boulder • New York • London

Rowman & Littlefield
4501 Forbes Boulevard
Lanham, MD 20706
301-459-3366 | www.rowman.com