AUGUST 2019

A REPORT
OF THE CSIS
INTERNATIONAL
SECURITY
PROGRAM

BY OTHER MEANS

PART II: ADAPTING TO COMPETE IN THE GRAY ZONE

PROJECT DIRECTORS

Kathleen H. Hicks
Melissa Dalton

AUTHORS

Melissa Dalton
Kathleen H. Hicks
Megan Donahoe
Lindsey Sheppard
Alice Hunt Friend
Michael Matlaga
Joseph Federici
Matthew Conklin
Joseph Kiernan

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

The views, opinions, and/or findings contained in this report are those of the authors and should not be construed as an official Department of Defense position, policy, or decision.

AUGUST 2019

A REPORT
OF THE CSIS
INTERNATIONAL
SECURITY
PROGRAM

BY OTHER MEANS

PART II: ADAPTING TO COMPETE IN THE GRAY ZONE

PROJECT DIRECTORS

Kathleen H. Hicks
Melissa Dalton

AUTHORS

Melissa Dalton
Kathleen H. Hicks
Megan Donahoe
Lindsey Sheppard
Alice Hunt Friend
Michael Matlaga
Joseph Federici
Matthew Conklin
Joseph Kiernan

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: 978-1-4422-8127-1 (pb); 978-1-4422-8128-8 (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

Objectives

CSIS proposes to catalogue U.S. tools for gray zone competition, highlight opportunities to refine or develop new tools, and recommend changes (if any) to policy, authorities, organization, and processes to improve effective use of U.S. capabilities to deter, compete, deny, or prevail in gray zone competitions. By so doing, CSIS aims to provide recommendations to assist policymakers and commanders in responding to gray zone challenges in a more coordinated fashion.

Specifically, the study will answer five questions:

1. What is the nature of the current gray zone challenge? Are there patterns of activity within or across actors or regions? What elements pose the greatest challenge to U.S. interests?
2. What agencies have responsibility for a U.S. response to gray zone challenges, and under what policies, organizational arrangements, and/or legal authorities do they operate?
3. How can intelligence, and especially geospatial intelligence and information, be collected, analyzed, and applied to better identify and enable the United States to more actionably anticipate and respond to emerging gray zone challenges?
4. What gaps, if any, exist with respect to processes, organization, authority, operation, or other aspects of effective U.S. identification of, and response to, gray zone challenges?
5. How can the United States government better organize itself to identify, prepare for, and respond to gray zone challenges around the world?

Based on the research and analysis to answer these five questions, the study will present options, and where possible, recommendations, that could be implemented to improve how the United States leverages sources of geospatial information and intelligence, including through conceiving of new frameworks to identify, assess, and ultimately counter current and future gray zone challenges. Integrating possible new ways of thinking about intelligence with improved policy and operational tools could lead to better outcomes against gray zone challengers seeking to exploit U.S. weaknesses.

Contents

Acknowledgments

The research team hopes that this report's findings and analysis can inform reforms within the U.S. government to enable it to better compete in the gray zone.

The authors are grateful to John Schaus for his insights throughout the project. We also relied on the expertise of many other CSIS colleagues, including Seth Jones, Todd Harrison, Haim Malka, Heather Conley, James Andrew Lewis, Jon Alterman, Matt Goodman, Michael Green, Rachel Ellehuus, Lieutenant Colonel Kurt Leffler, Brian Katz, Hijab Shah, Thomas Roberts, Kaitlyn Johnson, Pearl Risberg, Dylan Gerstel, Arthur Nelson, and Joseph Haberman for their research insights. Rebecka Shirazi and Jeeah Lee did an outstanding job managing the publication process.

Over 85 U.S. government and military officials as well as regional and functional security experts provided insights to shape and inform this study's research findings and recommendations. We especially thank Zack Cooper, John McLaughlin, Benjamin Schmitt, and CSIS's Suzanne Spaulding, each of whom went above and beyond the call of duty to help us understand key aspects of this complex issue set. The authors alone are responsible for the report's findings and recommendations and any errors in fact, analysis, or omission.

This report is made possible by support from the U.S. Department of Defense. It has been completed under a U.S. Department of the Army, U.S. Army Corps of Engineers, Army Geospatial Center contract number W5J9CQ18C0005 (CDRL A003).

BY OTHER MEANS

PART II: ADAPTING TO COMPETE IN THE GRAY ZONE

Geopolitical competition is increasingly playing out in the space beyond diplomacy and short of conventional war, sometimes referred to as the *gray zone*. The nature of this competition is forcing the United States to confront the liabilities of its strengths. This report assesses current U.S. government actions to deter, campaign through, and respond to competitors' gray zone tactics. Using the campaign planning framework established in *By Other Means Part I*, the report provides recommendations aimed at ameliorating American liabilities and building on its asymmetries to improve U.S. national security in the presence of rivals' gray zone approaches.

Dynamically Campaign along Interests-Based Lines of Effort

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

Priority Recommendations to Advance U.S. Government Campaigning

Strategic Action and Oversight: Build and synchronize the employment of U.S. power, and speed quality decision-making to improve signaling and risk management.

- Issue a gray zone presidential decision directive outlining a dynamic campaign approach and the supporting executive branch elements described herein.
- Designate a National Security Council (NSC) senior director, along with supporting intelligence-operations task force and senior interagency coordination mechanism, to drive efforts.
- Demonstrate bipartisan congressional leadership with rapid information sharing and solution generation on issues crossing multiple committee stovepipes.
  - Expand the membership of the Senate's bipartisan National Security Working Group to strengthen representation and linkages across domestic security, foreign, and defense committees.
  - Create a similarly scoped, staffed, and resourced bipartisan House National Security Working Group.

Intelligence and Warning Systems: Recognize campaigns from weak signals, including rivals' intent, capability, impact, interactive effects, and impact on U.S. interests.

- Designate a national intelligence officer for gray zone threat fusion, leveraging the capabilities of the National Counterterrorism Center, Cyber Threat Information Integration Center, and other-like bodies.
- Revitalize an "active measures working group," focused on covert action aspects of campaigning.

Strategic Communications and Narrative: Designate information as a critical domain of statecraft, with the NSC senior director for gray zone assigned to lead coordination efforts across domestic and international communication spheres.

- Deepen investments and expectations in domestic (Department of Homeland Security (DHS)) and overseas (Department of State) strategic narratives and misinformation reporting.
- Improve the Federal Bureau of Investigation and DHS reporting mechanisms for the private sector, universities, political campaigns, and the general public to access hotlines and public service announcements in the event of threats.

- Promote civic education and media literacy best practices and associated Department of Education grant opportunities; promote civics education in the Department of Defense's Education Activity schools.
- Regulate social media consistent with First Amendment principles, including establishing a social media oversight board, like the Privacy and Civil Liberties and Oversight Board, tasked with evaluating social media algorithms, misinformation, and disinformation based on common guidelines or policies.

National Cyber Capabilities: Buttress national cyber capabilities.

- Designate a cyber coordinator on the NSC staff to facilitate interagency collaboration and deconfliction.
- Create a code of conduct for U.S. cyber operations.
- Authorize and fully resource DHS's Election Task Force and federal assistance to election security.
- Develop capabilities for offensive cyber operations focused on deterrence against and defense of U.S. territory and institutions.

Coalition Building and Third-Party Inducements: Advance coalitions across borders and sectors, spanning public and private, as well as foreign and domestic, divides.

- Improve mechanisms to collaborate, share information, and develop coordinated approaches with the private sector at home and allies and partners abroad.
- Strengthen and expand inducements to allies and partners overseas, including through trade agreements, security cooperation, and targeted investment.
- Spur private sector security innovation at home through federal research and development investment, smart immigration policies, and incentives to reduce societal vulnerabilities.

1 INTRODUCTION

With requisite political leadership, the United States has the capacity to ameliorate the liabilities of its strengths. U.S. rivals are successfully preying upon its vulnerabilities, presenting challenges that often manifest over time and across regions and sectors. In prior points of crisis, whether in the Cold War or after September 11, 2001, the United States has shown an ability to adapt its government organization, policies, authorities, and tools to prevail in its aims. The United States now faces a similar critical test for its national security. Today's competition of interests is often playing out in a place beyond diplomacy and short of conventional war, which some experts refer to as the *gray zone*. Too often, rivals are gaining an advantage at the expense of U.S. interests, catching the United States off-guard and probing the agility of the U.S. toolkit.

The Center for Strategic and International Studies (CSIS) study team uses the following definition for gray zone challenges:

> *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.*

The 2017 National Security Strategy and 2018 National Defense Strategy make clear that competition against capable nation-states will be a central feature of the U.S. security landscape for the foreseeable future.[1] The coercive tools used by these 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 includes seven main areas:

- *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 decision-making 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 and 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.

In the course of surveying contemporary state-based gray zone challenges, the CSIS study team found that four countries conduct the lion's share of concerning activities. China, Russia, Iran, and North Korea all leverage gray zone tools to varying degrees of success, either directly against the United States or against U.S. allies, partners, and interests. Of these actors, China is the most concerning, followed by Russia, given the breadth and quality of each examined state's toolkit and their relative potential effects on U.S. interests.

The phenomenon of the gray zone is not new or unique.[2] Today, however, the approach has been adopted widely by U.S. competitors, and it is manifesting in significant threats to national security. The United States possesses a wealth of diplomatic, informational, economic, and military potential. However, competition in the gray zone is an underdeveloped area of U.S. strategy, planning, and synchronization of action.

In 2018, CSIS embarked on two-part project, *By Other Means*, to research, assess, and propose a new approach to buttress U.S. competitiveness in the gray zone. CSIS's *Beyond Other Means Part I* report proposed a concrete and actionable campaign plan in the gray zone for: protecting the U.S. constitutional system and the U.S. way of life; promoting the nation's economic vitality; and advancing U.S. influence. In turn, this companion report provides recommendations for priority adjustments to national security tools, authorities, policies, and organizations needed to implement the first study's campaign planning framework and better position the United States to anticipate and respond to competitors' gray zone tactics.

A CAMPAIGN PLAN FOR THE GRAY ZONE

Advancing U.S. interests in the face of competitors' known and projected gray zone tactics begins with building a U.S. playbook. CSIS's *By Other Means Part I* sets out such a strategic campaigning approach. The key features of the campaign plan are summarized here.

Mission Statement:

The United States will seek advantages in gray zone competition that bolster its national security interests. It will also seek to undermine competitors' gray zone tactics, from deterrence to effective campaigning to crisis response.

Key Assumptions:

- Campaign planning must be dynamic to be effective. Actors will adapt and opportunities will emerge.
- Concepts such as "winning" and "losing" will have less salience than measures of relative gain and loss, as assessed over time.
- U.S. laws, principles, and values are strategic *advantages* in gray zone competition. Even as the United States engages in gray zone tactics, it should do so in accordance with its principles.

NEXT UP: IMPROVING U.S. GOVERNMENT PERFORMANCE

Executing the campaign plan described above requires effective tools, authorities, policies, and organization to boost U.S. government (USG) performance. The CSIS study team conducted a 12-month analytic effort to catalogue the gray zone tools rivals use to advance their interests at the expense of the United States. The analysis informed the campaign plan design and the study team's assessment of how well-positioned the U.S. government is to execute it. This report builds upon its companion to detail the key aspects of that assessment and provides attendant recommendations for changes that will better enable the United States to deter, cam-

Priority Lines of Effort

- Protect U.S. constitutional tenets and the U.S. way of life.
    - Protect U.S. electoral processes, its judicial systems, and the legitimacy of its governance model.
    - Invest in national service models, civics education, and media literacy.
    - Strengthen social media regulation, respecting precedent on U.S. citizens' First Amendment rights.
- Promote the nation's economic vitality.
    - Maintain a healthy 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, Asia, and Africa.
    - Help U.S. businesses defend against cyber and economic coercion and rally their soft power, including through investments in U.S. innovation.
- Advance U.S. influence.
    - Strengthen international norms and their enforcement; develop new norms for constraining and regulating gray zone competition.
    - Ensure a healthy and reliable system of alliances.
    - Diversify and grow America's foreign policy toolkit beyond conventional military power and economic sanctions.

paign through, or respond to competitors' use of gray zone tactics. In so doing, the report aims to aid U.S. policymakers in advancing the nation's strategic interests.

The CSIS study team analyzed numerous prior studies on gray zone competition, assessments of national security organizational reform, and interviews with experts and practitioners drawn from policy, operational, intelligence, and other relevant communities. The CSIS study team also convened three stakeholder working group meetings and a private dinner discussion with senior experts to discuss, validate, and refine its analysis. Finally, it undertook three case study assessments to inform its consideration of reform proposals.

The main body of this report is organized into three parts. The next four chapters (Chapters 2 through 5) delineate how the seven gray zone tools described above threaten U.S. interests domestically and abroad, explore the key U.S. government players involved in addressing them, detail an assessment of those players' capabilities, and finally, offer an assessment of U.S. government performance versus those tools. Chapter 2 outlines the dangers of information threats and disinformation to U.S. and allied institutions and systems. Chapter 3 explores how political and economic coercion damage U.S. interests. Chapter 4 details cyber and space threats from U.S. rivals. Chapter 5 concludes the examination of gray zone tools with a focus on disguised forces, including proxy and state-controlled groups.

Chapter 6 highlights where U.S. government reform is needed in responding to and proactively addressing competitors' gray zone activities. These gaps also reflect *By Other Means Part I*'s findings, which fall in the categories of intelligence, strategic action, coalition building, effective oversight, and investments in strategic narrative and cyber capabilities. Chapter 7 builds on these findings, recommending changes to the U.S. government's organization, authorities, policies, and capabilities to implement the CSIS study team's gray zone campaign plan.

2 THE INFORMATION GAME

THE THREAT

Competitors are using false or biased information from online activity, state-sponsored media outlets, and official statements to break down the authority, legitimacy, and strengths of U.S. norms, values, and institutions. China has established centers like the Confucius Institutes to sponsor "sympathetic" spokespersons to reinforce Chinese Communist Party policies and stifle diverse opinion.[3] Analyst Michael Eisenstadt refers to information operations as a "centerpiece of Iran's way of war."[4] The most dangerous and successful adversary to use information operations against the United States is Russia, which deploys false news and disinformation to confuse and aggravate perceptions of the U.S. government, electoral processes, and political figures, as well as those of its allies and partners. Notoriously, Russia conducted a massive information and disinformation campaign during the 2016 U.S. presidential election.[5] This confusion seeks to damage the U.S. and allied critical infrastructure of democratic processes and economic institutions.

Information operations have proven to be both relatively cheap and effective, making them appealing to a wide range of potential actors who seek to deploy continuous operations. Recently, the Office of the Director of National Intelligence reported that China, Russia, and Iran had all used information operations in an attempt to influence the 2018 U.S. congressional election.[6] Information operations receive an exponential boost when paired with competitors' cyber capabilities, including the ability to mask activity, penetrate protected networks, and evade countermeasures. Moreover, democratic principles around privacy and free speech have created dilemmas for investigating potential information operations and for regulating underlying media platforms.

THE PLAYERS

The Department of Homeland Security (DHS) is engaged in countering foreign influence operations within the United States. Abroad, the Department of State (DoS) is in the lead, with assistance from the U.S. Agency for International Development (USAID). Support for countering information campaigns both within the United States and abroad has been provided by the Department of Justice (DoJ), the Department of Treasury, the Department of Defense (DoD), and the Intelligence Community. In reality, however, there are few USG directives and policies that seek to counter information operations and disinformation, and there is a lack of focus on developing narrative as a key function of U.S. national security policy.

Department of Homeland Security

The only government effort to build domestic resiliency against disinformation and information operations is DHS's Countering Foreign Influence Task Force (CFITF), which is supported by intelligence from the Federal Bureau of Investigation's (FBI) Foreign Influence Task Force. CFITF began operations in March 2018 with a focus on the 2018 U.S. midterm elections. Its main programs have been public awareness and messaging campaigns to build resilience against information operations, as well as to connect vulnerable public, media, and private-sector parties to the correct law enforcement, intelligence, and partners. It coordinates with the FBI as well as the private sector, including through research organizations, civil society organizations, and social media companies.[7]

Department of State

Abroad, the Department of State's Global Engagement Center (GEC) is the lead USG effort abroad to counter information operations that harm U.S. interests, such as U.S. allies and partners. The GEC does this by countering propaganda and disinformation from both state and non-state actors. Created in April 2016 by Executive Order 13721 and subsequently codified in the FY2017 National Defense Authorization Act, the GEC's mandate is to "lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining U.S. national security interests." A careful read of this mandate suggests the GEC could have overarching responsibility for countering malign influence within the United States and abroad, but that role has not been acknowledged or acted upon. It relies upon detailees from across the interagency and consultations with the private sector to staff and synchronize its efforts and to leverage best practices. It focuses on four core areas: science and technology, interagency engagement, partner engagement, and content production.

DoS also protects allies and partners from information operations through traditional soft power operations like targeted aid programs that promote accurate narratives and free and fair media, messaging, and diplomacy. For example, DoS's Energy Bureau addresses Russian disinformation campaigns and information campaigns relating to Nord Stream 2.

U.S. Agency for International Development

USAID has been restructuring its programs to address predatory Chinese development projects and the information operations that support them. USAID's new strategy has tailored programs to counter Chinese educational exchange programs and to support free and fair elections, youth empowerment, democratic governance, and free press. USAID's Russia regional teams have also been compiling a strategy for Russia's information operations. One strong point of USAID's programming is a system of indicators and measurements for a country's vulnerability to foreign influence and information operations. USAID also uses its programming to "name and shame" competitor's malign information operations.

The Office of Transition Initiatives (OTI) within USAID focuses on shorter-term political and violent crisis management that is often aggravated by information operations. With local partners, OTI supports pluralistic, independent media and seeks to bridge ethnic, religious, and political divisions. OTI has uniquely flexible and discretionary funding mechanisms, unlike most USAID programs and offices. USAID also delegates funding authority to their on-the-ground mission leaders, allowing OTI to quickly approve funding for programs that other programming from USAID and State normally could not. Of note, OTI has partnered with social media companies to resolve violent conflicts arising from information operations in sub-Saharan Africa, Eastern Europe, and the Balkans. It also deploys programs that support media literacy and free and fair media.

Department of Justice and Department of Treasury

The DoJ has the lead for investigating and prosecuting attempts at foreign influence within the United States. The FBI is DoJ's investigatory lead. Its Foreign Influence Task Force, established in 2017, draws on long-standing counterintelligence, counterterrorism, and cyber capabilities within the FBI. In addition to conducting investigations and undertaking operations to counter influence, the task force shares intelligence relevant to national security with a broad range of U.S. public- and private-sector entities. For issues pertaining to U.S. electoral integrity, for instance, the Foreign Influence Task Force works closely with DHS's CFITF. Aided by DoJ's investigation and indictments, the Department of Treasury's Office of Foreign Assets Control levies sanctions against foreign information operations.

Department of Defense and Intelligence Community

Over the past five years, the DoD has expanded its offensive capabilities and international partnerships in response to global foreign information operations. DoD has bolstered its internal policy direction to integrate DoD activities with those of other U.S. agencies, allies and partners, and international organizations to support "information strategies and operations to neutralize adversary propaganda and promote U.S. strategic interests."[8] In 2018, the U.S. Special Operations Command was assigned responsibility to create a global Military Information Support Operations (MISO) capability and had plans to stand-up a Joint MISO WebOps Center in 2019 to focus DoD efforts in this space.[9]

With the funding of the European Deterrence Initiative, DoD created the Operational Influence Platform, which engages in Russia counter-messaging.[10] DoD also uses public messaging to name and shame gray zone adversaries like Russia for deploying information operations.[11] Within the North Atlantic Treaty Organization (NATO), the U.S. European Command studies information operations and contributes to research products at the Strategic Communications Center of Excellence.[12] NATO's Cooperative Cyber Defense Center of Excellence conducts yearly Cyber Coalition exercises to study and prepare NATO forces for cyber assaults, which include components of disinformation and social media.[13] U.S. Indo-Pacific Command, or INDOPACOM, is also engaged in information operations to expose the downsides of China's investments in Southeast Asia, including the risk of debt traps.

Both the National Security Agency (NSA), a defense intelligence organization with authorities under Title 50 of U.S. Code, and U.S. Cyber Command (CYBERCOM), an operational military command with authorities under Title 10 of U.S. code, are DoD entities engaged in identifying and countering digital age information operations. The differences in their authorities are important. NSA is "charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes."[14] As a Title 50 organization, it can conduct covert signals intelligence operations abroad when directed to do so, such as to thwart attempts at foreign influence. As a Title 10 warfighting entity, CYBERCOM has been focused on executing missions for the military, such as efforts to counter the Islamic State on the ground in Syria.[15]

It appears that NSA and CYBERCOM have made significant strides to combat information operations.[16] Exactly how either organization engages in U.S. efforts to counter disinformation is cloaked in secrecy. With a strategy of "persistent engagement" and direct messaging, enabled by offensive capabilities authorized by the National Security Presidential Memo-13, CYBERCOM reportedly directly engages foreign information and cyber penetration operations.[17] Late in 2018, a member of Congress credited CYBERCOM with being "actively involved" in preventing Russian information campaigns from affecting election outcomes.[18]

The Russia Influence Group

Created at the initiative of DoS and DoD and operating with Title 22 and 10 authority, the Russian Influence Group (RIG) is an interagency platform where U.S. agencies can coordinate and share information about programs and strategies to counter Russian influence in Europe. It began with traditionally internationally engaged agencies like DoS, DoD, and USAID, and since then, membership has expanded to non-traditional partners like DoE, the Treasury Department, and DoJ. With this platform of structured discussions, U.S. agencies can avoid program duplication as well as recommend new avenues of support by sharing agency toolkits. Although the RIG is relatively new, this innovative model of coordination and information sharing can serve as a model for other U.S. agencies concerned with gray zone challenges.

ASSESSMENT OF U.S. GOVERNMENT PERFORMANCE

The United States has yet to formulate a synchronized and coherent approach to counter information operations targeting U.S. interests at home and abroad.[19] U.S. narratives that seek to expose the dangers adversarial political and market cultures pose to liberal democratic culture have been largely ineffective thus far due to the lack of integration across multiple arms of government. China and Russia have already made significant progress in damaging the perceptions and legitimacy of U.S. and allied and partner institutions.

Though U.S. agencies have publicly highlighted the dangers information operations pose to U.S. democratic institutions, there is no unified strategy from the White House or at the national level to coordinate which agencies should respond to these threats and how.[20] This lack of direction has forced agencies to adapt and create programs on an ad hoc basis without consolidated direction or measures of progress. Moreover, current U.S. government posture on information operations is largely reactive.

Currently, it is up to members of the U.S. public and private sector to take responsibility for the information and media they consume and promote. There are few incentives to evaluate sources and quality of information, to learn media literacy, or to identify disinformation attempts and stop their proliferation.

Policies

One overarching weakness in U.S. policy responses versus information operations is the lack of serious strategy devoted to this gray zone activity. The National Security Strategy acknowledges information operations as a threat to U.S. national security but does not indicate any new or stronger recommendations for responses. The strategy explains it will be "risk informed, but not risk averse, in considering our options," but its priority actions on information statecraft rely on traditional efforts like diplomacy and counter-narrative campaigns, with no indications of innovation or integration within the broader U.S. toolkit.[21]

On the domestic front, notwithstanding efforts by the intelligence and law enforcement communities,[22] the U.S. government has issued weak and inconsistent statements on the dangers of foreign information and disinformation operations on U.S. territory and institutions. Senior administration officials have been slow to acknowledge the interference and severity with which these operations threaten U.S. and international democratic institutions. The 2018 National Security Strategy includes no mention of how Russia manipulated the U.S. electoral system.[23] As a result, Americans do not have a clear and unified sense of the danger of these gray zone threats.

Further constraining domestic efforts to counter disinformation is the appropriate need to ensure protection of Americans' First Amendment rights. There is no administration policy regarding the possible regulation of social media, which prevents progress in the needed conversation over security needs and personal liberties in this space.

Overseas, DoS is struggling to address information operations as a department. Although allies and partners, especially Baltic members of NATO like Estonia, have made significant strides to bolster defenses to disinformation and information operations, DoS has been unable to apply lessons learned from allies and partners, most notably with respect to social media. For instance, for structural and societal reasons, the United States does not have the same culture of encouraging change by private social media companies or insisting on civilian data protections as the European Union. As a result, there are few incentives for social media companies to recognize and openly address the damage of information operations and enact change to mitigate their negative consequences.

When prioritizing and evaluating information threats, DoS has been largely reactionary. Regional and functional bureaus do not have a formalized process of identifying indicators and warnings of vulnerability, nor are there many measurements of success or progress. Although the National Security Strategy places clear priority on competing with China and Russia, DoS has made Iran the GEC's highest priority. Exacerbating these challenges, the U.S. administration's blunt pressure on European allies to burden share and fund their own defenses has eroded U.S. political ability to forge consensus and a common approach with allies, although collaboration at the technocratic level remains strong. Adding to these difficulties, DoS's GEC reportedly funded a counter disinformation platform that, unbeknownst to the GEC, trolled human rights advocates, scholars, and journalists that the group deemed too sympathetic to the government of Iran.[24] The GEC discontinued funding the platform once the trolling was flagged by other analysts on Twitter in June 2019. The incident highlighted a gap in vetting and oversight processes. Given that information is an underdeveloped tool of statecraft, DoS may not have sufficient staffing, resources, and know-how to scale-up the strategic information campaign the United States needs.

USAID programs have suffered from misalignment and de-prioritization in U.S. policy. Historically, USAID promotes programs and operational strategies that emphasize multilateral approaches. The Trump administration's emphasis on unilateral programs has thus adversely affected its efforts because allies and partners perceive less incentive to continue partnerships with the United States or to share information. In addition, lack of access to intelligence regarding competitors' gray zone activities undermines effective planning, as does the lack of alignment or coordination across U.S. agencies on the ground.

The relaxation of operational authority in cyberspace has been an advisable adaptation to the number and speed of threats the United States faces. Engagements such as the shutdown of Russia's Internet Research Agency's internet on the day of the 2018 U.S. midterm elections send important signals about what the United States considers vital to its interests and what it is willing to do to protect those interests. Nevertheless, the escalation dynamics around information operations are not well-tested, and the risks of retaliation are significant.[25] Russia has not shied away from shutting off power grids in Ukraine, and many experts worry Russia would do the same if the United States deploys attributable cyberattacks. Even as the CSIS study team applauds operational agility, it cautions the need for strategic goals and operational activities to be tightly linked.

Sanctions and indictments enforced by DoJ and the Department of Treasury function as the main punitive measures of the U.S. government against information operations. However, their effectiveness in this space is unclear. Current efforts seem to have brought attention and pressure to the issue, elevating the public's awareness of foreign information operations. However, these steps alone have not imposed enough costs on foreign actors to stop their campaigns. The Internet Research Agency continued to meddle with the 2018 U.S. midterm election, and other actors like Iran have begun increasing their own disinformation operations.[26] Sanctions are likely to work best in combination with other tools, such as law enforcement.

Authorities

DHS does not have the authorities needed to lead effectively in developing messages for the American people and countering disinformation at home. DHS's CFITF suffers from having insufficient legislative authority to effectively counter disinformation and information operations on domestic U.S. territory and institutions. The CFITF does not have the institutional purview to address broader information challenges to the nation, including critical infrastructure, or relationships with the private sector. This contrasts with DHS's efforts on cyber security, where the purview and relationships are well-established.

DoS's GEC does have sufficient legal authority from Congress to combat information operations that run counter to U.S. interests abroad. Public diplomacy—creating and promulgating narratives that advance U.S. national security policy—is clearly within the purview of the DoS. Other departments and agencies, including DoD and USAID, have established supporting roles.

Organization, Capabilities, and Resources

DHS's CFITF is hampered by fluctuations in staffing and a lack of resources. Its existent staffing model is project-based, so many employees left the team after the 2018 U.S. midterm elections concluded. Staffing was further diminished by the prolonged government shutdown of 2018. As DHS prepares for the 2020 presidential elections, the CFITF will be re-hiring and on-boarding more staff. However, this inconsistent operating model complicates long-term strategy and planning. Among the strategic elements currently missing are a focused effort to build resiliency and a means of harnessing the U.S. asymmetric advantages of transparency and accountability, such as through partnerships with the spectrum of independent U.S. media outlets.

The GEC faces challenges securing sustained attention and focus within DoS. Regional bureaus have historically overshadowed functional teams like GEC, impairing senior-most attention to areas like information operations that cross country and regional boundaries. Its full funding has only recently become available, and it still faces hurdles in its annual budget and justification process, being reliant upon DoD funds for much of its operations. The GEC's staffing model is also reliant on other actors, namely detailees from across the interagency. It must have the ability to consult deeply with the private sector to staff and synchronize its efforts and to leverage best practices, a task complicated by its orientation toward "main State" activities in Washington, D.C. Despite these challenges, it makes sense to maintain the GEC within DoS rather than be separated as an independent agency, such as the U.S. Information Agency was during the Cold War, in order to better coordinate with other arms of the Department.

Though the GEC was severely impaired by the 2018 shutdown, funding has been accessed, and programs in counter messaging and resiliency have expanded and matured. Despite this progress, the GEC's funding now needs to support programs with speed and flexibility to counter a gray zone tool that is by nature quick to adapt. Relatedly, DoS's Internet Freedom Program, which has the mission to promote internet freedom in countries like Iran, China, and Russia and had made many strides, has faced similar constraints and focuses largely on response mechanisms rather than a proactive approach.[27] Though internet freedom programming continues to be deployed on a country-by-country basis, programming could be expanded to fit the increasing threats that information operations pose to the international system.[28]

The DoS's weak capacity has kept it from leading effectively on public diplomacy and messaging. It has instead relied heavily on USAID, which suffers from relatively small, non-discretionary funding streams stretched across multiple priorities, diminishing their relative effectiveness. The resulting effort and impact are insufficient to the challenge.

Finally, DoS's efforts to curb information operations abroad and DHS's efforts to counter disinformation at home lack systems to identify, measure, and evaluate indicators of information activities, their magnitude, and the success of countermeasures. Only USAID has developed relevant indicators to monitor this gray zone tool. Without strong indicator and warning systems, as well as measurements and evaluations, agencies like DoS and DHS will remain largely reactionary.

3 POLITICAL AND ECONOMIC COERCION

THE THREAT

When competitors use the power of their economic and political influence by coercive means, they limit economic cooperation, undermine liberal democratic institutions, and erode the authority and influence of the United States and its allies in the international system. Competitors are already taking steps to alter the global economy to their advantage. CSIS colleague Heather Conley has written extensively about Russia's use of this strategy in her *Kremlin Playbook* series.[29] Conley explains:

> *In the first Kremlin Playbook report, we detailed what we called an "unvirtuous cycle" of malign influence that the Kremlin uses to influence and direct decision-making in Central and Eastern Europe. It does so through networks of economic and political patronage across the region and follows two tracks: one through economic influence in strategic sectors of a country's economy, which can in turn provide political influence; and the other through political influence, which can later deepen and protect Russian economic influence. Corruption allows both influence tracks to become highly intertwined.*[30]

President Xi Jinping's efforts to expand China's economic and political influence have raised similar concerns, especially his signature economic and foreign policy project, the Belt and Road Initiative (BRI). Coming as it does at a time when the United States has turned away from multilateral treaty initiatives and has asked its allies and partners to pay more into common security, significant Chinese engagement through BRI raises the prospect of undermining other nations' faith in the U.S. economic model, as it increases the credibility of Chinese state-directed capitalism.[31] The U.S. government and many experts believe China might seek these economic ties in part to create leverage that can shape other countries' interests and "deter confrontation or criticism of China's approach to or stance on sensitive issues."[32]

Because China has many state-owned enterprises and considerable influence over the rest, it is able to drive investments and digital controls in emerging markets. Unlike the United States and its allies, China does not pose questions or constraints about the receiving country's governance model or human rights standards. In addition, China's meddling in the private economic sector contrasts with the culture of free and fair enterprise the United States upholds. Furthermore, the global rise of populism and skepticism of global economic institutions also undermines the U.S. government's preferred approach to doing business and its historical reliance on such institutions.

Meanwhile, China's rapid advancements in technology combined with its aggressive market tactics have exposed the United States and other countries to intellectual property theft, debt traps, loss of market competition, cyberattacks, and breaches. With China's "Digital Silk Road" initiative, the installation of fiber-optic cables enables Chinese state-owned or state-affiliated enterprises control over vast amounts of personal, government, and financial data, which could ultimately be used by the Chinese government for leverage or even gains beyond the economic realm.[33] This is made worse by China's aim to lead fifth generation mobile network technology (5G) deployment, where the temptation for low-cost and readily-available 5G technology from companies like Huawei can come at the expense of breaches from Chinese state entities for intelligence gathering purposes. The cumulative effect can be leverage for economic and political coercion, security breaches, and intellectual property theft. The United States has banned Huawei technology from U.S. acquisitions and has urged other countries not to risk security breaches by accepting 5G infrastructure projects from Huawei. However, several allies and partners have continued to accept Huawei projects, in addition to previously incorporated Chinese-made telecommunications equipment. Huawei is estimated to have captured almost 30 percent of the worldwide telecommunications equipment market share as of 2018, and the state-backed company exerts significant pressure on markets founded on free and fair competition.[34] It also increases the risk that Huawei may impose service disruptions and collect intelligence.[35]

Domestically, China poses the main state-based threat of economic coercion to the United States. This takes the forms of unfair business contracts that force intellectual property transfers, sanctions, selective uses of domestic regulations, targeted customs inspections, and extralegal embargoes and boycotts on specific companies, all reinforced by state media and pressure from government officials.[36]

THE PLAYERS

DoS and USAID are the lead U.S. agencies that address foreign political and economic coercion abroad. The new U.S. International Development Finance Corporation (USDFC) will play a key role in helping the United States compete effectively. The Department of Commerce, Department of Treasury, the U.S. Trade Representative (USTR), and other U.S. independent agencies also play critical roles. At home, the FBI has the lead for investigations and law enforcement operations relating to countering foreign economic and political coercion. The Intelligence Community (IC) provides needed support across the range of today's political and economic coercion threats. Finally, Congress has taken particular interest in international development efforts aimed at responding to potential competition or coercion from foreign powers.

Department of State and U.S. Agency for International Development

These agencies have recently reframed their messaging, approaches, and programming to address new forms of coercion, especially those from China and Russia. Both have storied histories from the Cold War in building democracy and social resiliency and supporting free speech, fair media, and free and fair electoral systems. Through the public diplomacy mission, they are equipped to name and shame political coercion.

DoS has used its diplomatic networks and programming to counter political and economic coercion. In January 2019, Secretary of State Michael Pompeo toured the Middle East speaking out against Iran's political coercion.[37] In May, DoS issued a statement condemning Russia's failed coup in Montenegro and praised local Montenegrin courts in their conviction of 14 Russian, Serbian, and Montenegrins for their participation in the coup.[38] DoS programming to counter these types of coercion consists of promoting pro-democratic messaging in partnership with the U.S. Agency for Global Media. By coordinating through the Russian Influence Group (RIG), DoS and DoJ promote rule of law programming in Europe. Because of RIG, DoJ was able to expand their rule of law toolkits to aid in the conviction of those participating in the failed Montenegrin coup.

Concerned with China's development projects, USAID has reframed policy and programs to address a three-part strategy of messaging, programming, and partnerships to promote self-reliance and to counter political coercion. Knowing USAID cannot compete with China's project capacity size, speed of project completion, and funds, USAID has reframed its messaging to portray U.S. programs as offering principled self-reliance and sovereignty , in contrast to Chinese projects, which create corruption, state surveillance, and dangers to religious minorities.[39] USAID has also developed a system of indicators of a nation's vulnerability to political and economic coercion, an important step in better understanding, measuring, and formulating long-term strategies. The Office of Transition Initiatives offers similar programs and strategies with more flexible funds and higher accessibility to hyper-localized local government and civil society partners, though these programs only target priority countries. Such program priorities include: promoting democratic values; preventing violent conflict; identifying and stymieing political and economic exploitation; promoting the rule of law; and supporting free and fair media outlets. USAID and DoS both use diplomacy to name and shame the economic coercive behavior of adversaries like China, including through multilateral forums like the United Nations and the Association of Southeast Asian Nations.[40]

U.S. International Development Finance Corporation

In October 2018, President Trump signed the "Better Utilization of Investments Leading to Development (BUILD) Act" into law to reform U.S. development finance capabilities into a new federal agency. The USDFC will consolidate the capabilities of the Overseas Private Investment Corporation (OPIC) and USAID's Development Credit Authority. It will also offer new financial products to bring private capital to the developing world to drive economic growth, create stability, and improve livelihoods. In parallel, it is intended to boost U.S. competitiveness with China, providing "financially-sound alternatives to state-directed initiatives that can leave developing countries worse off."[41]

Department of Commerce, Department of Treasury, and U.S. Trade Representative

At the Department of Commerce, the Bureau of Industry and Security (BIS) has the mission of preserving "U.S. national security, foreign policy, and economic objectives" through export controls of dual-use goods, treaty compliance systems, and "promoting continued U.S. strategic technology leadership."[42] The BIS uses its dual-use export controls for national security and to "ensure the health of the U.S. economy and the competitiveness of U.S. industry," though striking a balance between the two goals can be difficult.[43]

Recently, Congress passed the Export Controls Act of 2018 which expands presidential power to "implement dual-use export controls."[44] Under the new act, it is the BIS's responsibility to "establish and maintain a list" of items and foreign persons that threaten national security and foreign policy, as well as to monitor and prohibit entry and transfers of these items to the United States.[45] With BIS's authority to maintain U.S. economic vitality, their export controls oversee electronics design development and production, computers, telecommunications, sensors and lasers, aerospace and propulsion, and other goods and technologies vulnerable to economic coercion.[46] In June 2019, BIS aided DoJ in the indictment of an Iranian national for attempting to acquire U.S. aircraft parts, thereby evading Export Administration Regulations, amongst other violations.[47] The BIS expands policy research and private-sector engagements through its Annual Conference on Export Controls. The Conference involves global experts on industry, government, and academia who discuss topics like 5G, artificial intelligence (AI), emerging technology, the Committee on Foreign Investment in the United States (CFIUS), and the Export Control Reform Act of 2018.[48]

The Department of Treasury plays two important roles in countering economic coercion. First, it restricts the export of goods in accordance with U.S. sanction laws.[49] Second, it regulates investments and projects that are potentially harmful to national security through the CFIUS. CFIUS reviews and determines whether certain foreign investments or transactions are a national security concern.[50] The Department of Treasury and broader U.S. agency efforts through the World Trade Organization (WTO) can also seek to punish economic coercion through arbitration and the "naming and shaming" of predatory business practices.

The White House has directed the Department of Commerce and Department of Treasury to impose tariffs on Chinese goods, launching a trade war meant to force China to renegotiate economic norms and practices, as well as to end its unfair business practices.[51]

Through the USTR, the United States and China have a network for economic dialogue as well as a platform for arbitration at the WTO.[52] In 2018, the USTR delivered its most recent report to Congress on the nature of China's WTO compliance.[53]

Department of Justice and the Intelligence Community

DoJ and the Department of Treasury have sought to clarify and expand punishment for coercive economic activity from China and other adversaries, including through indictments of intellectual property theft and other unfair business practices. In October 2018, DoJ, with the investigation aid of the FBI and coordination with Interpol for extradition, arrested and charged a Chinese national for economic espionage and theft of trade secrets from U.S. aviation companies.[54] In December 2018, DoJ, in coordination with the FBI, arrested and charged a Chinese national for committing theft of trade secrets from a petroleum company.[55]

In addition, U.S. stakeholders in the law enforcement and intelligence community have named and shamed malign actors for using research exchanges as opportunities to coerce intellectual property theft. In February 2018 at a Senate intelligence hearing on worldwide threats, FBI Director Christopher Wray spoke out against countries like China that "exploit[t] the very open research and development environment" of "nontraditional collectors, especially in the academic setting, whether it's professors, scientists, students."[56] Because research circles are now vulnerable to national security threats and economic coercion, U.S. government agencies are increasing their oversight of researchers, and exchanges with countries of concern.[57] U.S. policymakers are also proposing legislation and visa restrictions to block foreign student access to sensitive research projects.[58]

The IC also aids DoS and USAID in their investigations of political and economic coercion. In cases of economic coercion, the IC provides intelligence to inform steps to expose foreign states and actors' wrongdoing and to aid investigations and indictments. The IC also conducts intelligence on political coercion and malign influence, including recently for exposing Russian interference in the Prespa Agreement between Greece and North Macedonia in 2018.[59]

Independent Agencies

The Federal Trade Commission (FTC) seeks U.S. consumer protection and promotes fair competition by advancing research and policy. It also prosecutes domestic and foreign businesses in violation of their standards.[60] To protect U.S. industries from economic coercion, the FTC produces policy research and reports to advise the private sector and public consumers about threats to consumer protection and economic competition. The FTC seeks to investigate and fight coercion—by filing suits against companies and people that violate consumer protection laws—enforces antitrust laws, and challenges business mergers and practices that would result in price hikes, hurt competition, and slow innovation.[61] The FTC has diplomatic channels to promote economic resiliency and to speak out against coercion, participating in events like a recent G7 Panel on Digital Innovation and Competition and the Global Antitrust Economics Conference.[62]

The U.S. Securities and Exchange Commission (SEC) has the mandate of protecting investors, ensuring fair markets, and enabling capital formation to ensure economic growth.[63] Punishments for violating SEC laws include trading suspensions, complaints, and litigation.[64] The SEC seeks to protect investors by regulating investments and providing toolkits to the public to ensure rules and regulations are understood.

U.S. Congress

The U.S. Congress passes bills to expand international aid to countries and regions vulnerable to economic coercion, especially from U.S. competitors like China and Russia. Congressional ratification of the Asia Reassurance Initiative Act in December 2018 authorized more funding to DoS, DoD, and USAID. It mandated that the funds would, "ensure that the regulatory environments for trade, infrastructure, and investment in partner countries are transparent, open, and free of corruption" in building trade capacity, increased economic cooperation, and increased regional diplomatic dialogues.[65] The Ukraine Freedom Support Act of 2014 directs the president to work with the World Bank Group, the European Bank for Reconstruction and Development, and other international financial institutions to stimulate public and private investment in Ukraine.[66]

ENERGY COERCION

As a subset of economic coercion, energy coercion has yet to present itself as a direct national security concern to the United States. However, it gravely affects regions like Europe, where Russia's energy markets threaten the security of the region. Because energy coercion has not been accepted as a major concern with consensus across Europe, experts worry U.S. allies and partners have lost significant ground to Russian energy markets.

DoS's Bureau of Energy Resources, working with the DoE, USAID, Department of Treasury, and others, seeks to build the resiliency of friendly states from energy coercion. The bureau has tailored its programs to encourage energy diversity and resilience to counter energy and economic coercion from actors like Russia, which has shut off gas lines to Ukraine, or from Iran, which uses its oil resources as a point of leverage.[67]

USAID has also emphasized programs that improve access to and the diversity of energy markets. Private-sector energy partners have been especially helpful, and USAID plans to continue collaborating in the private sector. USAID uses diplomatic networks to name and shame the energy coercion conducted by adversaries like Russia.

Per the Ukraine Freedom Support Act of 2014, Congress directed OPIC (now to be folded under the USDFC) to support investments in energy diversity, energy efficiency, and renewable energy to counteract Russia's coercive energy practices in the region.[68]

Though DoE historically had few opportunities to work in international energy security, DoE has recently grown its presence, capabilities, and programming to counter energy coercion abroad. Through the RIG, DoE has expanded programs in energy security and diversification in Europe.[69] In its Office of International Affairs, DoE has expanded diplomatic cooperation and partnerships in the international system. In conjunction with USAID, DoE has developed products that support the development of natural gas markets and liquid natural gas (LNG) options in Africa.[70] The Asia Reassurance Initiative Act compels the president to develop a "comprehensive, integrated, multiyear strategy" to build energy markets and reinforce energy security for Asia, to be enforced by DoE.[71] Within the RIG, the Department of Treasury has offered its toolkit in improving allies and partners' sanctions against Russian energy coercion.

ASSESSMENT OF U.S. GOVERNMENT PERFORMANCE

The Trump administration has focused over the past year on efforts to name and shame Chinese economic coercion and to warn and threaten allies and partners away from questionable Chinese activity. Yet these punitive tactics are not well-linked to inducements that would draw allies and partners closer to the United States instead. With the advent of competition surrounding the development of 5G technology and the global overhaul of infrastructure projects, the stakes for U.S. interests are high.[72] Struggles in funding (both in size and flexibility), the lack of interagency coordination, and the disagreements over multilateral versus unilateral solutions have further compounded difficulties in department and agency efforts to reinforce democratic values and a free and fair international economic system.

Policies

The overarching issue in U.S. policy against political and economic coercion is that there is yet to be a strategy to align and sequence action and incorporate not only punitive measures but also inducements. There have been targeted, punitive tariffs aimed at bringing China to the table and negotiating an end to their unfair business practices, but there has not been a proactive drive to demonstrate an alternative U.S. economic and political vision that seeks to compete. A confident United States would be putting forward a significant trade agenda in Europe and Asia, facilitating overseas investment for U.S. business, and otherwise building on the asymmetric advantages of its unparalleled alliance and partner system.[73] Instead, the administration has de-prioritized DoS and USAID programming in these spaces.

Overseas, the president's strongly negative rhetoric about alliances and rejection of multilateral approaches is also an impediment to advancing the U.S. way of life and economic vitality in the face of significant Chinese economic pressure. Local governments and civil society organizations are less willing to partner with the United States on projects relating to political or economic resiliency or to share information versus competitors' actions. European allies and partners disgruntled with U.S. unilateralism have opposed U.S. and NATO calls to diversify their energy markets. Furthermore, existing sanctions efforts, such as those toward Russia, are not fully aligned with broader foreign policy goals and may present blowback risks to development and stabilization efforts.

In addition, neglect of international trade organizations, their trade arbitration capabilities, and multilateral trade arrangements complicate U.S. responses to coercion. While the USTR could have a larger role in deterring unfair Chinese business practices through outlets of arbitration like the WTO, the Trump administration has undervalued the utility of a U.S. presence at the WTO. More broadly, the United States has pulled away from multilateral trade arrangements such as the Trans-Pacific Partnership, while allies and partners have pressed ahead.

On the domestic front, U.S. government efforts to target unfair Chinese business practices within the United States beyond the cyber realm have been met with push back by some U.S. businesses that value Chinese investments. Taken together, these inconsistencies in U.S. policy result in uneven effectiveness in influencing areas where U.S. strengths have the most potential leverage.

Authorities

The lack of authorities and resourcing to better deploy energy resiliency programs in allied and partner countries has hindered DoS's ability to tackle energy coercion, especially in Europe against Russian LNG market dominance. In one instance, DoS stakeholders wanted to give an allied country emergency energy supplies, but the Energy Bureau's authorities were too slow and too hindered by legal structures to quickly respond.

Though the consolidation of OPIC and the Development Credit Authority into the USDFC is a positive step in modernizing and imposing efficiency into the U.S. government's finance and investment toolkits abroad, its deployment has been complicated. One major issue is an undetermined sovereign loan guarantee (SLG) legislative authority. With a limit at $29 billion, SLG had previously been under the purview of DoS, but with a new limit of $60 billion to expand partnerships and programs, SLG is without a designated legislative authority.[74] Likewise, legislative language on equity authority, an inadequate budget that does not accommodate staff growth, and the slow dispersal of funds have complicated the trajectory of this new agency's growth and success.[75]

Moreover, the overall lack of discretionary and adaptive funding streams, combined with downward pressure and skepticism of U.S. foreign assistance is limiting the U.S. ability to compete with China in particular. Though USAID has taken China's gray zone competition seriously and adapted its messaging accordingly, USAID stakeholders have found they cannot currently meet or surpass Chinese aid and development funding.

Organization, Capabilities, and Resources

The sizeable gap and lack of coordination in the information domain is constraining the U.S. ability to expose and push back on Chinese and Russian political and economic coercion. Because of weakened capacity, DoS has had to delegate its traditional role of messaging to USAID in some areas. However, USAID has struggled with the heavier burden. This is compounded due to recent organizational challenges within the U.S. Agency for Global Media and its lack of messaging and narrative innovation.

As China's unfair and coercive business practices have gone unchecked for years, the size and capacity of U.S. development and finance programs are solidly outmatched by those of China. U.S. efforts to counter Chinese coercion, build resiliency in allied and partner countries, and regain influence in the international system thus face a particularly steep curve.

Congressional ratification of the Asia Reassurance Initiative Act in December 2018 authorized more funding for DoS and USAID overseas programs that ensure "trade, infrastructure, and investment in partner countries are transparent, open, and free of corruption."[76] Despite this and the BUILD Act, Chinese development investments likely will continue to outpace U.S. investments because the U.S. government fails to direct engagement and resourcing to the right regions where it can have the most impact or use its programs effectively and efficiently. U.S. comparative advantages to mobilize its own public- and private-sector resources, to provide quality partnerships and innovative techniques, is not being applied in a targeted or coherent way. Furthermore, as DoS continues to operate without indications and warning systems for political and economic coercion, as well as measurements and evaluations for U.S. programs, DoS approaches in the region will continue to be short-term and reactionary.

Another capability gap involves the speed and flexibility of programming and the capacity of key skillsets in the field. Because U.S. aid and development projects are slow to disburse from agencies and account for the requirements of social and environmental impacts, Chinese development projects continue to have an advantage in speed. Moreover, the United States is less competitive as there are few DoS economic and commercial officers at U.S. embassies conducting training on economic diplomacy. In addition, the Treasury Department's light footprint in U.S. embassies internationally may limit their reach and effectiveness. Promoting CFIUS-like mechanisms with allies and partners abroad to review the security concerns of financial transactions like Nord Stream 2 could increase the effectiveness of the financial security toolset.

Also, the lack of information sharing between the U.S. government and private enterprises hinders U.S. effectiveness. Private enterprises do not report cases of forced intellectual property transfer and other instances of economic coercion for fear of retaliation from business competitors or from China itself. The Chinese government has targeted specific companies that try to counter their coercive policies with extralegal embargoes and state-enforced boycotts.[77] Due to these dynamics, companies often do not have the motivation to share information with or assist the U.S. government in investigations regarding coercion.

Broadly, many allies and partners do not yet have mechanisms as strong as the U.S.-based CFIUS tool. The European Union has adopted a framework of foreign direct investment (FDI) screening that will take effect in October 2020. The EU mechanism will engage public and security entities to consider several elements, including: direct or indirect foreign investors; critical infrastructure, technologies, and inputs like energy; sensitive information; and freedom and pluralism of the media.[78] This framework does not yet have the ability to block investments nor does it unify the national-level FDI frameworks of individual EU nations. However, this is a step forward for the European Union to increase its resiliency.

4 CYBER AND SPACE THREATS

THE THREAT

As cyber threats expand, the international system is becoming increasingly vulnerable to foreign adversaries like China, Russia, Iran, and the DPRK. The most threatening source of malicious cyber activity is China. China and Iran have deployed many denial of service attacks and breaches to steal intellectual property from industrial and military sectors.[79] North Korea's cyberattacks target financial institutions for monetary gain, intellectual property theft, and to advance national interests.[80] The 2014 attack on Sony was indicative of how cyberattacks can serve political purposes, as it seemingly destroyed servers, froze operations, and leaked sensitive emails in retribution for Sony's release of a film negatively portraying the North Korean government.[81] Elsewhere, nations like Russia have breached sensitive emails like those of the Democratic National Committee to interfere in political processes. Cyberattacks can also damage critical infrastructure, like Iran's attack on dams in New York or Russia's shutdown of Ukraine's electric grid.[82] In a globalized world of economic and informational services, USG agencies and private industry must find a way to mitigate the damages of IP theft, protect the national security of the United States, and work with U.S. allies and partners to safeguard their national security and economic interests.

Experts interviewed by the CSIS research team warn that the counterspace activities of adversaries like China and Russia, and those emerging in Iran and North Korea, are of great concern for U.S. security. Space has been left out of many conversations about gray zone threats, yet it is a domain ripe for exploitation in the gap between diplomacy and conventional war. The U.S. military is critically dependent on space systems for communications, imagery, signals intelligence, electronic intelligence, weather, missile warning, navigation, and timing. Russia and China have developed, tested, and operationally fielded a wide range of counterspace weapons designed to disrupt, degrade, or destroy U.S. space capabilities. Many of these counterspace weapons are reversible forms of attack, such as jamming or spoofing the signals to or from satellites, making them appealing gray zone tactics. Though much of the information of this threat is classified, experts warn of these threats increasing. It is furthermore troubling that many of these threats have limited or uncertain levels of attribution and may not be visible to the public, which narrows the options U.S. policymakers may wish to use in response.[83]

Space provides an ideal environment for nations like Russia and China to engage in gray zone activities. Because of its remoteness, monitoring activities in space with enough fidelity to discern intent can be challenging. Because many of the counterspace weapons being developed, tested, and deployed by Russia and China are reversible forms of attack, they can be turned on and off at will, and some forms of attack in space can be difficult to attribute in a timely manner. When combined, these characteristics can make attacks against space systems a key tactic employed in a gray zone activity, where the intent is to have incremental effects that alter the status quo over time without triggering an escalatory response.

The forms of counterspace weapons that are most applicable to a gray zone environment include satellite jammers, spoofers, laser dazzlers, and various forms of cyberattacks against satellites and the ground stations that support them. Satellite jammers attempt to interfere with the signals going from a user up to a satellite or from a satellite down to a user. Jamming is a completely reversible form of attack, and the use of intermittent mobile jammers can make it difficult to geolocate and attribute an attack. A spoofer attempts to confuse a receiver into believing a false signal is in fact the correct signal from a satellite or user, and like jamming, it is completely reversible and can be difficult to attribute. A GPS spoofer, for example, can be used to guide bombs and missiles off course by causing the GPS receivers in these weapons to believe they are in a different location than they actually are. A laser dazzler can be used to temporarily blind the sensors on a satellite so that it cannot image or otherwise surveil an area and provided the power-level of the laser is sufficiently low, the attack can be completely reversible. Cyberattacks can be used to infiltrate a satellite network and corrupt the data or, in extremis, to take over command and control of a satellite to disrupt its operations or cause permanent damage. As in the case of cyber-attacks in other domains, cyber-attacks against space systems can be difficult to attribute.[84]

Russia, China, and others are already using gray zone tactics in space to gain advantage and pre-condition others to accept their actions as normal. For example, Russia has engaged in extensive satellite jamming and spoofing in Syria and Ukraine and in bordering states like Norway and Finland. Since 2014, Russia has jammed GPS and satellite communications signals in Ukraine, resulting in the loss of navigation and timing for radios and phones and the grounding of some remotely piloted aircraft. In Syria, Russian forces have deployed sophisticated jamming equipment, and according to press reports, this has affected the operation of small U.S. drones in the region. Since 2017, Russia has been intermittently jamming GPS signals in Norway and Finland during NATO and allied military exercises, such as the Trident Junction 18 exercise in October and November 2018. And GPS spoofing has been detected in the Black Sea, which caused ships to report GPS navigation errors of up to 30 miles.[85] In each of these examples, Russia has not acknowledged its illicit activities, and response from the United States and its allies and partners is not visible.

THE PLAYERS — CYBER

Perhaps more than any other gray zone areas, responsibility for cyberspace is divided among many departments and agencies. DHS has clear authority to lead domestic cybersecurity. DoS's cybersecurity focus is wholly overseas, but most other departments and agencies engaged in cyber efforts play key supporting roles at home and abroad. This includes the law enforcement and intelligence communities and DoD, DoE, Department of Treasury, and the Department of Commerce, as well as several independent federal agencies.

As described in the prior chapter, the FTC and the SEC play important roles in countering economic coercion, including by cyber means.

Department of Homeland Security

Per National Presidential Policy Directive 41, DHS is the lead agency for domestic cybersecurity concerns.[86] DHS established the Cybersecurity Infrastructure Security Agency (CISA) to lead critical infrastructure and 5G technology security, as well as public-private partnerships.[87] CISA's National Cybersecurity and Communications Integration Center (NCCIC) is the country's lead cyber defense, incident response, and operational integration center.[88] The NCCIC also assists allies and partners like Ukraine during cyberattacks that shut down their power grids.[89] CISA's Election Task Force seeks U.S. election integrity by conducting assessments of electoral system safety and offering cybersecurity programs to states.[90]

Department of State and Department of Energy

DoS has focused its cyber efforts on leveraging international agreements and messaging campaigns. In 2016, the United States and NATO agreed to expand language in Article 5 to include cyberattacks as a valid invocation for the collective defense clause.[91] The Wassenaar Arrangement and the Budapest Convention on Cybercrime are both major international agreements that discourage malicious cyber activity.[92] DoS also uses diplomatic networks to name and shame malicious cyber activity. In October 2018, DoS added to the UK and Dutch governments' combined effort to deliver a unified denunciation of Russian cyberattacks on anti-doping agencies, an investigation studying the Skripal poisonings, and investigations of the downed Malaysian flight over Ukraine in 2014.[93] These coordinated diplomatic reproaches, especially deployed alongside other targeted policies, can impose costs on malign cyber actors by damaging their legitimacy in the international system.

DoE also has an important stake in cybersecurity, as energy infrastructure is a major component of national security. After an attack from Chinese hacker group APT 10 on critical infrastructure and energy information, DoE reaffirmed the importance of cybersecurity in the energy sector as well as the necessity of private and interagency coordination.[94] In January 2019, DoE announced an initiative for a grid modernization project.[95] To ensure its activities are aligned with threat priorities, DoE is a member of the intelligence community.[96] Though DoE traditionally does not engage in international energy security programs, DoE has worked alongside counterparts in DoS, facilitated through the Russian Information Group (RIG), to deploy programs in energy cybersecurity and technical assistance in Europe and especially in Ukraine.[97]

Department of Justice

Since DoJ has expanded its investigations into cybercrimes and has established a Cyber Digital Task Force (with the aid of the FBI), the Trump administration has sought to bring attention to and indict more foreign and domestic actors that deploy influence operations and other cyber incidents.[98] The task force has sought to expand investigations and detection domestically and abroad, disrupting cyber threats like breaches and botnets through prosecution and training the private sector to build cyber resiliency.[99] Information compiled by DoJ investigations has helped other agencies like DoS "in diplomatic efforts to attribute malign conduct to foreign adversaries, to build consensus with other nations to condemn such activities, and to build coalitions to counter such activities."[100] In the wake of Special Counselor Mueller's investigation of foreign meddling in the 2016 U.S. presidential election, the DoJ indicted 13 Russian individuals and three Russian companies for deploying information operations and another 12 Russians for hacking into the Democratic National Convention's emails.[101]

Intelligence Community

The NSA protects national security information systems pertaining to defense and intelligence missions, deploys foreign intelligence missions to investigate malicious foreign cyber activity, and shares information on best cyber security practices.[102] NSA has acknowledged engaging in "persistent engagement" overseas, in partnership with U.S. Cyber Command (CYBERCOM).[103] The FBI's National Cyber Investigative Joint Task Force is the lead entity on coordinating and integrating investigations of malicious cyber activity. It also supplies and supports intelligence analysis for decision-makers and synchronizes efforts to focus on identifying, pursuing, and defeating adversaries who seek to compromise U.S. domestic cyber systems.[104]

The Cyber Threat Intelligence Integration Center (CTIIC), established by presidential memorandum in 2015 under the Director of National Intelligence, is a fusion center that serves as the federal lead for intelligence support to significant cyber incidents and foreign cyber threat responses. It provides intelligence and analysis for integrated threat trends, strengthening situational awareness and "support[ing] interagency efforts to develop options for degrading or mitigating adversary threat capabilities."[105] The CTIIC also seeks to downgrade classifications of malicious cyber activity to share as much information with U.S. government entities and the private sector. It coordinates activity to counter cyber threats with U.S. diplomatic, economic, military, intelligence, homeland security, and law enforcement institutions.[106]

Department of Defense

DoD has centralized its cyber efforts, expanded its offensive capabilities, and projected a greater international presence. There are numerous cyber-relevant capabilities and workforces across DoD. Of greatest significance is CYBERCOM. Congress gave CYBERCOM authority to "conduct military cyber activities or operations in cyberspace, including clandestine military activities or operations in cyberspace, to defend the United States and its allies, including in response."[107] CYBERCOM's expanded writ for offensive operations was also directed in President Trump's National Security Presidential Memoranda 13, from September 2018.[108] During the 2018 U.S. midterm elections, CYBERCOM and the NSA (see above) monitored foreign cyber adversaries, gathered intelligence, and provided information leads.[109] They also reportedly conducted an offensive cyberattack against Russia's disinformation operations by shutting down the Internet Research Agency on the day of the midterms, an approach its leadership has referred to as "persistent engagement."[110] CYBERCOM reportedly has "put reconnaissance probes into the control systems" of Russian electric grids since 2012, serving to match Russian offensive cyber capabilities.[111]

DoD is also engaged in international cyber cooperation through regular alliance mechanisms. As an example, the United States is a member of NATO's Cooperative Cyber Defense Centre of Excellence. The center conducts research, hosts conferences, presents policy recommendations, produces Cyber Law Toolkits, and conducts exercises to prepare for major cyberattacks.[112]

Department of Treasury, the Department of Commerce, and the Federal Communications Commission

The Department of Treasury provides important capabilities for deterring and protecting the United States from cyber threats. Through laws and orders like the Countering America's Adversaries Through Sanctions Act of 2017 and Executive Orders 1357 and 13694, the Treasury Department's Office of Foreign

Assets Control has sanctioned Russia for malicious cyber activity.[113] The Treasury Department also regulates investments and projects that are potentially harmful to national security through the Committee on Foreign Investment in the United States (CFIUS).[114] The Foreign Investment Risk Review Modernization Act of 2018 updated CFIUS review processes for the first time in 11 years, including language to screen for acquisitions and transactions that are "likely to exacerbate or create new cybersecurity vulnerabilities or result in a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities."[115]

The Department of Commerce assists in cyber defense through its role in preventing the entry of information technologies that are potentially harmful into U.S. markets.[116] Recent concerns over the expansion of Chinese telecom giants like Huawei and ZTE into U.S. and other markets highlight the role the Department of Commerce can play. It has been preparing for the advent of 5G through the National Telecommunications and Information Administration, which formulates research and policy on the security of implementing 5G technologies.[117]

The Commerce Department also has announced restrictions on Huawei and its affiliate companies on the grounds that their businesses pose national security risks.[118] These restrictions now require Huawei and its affiliates to seek USG approval before purchasing U.S. parts and technologies.[119] In May 2019, the Trump administration issued an executive order, Securing the Information and Communications Technology and Services Supply Chain, that reinforced the Commerce Department's restrictions on Huawei. The order prohibits "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) . . . that poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States."[120] Though not explicit, the order is expected to lead to the U.S. ban on Huawei and ZTE technology.[121] The order also clarifies authorities and oversight from relevant U.S. agencies.

The Federal Communications Commission addresses 5G concerns through the Communications Security, Reliability and Interoperability Council. The commission is a public-private advisory council for the communication industry.[122]

THE PLAYERS — SPACE

National security space operations are divided between DoD and the Intelligence Community (IC). The U.S. Air Force engages in this domain on behalf of DoD with defensive and offensive counterspace operations, like spoofing, impairing, and denying adversary's space systems.[123] The Trump administration has proposed a significant reorganization for military space, creating a new military service known as the Space Force and a separate Space Development Agency.[124] Until any form of reorganization takes place, DoD and the IC will continue to oversee space operations and acquisitions through a complicated patchwork of over 60 separate space-related organizations across the military services and the Office of the Secretary of Defense.[125]

ASSESSMENT OF U.S. GOVERNMENT PERFORMANCE

Cyber Policies

The most coordinated and robust U.S. government response to competitors using gray zone tactics has been focused on averting and deterring cyberattacks. As cyber threats affect the security of every U.S. department and agency, strategies and directives have asserted the seriousness of cybersecurity and outlined funding, lead agencies, and reporting structures to execute it. Though there has been much progress in cyber structure and capabilities, the scale and severity of the challenge from multiple actors poses continuing concern.

Though the Trump administration published a National Cyber Strategy in 2018, it has failed to clearly delineate how U.S. policy will translate into action.[126] Considering supply chain risks, the document explains that the federal government will "ensur[e] better information sharing among departments and agencies to improve awareness of supply chain threats and reduce duplicative supply chain activities within the United States Government, including by creating a supply chain risk assessment shared service."[127] However, without clarity of how information sharing will be achieved, agencies will have to interpret their own ways of moving forward, risking duplication, gaps, or inefficiencies.

In May, President Trump issued a cybersecurity executive order ("Securing the Information and Communications Technology and Services Supply Chain") that has prompted concern with experts and government officials for its limited scope of only targeting specific businesses (Huawei and ZTE), unwillingness to take a multilateral approach, and inability to address long-term supply chain risks. Though lawmakers have praised the short-term progress of the executive order on cybersecurity, they argue "a coherent, coordinated, and global approach is critically needed."[128] By not implementing an internationally coordinated policy that clearly delineates which countries or parties constitute a "foreign adversary," other nations have less opportunity and incentive to partner with U.S. policy to combat a broader range of potentially malicious technological acquisitions.[129] Other concerns arise from whether U.S. technological exchanges will suffer if they cannot do business with companies that use Huawei components and that blocking sales from one company (Huawei) will not address the root causes of this gray zone tactic that transcends cyber and economic coercion.

In addition, the U.S. government's underutilization of the authority and influence of its diplomatic, economic, and technological agencies overseas undermines its effectiveness. For example, the Department of Commerce could be doing more to dissuade countries from incorporating Chinese 5G technology into telecommunications infrastructure, which may be closely linked with Chinese intelligence services, or to recommend competitive and safer alternatives.[130] These might include a mix of information sharing and engagement, other inducements, or even punishments, depending on the country and circumstances involved.

Another question of policy arises around the nascent increase in offensive cyber operations. Some experts like Michael Sulmeyer have written that the U.S. government through CYBERCOM needs to employ "a more active cyber policy."[131] The United States' cyber posture has long been deterrence-based through the use of punitive measures like sanctions and indictments, which do not appear to have curbed malign behavior from China, Russia, North Korea, Iran, and non-state actors. Because the current threat landscape is based on undeterred behavior, experts like Sulmeyer argue that the United States must be proactively defensive. Recent disclosures signal that the United States is newly focused on increasing its risk-tolerance for offensive cyber operations. However, some experts interviewed worry U.S. escalations in cyberspace will only create more chances for conflict and retaliation between major powers.

Space Policies

Space policy is more nascent than its cyber counterpart. Almost all of the high-level attention around space issues has been consumed with how to organize the national security space. That said, the Trump administration issued a National Space Strategy in 2018. The strategy had four priorities: bolster space architecture to be more resilient; strengthen deterrence and warfighting options; improve foundational capabilities, structures, and processes; and foster conducive domestic and international environments for space-related activities.[132] DoD has yet to define publicly how these priorities intersect those of the National Defense Strategy.

The Trump administration's proposal to reorganize and enhance U.S. national security space activities includes a plan for DoD to use its existing authorities to elevate and marshal its space resources to deter and counter threats in space and to develop a legislative proposal to establish a U.S. Space Force within the Department of the Air Force.[133] This proposal is now being reconciled by the House and Senate Armed Services Committees for the National Defense Authorization Act for FY 2020. These markups will determine whether or not this reorganization will take the form of a Space Force, as the Senate markup proposes, or a Space Corps, as the House markup suggests, along with other reorganization recommendations.[134]

Cyber Authorities

Critically, in advance of the U.S. 2020 election, DHS's Election Task Force lacks sufficient and stable personnel and funding streams. Though DHS has responsibility to monitor the integrity of U.S. elections systems, it is forced to do so with a restricted budget. As DHS's Election Task Force is project-based, staffing has fluctuated greatly, casting doubt as to whether DHS is properly prepared for the 2020 presidential elections.[135]

Space Authorities

The lack of a senior "advocate" for space within DoD with the authority to manage the array of space programs complicates prioritization and strategic planning for space to keep pace with competitors' tactics and technological advancements. Proposals to reform DoD space activities aim to rectify this problem to ensure there are senior leaders responsible for the manning, training, and equipping for space-related missions, conducting space-related operations, and increasing coherence and agility of space acquisitions.[136] However, the interrelationship and command and control among and across these three functions, particularly as they relate to the U.S. Air Force and IC structures, have not been developed or made transparent to the public.

Current markups between the House and Senate propose different authority models for future space operations. DoD, the House, and the Senate all propose the addition of a four-star general officer in charge of a Space Force, Corps, or Command to the Joint Chiefs of Staff.[137] Pending approval of the reestablishment of a Space Command, the Senate also proposes the commander of SPACECOM serve as the commander of a Space Force for the first year.[138] Depending on pending markups and approval from Congress and the administration, the elevation of space operations within DoD could better ensure the incorporation of space threats into global U.S. planning and operations.

Cyber Organization, Capabilities, and Resources

CYBERCOM is working closely with election defense teams at DHS, the FBI, and industry sectors targeted by Russian hackers that might have early warnings about threats to the U.S. 2020 presidential election. Under the Pathfinder program, financial services and energy sectors work with DHS to identify digital threats, DHS relays those findings to CYBERCOM, and CYBERCOM identifies information that will help the industry partners defend themselves.[139]

Information sharing between DHS and the IC is currently productive in enabling domestic cybersecurity investigations. Furthermore, as CISA was reorganized per a presidential directive that created new reporting mechanisms, progress and strategy in meeting its domestic cybersecurity mission will be reported to facilitate strategic-to-operational feedback.[140] However, significant barriers remain to effective interaction between the federal government and private sector. These include challenges to public-private information sharing due to cultures of keeping information siloed or not shared (i.e., "stove-piping") within the private sector, challenges gaining the security clearances needed to share information, and competitiveness incentives that dampen industry interest in revealing cyber threats. More fundamentally, many U.S. companies appear to lack an understanding of both their vulnerabilities and how those vulnerabilities could damage U.S. national security.

DHS has taken steps to overcome these hurdles, though gaps remain. Its Financial Systemic Analysis and Resilience Center provides a register of cyber scenarios to help financial services and government partners prioritize systemic risks and build common steps toward resiliency. It currently includes 16 members of the financial sector. In the process, companies have had to overcome trust barriers in sharing information with each other, as they are required to expose their vulnerabilities to market competitors. In addition, companies expect an "equal commitment" from the U.S. government to provide privileged information and financial incentives, though the government cannot preference only a handful of companies that have agreed to participate.

DoD's stepped-up posture of "persistent engagement" bodes well for an active cyber defense, but questions remain as to whether it enables offensive operations to be deployed fast enough to address ever-changing threat profiles and to manage escalation potential. Moreover, the approach requires tight coupling of strategic ends—typically identified in an interagency policy process—and operational effects. It is not clear that the U.S. national security system is currently able to deliver that coupling, which can create risks of unintended escalation or self-defeating effects not understood by policymakers. Finally, gaps remain in intelligence and warning for cyber incidents, as well as normative frameworks to guide responsible use.

Broadly, there is an ongoing debate on the appropriate U.S. government organization for cybersecurity. Some experts like Ted Schlein believe that unifying all U.S. government cybersecurity efforts into one cabinet-level department will improve the efficiency of U.S. government efforts. Schlein argues that a streamlined organization with clarified responsibilities and authorities, simpler oversight, and more efficient acquisitions and staffing would enable stronger U.S. responses to cyber threats.[141] On the other hand, Suzanne Spaulding argues that unification would be disruptive and damaging, as the current structure with divided responsibilities is better.[142] Spaulding argues each agency has spent years to decades honing its unique expertise and relationships between sectors. As she explains, the IC has unique intelligence authority and capabilities, while DHS has developed a deep relationship with the private sector. Furthermore, consolidating departments could lead to duplication, increasing spending, not savings.

Space Organization, Capabilities, and Resources

Multiple U.S. Government Accountability Office reports point to overlap and fragmentation in national security space acquisition oversight and management. These reports highlight program cancellations and delays, inefficient operations, and cost overruns. Fragmented leadership reportedly "contributed to poor coordination and lengthy decision making . . . [these] challenges are magnified in space programs because their technologies are frequently obsolete by the time systems are deployed."[143]

DoD has requested $14.1 billion for space in FY2020. Approximately $72 million of that amount will be applied to the initial stand-up of the new Space Force.[144] As the Space Force matures as a bureaucracy, it will be met with oversight pressures to keep its personnel and resourcing requirements within scope. Notably, Congress has sought to decrease staff at DoD headquarters in recent years.

5 DISGUISED FORCES

THE THREAT

Proxy forces and state-controlled forces pose major threats to U.S. security interests. Although the United States has clear parameters of responding to conventional threats for itself, its allies, and its partners, rivals' uses of proxy forces and state-controlled forces pose confounding challenges. Iran has been prolific in using proxy forces to build influence or disrupt the authority, legitimacy, and influence of the United States, its allies, and its partners in the Middle East. Decades of U.S. efforts to pressure, constrain, and disrupt have largely failed to curb Iran's use of proxy forces to shape and influence the region to its advantage. In Syria, U.S. forces have had to calibrate their operations in the presence of both Iranian-backed militias and Russian mercenaries, managing for escalation risks.[145] Since 2013, Chinese state-controlled forces, protected primarily by its coast guard and maritime militias, have engaged in the dredging and artificial island-building in the Spratly Islands—creating 3,200 acres of new land—and building outposts throughout the Parcel Islands.[146] According to U.S. Pacific Command's Admiral Philip 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."[147] In addition, China's use of commercial fishing vessels have challenged international maritime access. Furthermore, extrajudicial killings like the Skripal attacks from Russia and the murder of Kim Jong Nam by North Korea add further strain to already frayed international relations and rule of law norms in the international system.[148]

Like China and Russia, Iran's Islamic Revolutionary Guard Corps Quds Force (IRGC-QF) has fewer restrictions when adopting new partners and less responsibility to maintain a code of conduct than the United States.[149] Despite a decade of U.S. partnership-efforts in Iraq, Lebanon, and Yemen, the United States has largely failed to halt the growth of IRGC-QF activities and its Middle East affiliates. Recent reports indicate that the IRGC-QF has continued to expand its number of partners in the region, thereby forming a land bridge from Iran to Lebanon through Iraq and Syria.[150] The IRGC-QF has also worked to advance the capabilities of its partners with advanced weapons and missile systems and cyber capabilities.[151] Until the United States can capitalize on weaknesses of the IRGC-QF—like its weak economy, infighting within Shia factions, and the diplomatic isolation of Iran—via commensurate growth in alternative local governance and security models, and absent a change Iran's strategic calculus, the IRGC-QF likely will continue to outperform the United States in the use of proxy forces.

THE PLAYERS

DoD and the Intelligence Community (IC) are the lead U.S. agencies for protecting the United States and its allies and partners from state-controlled forces. In addition, the Treasury Department has multiple mechanisms to sanction adversaries for their financial support of proxy and state-backed forces if they classify as terrorist groups.[152] With strong support from Congress, DoD has had ample legislative authority and funds to conduct security cooperation, build allied and partner capacity, and assert the principles of the freedom of navigation to push back against competitors' gray zone activities. DoS security-sector assistance, governance, and development programming and diplomacy bolster these efforts.

Department of Defense

In recognition of the prevalence and increasingly creative forms of competitor use of masked forces, DoD has deployed a range of programs in deterrence and resilience. In support of DoS's traditional lines of diplomacy, the DoD engages with organizations like NATO and the Association of Southeast Asian Nations (ASEAN) to reassure allies and partners, build combined military capability, and promote security cooperation. DoD organizations specifically tasked with countering Russia's and China's threats are the U.S. European Command's (EUCOM) Russia Strategic Initiative (RSI) and U.S. Indo-Pacific Command (INDOPACOM) China Strategic Initiative, respectively. These groups serve as a "forum for coordinating efforts and requirements" and create products for combatant commanders to "enable a more efficient application of existing resources and planning efforts."[153]

DoD also leverages its forward posture, including military exercises, activities, and operations, to shape and deter actions in the gray zone. To deter future territorial aggression from China in the South China Sea, the U.S. Navy conducts presence patrols. It performs Freedom of Navigation Operations (FONOPs) to deter interference with shipping lanes. In Europe, EUCOM through NATO conducts exercises like the Trident Juncture to discourage Russian territorial aggression or the use of proxy or state-backed forces. FONOPs also are increasingly considered a useful tool to reinforce freedom of navigation in the North Sea Route and to prevent parties like Russia and China from violating the UN Law of the Seas Convention.[154]

DoD buttresses allied and partner security forces globally by providing lethal and non-lethal aid. The European Deterrence Initiative counters Russia's territorial aggression and proxy support in Europe by mandating hard defense like "prepositioning equipment, deploying rotational forces, and improving infrastructure."[155] The Ukraine Freedom Support Act, through presidential authority, gives DoD authority to provide, "defense articles, services, and training to the Government of Ukraine [for] countering offensive weapons and reestablishing the sovereignty and territorial integrity of Ukraine."[156]

Special Operations Forces, often in coordination with the IC, counter adversaries' gray zone military aggression, like state-backed or proxy forces, through a range of activities. These include conducting operations with and training, advising, or assisting allies, partners, and at times, their own local proxy forces. DoD's irregular warfare directive set the policy that DoD may conduct irregular warfare independently or in combination with conventional warfare in activities and operations like "counterterrorism, unconventional warfare, foreign internal defense, counterinsurgency, stability operations, . . . and establishing or re-establishing order in a fragile state or territory."[157]

In addition, conventional forces are increasingly engaging in security cooperation with allies and partners to enhance their capabilities; the U.S. Army has created the Security Force Assistance Brigades to specialize conventional army forces in building partner capacity.[158] DoD conducts security cooperation, including combined exercises, training, advising, equipping, and institution building, under Title 10 DoD authorities.[159] The United States provides grant security assistance and foreign military sales under Title 22 DoS authorities, executed by DoD.[160]

The Intelligence Community and Department of Treasury

The IC contributes intelligence sharing to counter territorial aggression by proxy and state-backed forces. Through the "five eyes" (the United Kingdom, Canada, Australia, New Zealand, and the United States), intelligence collection and sharing has been adequate. Elements within the IC also have responsibility for conducting covert action, when so authorized. In the context of masked forces, this could include covert support to allied or partner governments or their proxies or the actual armed engagement of U.S. IC members or units in a masked role.

The Treasury Department enforces U.S. interests by imposing sanctions on states and non-state actors that violate U.S. interests, rules, and norms. In March 2018, DoS imposed sanctions on Iran for its affiliation with foreign terrorist organizations and North Korea for its extralegal murder of Kim Jong-un's half-brother Kim Jong-nam in Kuala Lumpur.[161] The White House has sought to curb the IRGC's influence by designating it as a foreign terrorist organization, which levies economic sanctions and travel restrictions on the IRGC and any business or organization with whom the IRGC interacts.[162]

ASSESSMENT OF U.S. GOVERNMENT PERFORMANCE

Policies

In this area more than any other assessed by the CSIS study team, U.S. policy on when and how to compete with state-controlled forces has varied significantly, both between the Obama and Trump administrations and by issue within each administration. It is not clear if the United States has been effective under either administration in deterring the further use of such forces by Russia and China. A promising example of success is that the effort since 2014 to fortify European allies and partners and build resilience against potential Russian gray zone military aggression has borne fruit in Eastern Europe. The Trump administration provided defensive equipment to Ukraine where the Obama administration did not and engaged Russian proxy forces in direct combat in Syria.[163] However, the United States and its allies have been failing to respond or deter Russia's aggressive behavior at the Kerch Strait in the Sea of Azov and its seizure of oil rigs in the Black Sea—which could be easily be militarized as China has done with its island building.[164] Just as Russia expanded its "military advisor" presence in Syria during the Obama administration, it has done so in Venezuela during the Trump administration.

The Asia Reassurance Initiative Act of 2018 seeks "to improve the defense capacity and resiliency of partner nations to resist coercion and deter and defend against security threats, including through foreign military financing and international military education and training programs."[165] It also seeks to reaffirm and expand treaty alliances with the Indo-Pacific region, the U.S.–China relationship, U.S.–ASEAN, quadrilateral security dialogue, enhanced security partnerships in Southeast Asia, FONOPs, counterterrorism, and cybersecurity.[166] DoD's 2019 Indo-Pacific Strategy Report emphasizes the importance of preparedness, partnerships, and the promotion of a networked region capable of deterring aggression, maintaining stability, and ensuring free access to common domains.[167] U.S. freedom of navigation operations in the Pacific have increased significantly since late in the Obama administration and particularly under the Trump administration. However, militarization continues on islands already created by China, and many of the interviewed stakeholders believe territory in the South China Sea is impossible to retake without conventional means.

U.S. policy versus Iran involves pursuing "maximum pressure" of economic sanctions and diplomatic isolation. Fiscal pressure on Iranian proxies such as Hezbollah have resulted in reported changes to fighters receiving pay and mounting currency problems within Iran itself. However, thus far, Iran seems undeterred from leveraging its 40-year-old asymmetric strategy and reliance on an influence network of proxies at varying levels of control, influence, and penetration in the region. The Trump administration's decision to unilaterally depart from the Joint Comprehensive Plan of Action on Iran's nuclear program has subsequently made European multilateral cooperation to address Iran's broader threat profile, including its use of proxy forces, quite difficult.

Another U.S. policy that has set the United States, its allies, and partners in NATO at a strategic disadvantage is withdrawing from the Intermediate-Range Nuclear Forces (INF) treaty. Firstly, the United States did not adequately consult NATO and EU partners before withdrawing, which led to a serious decoupling of U.S., EU, and NATO security goals.[168] Secondly, per the research team's conversations with NATO experts and stakeholders, if Russia enters into a conflict with NATO, it likely will take the form of a quick landgrab by disguised forces, reinforced by intermediate range missiles. As NATO currently has conventional disadvantages along the border with Russia, NATO forces cannot easily defend territory in such a scenario. Now with intermediate range missiles freed from the INF Treaty, Russia has a strategic advantage when the actions of disguised forces are protected by intermediate range missiles. Considering how Russia had already been violating the INF Treaty—and conversations with NATO stakeholders indicate Russia does not have the incentive to renegotiate a new intermediate range missile treaty—the United States and NATO now must grapple with the disadvantages that have deepened following the treaty's dissolution.[169]

Authorities

Title 10 and Title 22 authorities grant DoD and DoS authorities to support, train, and partner with forces, with legal checks and controls on human rights and accountability measures. However, there is no clear delineation over whether to build or counter U.S. local partners should be under Title 10 or Title 50 (Central Intelligence Agency (CIA)) authorities, and thus, the question of who should own long-term proxy strategy and operational development remains unanswered in the U.S. interagency.

Organization, Capabilities, and Resources

Groups like EUCOM's RSI and INDOPACOM's China Strategic Initiative have had success in synchronizing DoD activity, including by connecting effectively to leadership at the Pentagon and linking with broader interagency processes. Nevertheless, they are operating largely at the operational level; the greatest gaps are found not here but in strategic direction from Washington. Without a formalized methodology for defining and assigning policy priorities and actions, effective long-term strategies for deterring, competing against, and responding to competitors' use of state-controlled forces will likely be limited.

Capability gaps have also hindered U.S. competition with disguised forces. The United States cannot maintain sufficient force structure to be everywhere at once, which creates force advantages for rivals when U.S. forces must operate far from their bases. This includes the U.S. Coast Guard, which has authorities and capabilities well-designed for many aspects of maritime gray zone challenges, but which is not of size to decisively contribute in most instances. As the United States looks to improve its military capabilities for competition against China and Russia, it must weigh its policies, operational concepts, force positioning and activities, and force capabilities—measured as the cumulative effect generated by force readiness, structure, and modernization, among other attributes—against its ability to deter and challenge rivals' use of disguised forces, as well as its preparedness for their conventional and strategic capabilities.

A significant challenge also exists in information sharing between allies and partners. U.S. intelligence and military personnel are restricted in what information they can share. The IC's effectiveness is undermined by the hesitation of local allies and partners in concerned regions to work with the United States. Such doubts arise from perceptions of lack of U.S. commitment in the Middle East and the downplaying or erosion of international alliances under the Trump administration. Furthermore, there is concern that the Pentagon has over-dominated the policy priorities of the IC. Though it is necessary and beneficial for DoD and the IC to partner in competitive strategies, including in covert action, some experts believe the CIA is too focused on supporting military and counterterrorism operations, which has "distracted it from the type of (strategic intelligence) collection activities and strategic analysis it was created to provide."[170] Stakeholders indicate that it would be beneficial to reevaluate how and where the intelligence and talent of the IC is best served throughout U.S. agencies to focus on rivals' intent, motivations, capabilities, and resources.

6 U.S. GOVERNMENT REFORM PRIORITIES

The preceding chapters detail the degree to which the U.S. national security apparatus is actively engaged on many aspects of the gray zone challenge set. At the same time, the study team's findings point to numerous challenges in synchronizing priorities, resources, and action to leverage a broad toolset and eliminate stovepipes. Many of these issues have been previously documented and analyzed, yet they largely remain unaddressed in practice.[171]

In cataloguing needed reforms, the United States should avoid efforts to mirror-image its competitors. Rivals often employ tactics that violate the norms of the liberal international order, even as they benefit from its open markets. Corruption, illicit finance, elections interference, debt traps, the restriction of free speech, the spreading false narratives, territorial aggression, and extra-legal operations are lines the United States should not cross. Instead, the United States should primarily rely upon asymmetric advantages of transparency and rule of law and its system of alliances and partners to extend free and open spaces.

Policymakers should also take a pragmatic view of what reforms may be possible, given political and budgetary constraints, while still equipping the U.S. government with the change necessary to compete effectively in the gray zone. As such, U.S. reform priorities should be set around capitalizing on U.S. strengths and mitigating current gaps in the ability to execute the interest-based campaign plan described in Chapter 1 and further delineated in *By Other Means Part I*.

The study team's determination of reform priorities was also informed by three case studies aimed at illuminating organizational best practices in the face of emergent multi-vector challenges.[172] Across these three case studies, four best practices are apparent: (1) organizational reforms should seek to minimize redundancy, encourage organizational initiative, and eliminate anachronisms; (2) gray zone competition takes a coalition, across international borders and sectors; (3) reforms should build in flexibility for initiative without losing organizational and strategic principles; and (4) the U.S. government should treat oversight like an enabler, rather than a bureaucratic impediment, to encourage innovation, uphold democratic principles, and ensure that strategic objectives and outcomes are met.

If the U.S. government is to succeed in leading campaigns in the face of competitors' gray zone threats, five major areas stand out for needed reform: intelligence systems; strategic action and oversight; coalition-building; and capability investments.

INTELLIGENCE SYSTEMS

Buttressing U.S. competition against its rivals will require recognizing competitive campaigns from weak signals, including competitor intent, capability, impact, how competitors interact, and why these dynamics matter to U.S. interests. Identifying and assessing the true nature of gray zone threats is intrinsically the intelligence mission, guided by the policy priorities set at the national level.[173] Gray zone threats are challenging given that warning requires detection of a weak signal through global noise and across threat vectors and regional boundaries. Activity exists below the threshold of armed conflict but within the bounds of competition, obscuring intent, capability, and impact. Further weakening the signal, gray zone activity is most effective when malign activity is executed within legal boundaries so as not to set off any alarms or cross traditional warning trigger points.[174] Three interconnected gray zone elements characterize the nature of the activity: *temporality, attribution, and intent*.

First, gray zone threats are *temporal* in nature. The nature of gray zone threats truly requires a "big picture view" over long timescales and across regions and functional topics. On their own, individual events are difficult to distinguish from one-off actions, statecraft, or diplomacy. temporality of gray zone threats requires the synthesis of observation with contextual understanding early in the identification and assessment process.

Second, *attribution* of an activity to an actor serves both to enable policy and operational decisions and public attribution. However, requiring an "almost certain" or "nearly certain analytic assessment before acting costs time and analytic effort.[175,176] In some cases, the investment in human and technological resources needed to reach a confident claim of attribution can be prohibitive.[177] Across interagency units, lessons learned from high-conflict scenarios indicate that a lower threshold of certainty could be a suitable baseline for gray zone attribution.

Third, the challenges associated with temporality and attribution directly influence the *judgement of adversarial* intent to conduct gray zone activity. Indeed, the purpose of countering gray zone threats is to deter adversaries from fulfilling their intent to act. While attribution is one piece of the puzzle, closing the space around intent often means synthesizing multiple relevant indicators and warnings, including the state's geopolitical ambitions, military ties, trade and investment, level of corruption, and media landscape, among others. In addition to challenges posed by threats themselves, constraints to addressing gray zone activity exist within the policy and intelligence bureaucracies. Process flow, lack of communication, unclear policy direction, and structural silos are barriers to cohesive interagency coordination and shared threat assessments and priorities.[178] Near-term and long-term U.S. priorities are often at odds, while simultaneously crossing public-private and foreign and domestic policy boundaries.[179] When responses are undertaken, a gap exists in policy and process between U.S. strategic intent and the plans, tasks, and activities that various U.S. government organizations are undertaking. The result is unclear prioritization and resource allocation for driving intelligence prioritization, collection, and analysis.

Within the intelligence community, addressing the three gray zone warning elements requires data visualization, the fusing of multiple sources, and mechanisms to make a reasonable judgement in uncertain circumstances.[180] Like the gray zone threat, the intelligence process must similarly be dynamic, flexible, adaptable, iterative, and continuously experimenting, testing boundaries and taking in lessons learned to achieve an outcome. Unfortunately, long-established processes are not sufficiently elastic to adapt to the different kinds of data and information.

Finally, further complicating a credible U.S. response is the varying degrees to which allies and partners, as well as private-sector actors, perceive foreign adversaries as posing a gray zone threat. There is a growing uncertainty among foreign policy commentators about the degree to which future inter-allied gray zone responses will be possible due to disparities in common understanding of threatening activity and lack of strong national narratives on gray zone challenges. Positive engagement and active cooperation between public and private actors are critical and require highlighting the risks now facing many companies in the global economic and security environments.

STRATEGIC ACTION AND OVERSIGHT

Effective competition in the presence of gray zone tactics will require systematically building and synchronizing the employment of U.S. power and speeding quality decision-making to improve signaling and risk management. Overall, the U.S. government has a very decentralized approach to gray zone threats. National strategies, legislative mechanisms, and executive orders have left the response to gray zone threats largely to individual U.S. departments and agencies. Although some agencies have taken the initiative to create more systemic mechanisms for coordination, such as DoD and DoS have done with Russian Information Group (RIG), the general lack of common direction has led to confused messaging, the misalignment of efforts, and inefficient programs.

Though the lack of centralization has been frustrating to many experts, decentralization does have some virtues. The White House and the National Security Council (NSC) are vastly underequipped to address every gray zone activity in every sector adequately. With a centralized authority delegating gray zone policy goals, departments might actually communicate less, leading to stove-piping. Finally, decentralizing efforts can insulate well-functioning programs from failures elsewhere in the national security system. If centralized authority adopts a flawed strategy, such a strong directive from the top can affect any and all related agency programs. With more autonomy, agencies can be more flexible when innovating responses to gray zone activities.

An alternative model need not accrue these challenges. Instead, it could seek centralization not as a control but as an enabler. In fact, treating executive and legislative oversight as an enabler to drive innovation and accountability in accordance with U.S. interests and values could set strategic priorities and focus intelligence collection and interagency action, with iterative feedback mechanisms.

Authorities remain ill-equipped to address some gray zone threats. This is particularly notable for oversight of information operations that could affect Americans at home. As previously discussed, this is even more problematic when used in combination with malicious cyber actors. DHS stood up its Countering Foreign Influence Task Force (CFITF) and consequently has little legal authority to do anything. What is worse, without legal authority, the CFITF has no access to adequate funding streams. Lawmakers should evaluate and assess how constrained agencies' efforts in gray zone competition currently are and be sympathetic to future legislative proposals aimed at closing these gaps.

As the current status of U.S. agency response to gray zone competition has been decentralized, the role of presidential authority and personality varies. Some gray zone threats like cyber have maintained the same policy goals across administrations, while others like information operations have suffered greatly from leadership gaps. Furthermore, traditional agency policies have come into question from executive personality. While U.S. agencies like DoS and USAID are designed to leverage multilateral approaches, the Trump administration has often prioritized unliteral approaches, while also underfunding DoS and USAID when their unique capabilities are required. To drive changes to U.S. organization, policies, authorities, and tools, leadership at all levels of government matters critically.

As several stakeholders have expressed, the NSC has failed to adequately centralize policy with strategy on gray zone threats and to disseminate executive policy aims in the gray zone. This is especially apparent in the realm of cyber, where the NSC eliminated the role of Cyber Coordinator in May 2018.[181] Without a coordinator to disseminate the policy and strategy of the NSC to U.S. agencies (of whom all are concerned with cyber), experts have indicated they feel left in the dark in cybersecurity planning and strategy. Ignoring strategic campaigning and building interagency coalitions seriously damages the organization and coordination of cyber warning systems and the agility of agencies.

Furthermore, the RIG is one of few examples of interagency coordination against gray zone threats. Though the group is by definition restricted to Russia and focused on effects in Europe, the RIG is an important platform for relevant agencies to share best practices and lessons learned and expand their toolkits. The U.S. government currently has ways of organizing and prioritizing action across agencies, but few that foster such interagency coordination. Greater alignment of priorities and delegation of tasks would enable more agencies to coordinate responses, communicate best practices regarding gray zone threats, improve U.S. campaign strategy, and promote adequate use of warning systems in the gray zone.

Although U.S. strategy documents (e.g., the 2017 National Security Strategy and 2018 National Defense Strategy) highlight the importance of strategic competition with China and Russia, U.S. policy implementation of these strategies is uneven, thereby hindering U.S. response and proactive posture in the gray zone. Weakened international coalitions and partnerships have diminished U.S. competitive potential. The ability to leverage allied and partner goodwill and capabilities has diminished as the Trump administration increasingly favors unilateral approaches, which has combined with antagonism directed toward multilateralism, notably against NATO. By straining relations with allies and partners, U.S. reputation and credibility abroad has been damaged. Specifically, international allies and partners are more distrustful of U.S. narrative campaigns and less likely to partner with U.S. projects because of credibility concerns. This damaged credibility also makes allies and partners less likely to collaborate with U.S. efforts or volunteer information. If allies and partners are unwilling to contribute to U.S. gray zone efforts abroad, this seriously damages U.S. agility and the scope and coordination of gray zone defenses and capabilities.

Strategic action and effective oversight could also help correct the current lack of alignment between U.S. action and U.S. key advantages. As experts like Suzanne Spaulding have explained, the U.S. use of transparency as a tool, both as a defense against adversaries as a proactive measure against them, "naming and shaming" is a U.S. advantage in the gray zone that is currently underutilized. Because competitors are authoritarian and rogue regimes, their government's transparency is nonexistent. To the rest of the world, transparency is an element of U.S. norms and values that adds credibility to the U.S. narrative.[182] On the offense, the United States can do more "naming and shaming" of gray zone adversaries' own records of corruption and coercion. As defense, the ability of the United States to "own up" to any instances of corruption or political miscalculation denies Russia and other adversaries the opportunity to use such information as an attack on the U.S. systems' norms, values, and narrative. Transparency, or rather "to fight in the light," as Spaulding notes, is an asset to the U.S. toolkit and a U.S. advantage in the gray zone that, when underutilized, weakens U.S. policy narratives and agility in the gray zone.

The purpose of bringing gray zone activity into the light, sometimes in the form of naming and shaming another state, is threefold. First, public attribution puts the targeted state on notice that the United States is serious about deterring the behavior, and if necessary, is willing to escalate its response. Second, going public can serve as an opportunity for the United States to mobilize a coalition of international allies and partners to maintain multilateral pressure on the targeted state. Third, the "shaming" component of the strategy implies that the negative effects experienced by the target state—such as economic sanctions and diminished international status—will ultimately deter future actions by that state and others considering a similar course of action.

With a greater emphasis on "naming and shaming," the United States can create a stronger narrative at home and abroad. For populations under adversary authoritarian systems, fighting in the light damages adversaries by encouraging stronger public debate, generating a desire for access to denied information, and providing free and fair information outlets for better public understanding. With objective assessments and intelligence that are forward-leaning, the U.S. toolkit can have greater defensive resiliency and stronger offense measures to impose costs on adversaries.

Finally, many stakeholders have expressed that strategies fail to translate into effective implementation plans to synchronize action across government. The National Security Strategy, National Defense Strategy, and the National Intelligence Strategy outline gray zone threats as a priority for national security, but these strategies do not specify clearly how U.S. agencies should fulfil their strategic intent. Without a coherent approach and connection to programs, capabilities, and resources to make strategy and policy operational, the U.S. toolkit to address gray zone challenges lacks agility and integration.

COALITION BUILDING

Gray zone campaigning takes a coalition to cross borders and sectors and to leverage comparative advantages. It necessitates working closely with allies and partners, bolstering public-private partnerships, and overcoming the technology sector's skepticism of the U.S. government as well as the U.S. government's lack of engagement or knowledge of technology. The U.S. government faces three major challenges in coalition building today.

First, U.S. agencies do not share enough information with each other to improve gray zone responses, and often they do not share sufficiently with allies and partners to mobilize combined efforts. Due to security clearance restrictions, as well as the bureaucratic culture of parochialism and stove-piping, many U.S. agencies, offices, allies, partners, and civil society organizations do not have access to important intelligence that could align priorities and investments and mobilize action in a more effective manner.

Second, the U.S. government faces the operational limitation of not receiving enough information from the private sector. Because the private sector is wary to report gray zone attacks and conduct investigations with the U.S. government, information sharing continues to create even more of an awareness and agility gap at the operational level. For example, the private sector has little incentive to report cyber intrusions or intellectual property theft because a loss of faith in a company from a board of directors, stockholders, and the greater public can jeopardize its financial stability. By keeping these breaches under wraps, the U.S. government loses the opportunity to study these attacks and its ability to prosecute gray zone adversaries for wrongdoing. Furthermore, a high number of unreported threats mask concerning patterns of adversaries' behavior, to the benefit of their reputations. The United States will have a stronger, more compelling narrative against competitors when the greater public has a deeper understanding of the degree of penetration into U.S. companies and private-sector entities. Until the private sector has enough incentives to report these attacks to the U.S. government, the ability to track, understand, and impose costs on competitors is at a great disadvantage.

A third weakness is the absence of a domestic toolkit to improve public awareness, education, and resilience against gray zone threats. Though DHS works to ensure cybersecurity to U.S. agencies and in the private sector, DHS is vastly unequipped to deploy mechanisms to build resilience against disinformation campaigns and other information operations. Beyond DHS, only a few agencies like DoJ have the purview or tools to defend and build resilience in the domestic sphere against cyber threats and economic coercion. Without deploying integrated and adequate resilience tools across U.S. agencies, crossing foreign policy and domestic policy boundaries and effective U.S. intelligence and warning systems, let alone strategic action, will continue to lag.

Increasing partnerships and engagement with the private sector will be critical to ensuring the resilience of the U.S. economy to gray zone penetration, harnessing innovations and best practices for countering harmful gray zone activities, and bolstering U.S., allied, and partner competitiveness in foreign markets. This approach will be in tension with some elements of the private sector which prize independence, doubt U.S. government motives, have incentives to work with and within competitor markets that use gray zone tools (especially with China), and do not wish to be treated as surrogates of the

U.S. government. However, valuable lessons from recent DHS experiences in incentivizing and information sharing with the private sector can instruct a new approach (Reference text box).

CAPABILITY INVESTMENTS

The U.S. government must also direct resourcing to key priorities where there are gaps in U.S. structure, policy, and practice, including:

Strategic Communication and Narrative

The U.S government should treat information as a critical domain of statecraft. It should develop political narratives directly linked to the U.S. campaign plan for the gray zone and why it matters for U.S. interests. It should advance investments in civics and social media engagement to spread public awareness of deliberate attempts by adversaries who use gray zone tools to undermine U.S. institutions and exacerbate existing domestic fissures. Overseas, public diplomacy must include programs aimed at undermining competitors' efforts to manipulate and control media, undermine free markets, and suppress political freedoms. This public narrative should be coupled with investments in overseas overt and covert information operations as an integral part of regional and country strategies. At the same time, the United States must address significant gaps in legislative authorities to enable the integration of information.

Cyber

Although the United States has taken significant strides to recognize, organize, and resource for cyber challenges, greater policy prioritization, alignment with broader strategy, and additional capabilities are needed. Cyber challenges present a particularly pernicious source of gray zone activity, especially when used in combination with information operations, and must be a central concern for adapting the U.S. government's approach to the gray zone. Mobilizing public-private sector engagement, as well as allied and partner collaboration, will be crucial to buttressing U.S. cyber capabilities.

Inducements

The U.S. government has focused heavily on punishing malign actors and is undervaluing a key asymmetric advantage: the full range of its incentives and inducements to build a network of allies, partners, third parties, businesses, civil society organizations, and U.S.

"Section 9" Cybersecurity Cooperation

By the 2013 Executive Order 13636, DHS, in coordination with other agencies, annually identifies and maintains a list of cyber targets with infrastructure vulnerabilities that could disrupt U.S. power, water, communication, and other critical systems. These "Section 9" entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." President Trump's Executive Order 13800 further directs DHS and other agencies to identify authorities and capabilities that the federal government could employ to support the cybersecurity efforts of Section 9 entities.[183] The Section 9 exercise has helped overcome a public-private sector debate within the resilience community on whether to treat all companies the same or to recognize the importance of some over others to provide them with more privileged information. To bridge potential and resulting resentment among companies "left out" of this mechanism, Section 9 companies had to create a charter that included a mission objective to help the broader sector improve their resiliency by sharing information. DHS also engaged in a dialogue with private-sector companies on their distinct vulnerabilities and included an appeal if a company wanted to "opt out" of inclusion on the Section 9 list, reflecting a two-way dialogue between the public and private sector rather than the federal government dictating the terms of participation.

citizens. Maintaining America's competitive edge will require additional authorities, resourcing, policy prioritization, and political leadership to leverage strategically and to maximize impact.

Looking Ahead

Gaps and deficiencies in U.S. government structure, policy, and practice impede its competitiveness. There are tactics and tools used by U.S. rivals that the government simply cannot match in kind due to capacity or should not due to constitutional or normative limits. Other gaps arise from policy, bureaucratic structures, organization, and ineffective investment. These gaps inhibit effective intelligence, hamper strategic campaigning, weaken interagency, international, and domestic coalitions, and greatly reduce effective oversight. However, the gaps can be closed with changes to U.S. government organization, policy, authorities, and capabilities to enhance U.S. competitiveness.

SUMMARY OF REFORM PRIORITIES FOR THE GRAY ZONE

Area of Reform	Reform Challenges	Reforms Required
Intelligence Systems	• Individual events are difficult to distinguish as trends vs. one-off actions • Certainty of assessment before acting costs time and analytical effort • Adversary intent is difficult to determine, due to process flow, lack of communication, unclear policy direction, and structure	• Data visualization, the fusing of multiple sources, and mechanisms to make a reasonable judgment in uncertain circumstances • Feedback mechanisms must be continuous and drive operational cycle
Strategic Action and Oversight	• Approach to gray zone threats is decentralized • Authorities remain ill-equipped • Leadership is inconsistent • NSC staff has failed to centralize competitive strategies and gray zone policy elements and to disseminate executive policy aims • Interagency lacks coordination • Strained relations with allies and partners means they are less likely to collaborate with U.S. efforts • U.S. action and U.S. key advantages lack alignment • Strategies fail to translate into effective implementation plans	• Approach that is centralized and enables innovation and accountability • Leadership at all levels of government matters critically • Coordinator to disseminate the policy and strategy; greater alignment of priorities and delegation of tasks enables greater agency coordination • Credibility rebuilt with allies and partners • Emphasis on "naming and shaming" • Coherent approach and connection to programs, capabilities, and resources are implemented • Intelligence cycle is tied in
Coalition-Building	• U.S. agencies do not share enough information with each other • U.S. government does not receive enough information from the private sector • Absence of domestic toolkit to improve public awareness, education, and resiliency against gray zone threats	• U.S. agencies increase collaboration • Incentivize private sector to work closely with U.S. government • Integrated and adequate resilience tools deployed across U.S. agencies, crossing foreign policy and domestic policy boundaries
Capability Investments	• Strategic communication and an overall narrative are lacking • Cyber challenges require greater policy prioritization and alignment with broader strategy • Overreliance on punishing malign actors	• Develop political narratives directly linked to the campaign plan, advance investments in civics and social media engagement, ensure that public diplomacy includes programs aimed at undermining competitors' efforts, and public narrative should be coupled with investments in overseas overt and covert information operations • Buttressed cyber capabilities require mobilizing public-private engagement as well as allied and partner collaboration • Full range of incentives and inducements utilized to build network of allies, partners, third parties, businesses, civil society organizations, and U.S. citizens

7 RECOMMENDATIONS

Closing the five priority areas highlighted in the prior chapter (intelligence systems, strategic action, oversight, coalition building, and capability investments) will require several cross-cutting changes to U.S. policies, authorities, organizations, capabilities, and resources. The U.S. government should undertake reforms in the following areas:

1. Driving strategic action from policy to operations to synchronize the employment of U.S. power, facilitate quality decision-making, improve signaling, manage risk, and foster innovation and accountability;
2. Fusing intelligence and improving warning;
3. Prioritizing key capability investments, such as elevating information as a critical domain of statecraft and buttressing national cyber capabilities; and
4. Enabling all lines of effort through coalition building with allies and partners and public-private partnering, leveraging a range of inducements.

Where applicable, this chapter highlights areas where allies and partners have shifted their strategic cultures, processes, organizations, and policies to adapt. Political and societal differences can make direct comparisons difficult. Nonetheless, illustrations of how other democracies are advantaging themselves in the presence of gray zone challenges should inform consideration of potential options in the United States.

STRATEGIC ACTION

A more strategically comprehensive and agile decisionmaking culture is required to address the phenomenon of gray zone competition. Ideally, such a shift would evince a broader move toward integrated campaigning across the national security enterprise. Overarching national security reform is a worthwhile topic for future research, but it is beyond the scope of this study. Its absence, however, should not prevent the United States from making changes now to improve the U.S. approach to gray zone tactics, as several U.S. allies have done. Doing so will redound positively to any broader national security strategy the United States is likely to pursue. The challenge of adapting to gray zone challenges is perhaps most akin to prior improvements in U.S. approaches to countering terrorism or weapons of mass destruction: a major enabler to broader regional and global strategy that must cross regional and functional, foreign and domestic, and public and private-sector boundaries. It will have significant value unto itself and could generate momentum for further change.

Business-As-Usual Model

In practice, there is no designated lead actor in the U.S. government today charged with looking across the range of gray zone challenges and rivals to inform national security decisionmaking or coordinate interagency actions—let alone coordinate with the private sector or allies and partners. Policymakers largely rely on a bottom up approach from individual agencies to highlight gray zone concerns as they arise, which in turn impedes the development of forward-thinking and synchronized approaches to China and Russia, the two foremost challengers to U.S. interests cited in the National Security Strategy. The current interagency process thus tends toward short-term and even reactive thinking. Moreover, with integration largely stove piped around single rivals, decisionmakers are hampered in gaining visibility into how actors may be influencing or capitalizing upon one another's activities. Coordination with and feedback from the U.S. private sector is particularly limited. As gray zone challenges are increasingly multidisciplinary, there are few organizations within the U.S. national security structure that are equipped with the broad-spectrum capability to effectively counter Russian and Chinese gray zone tactics in real time. Furthermore, institutional hurdles currently impede diverse subject matter experts, hailing from outside of the traditional national security and foreign policy disciplines (e.g., physical science, engineering, media, legal, and economics fields), from contributing to the direct development of national security countermeasures to emerging gray zone threat vectors.

Interagency Driver Model

The U.S. government would benefit from better strategic integration and centralized authority and responsibility for applying the gray zone lens to U.S. policy. A form of this centralized and directed decision-making could be driven by a designated lead agency.[197] However, housing this function in the NSC staff will be most effective, given the need to cross foreign policy and homeland security boundaries and the sheer breadth of relevant tools and capabilities to be leveraged. In fact, Congress has recognized the need for such an NSC lead, legislating a requirement for a coordinator for countering foreign malign influence operations on the NSC staff.[198] The administration does not appear to have made such an appointment. Placing this responsibili-

LEVERAGING LESSONS FROM ALLIES, PARTNERS, AND THIRD PARTIES

Allies and Partners' Government Reform to Address Gray Zone Threats

Key lessons for security organization to counter gray zone challenges can be derived from allies and partners. For example, Sweden has embraced reorganizing its security agencies to better address gray zone threats. After the U.S. 2016 presidential election, Sweden took notice of the dangers of disinformation campaigns and developed a holistic strategy to reorganize and mobilize the Swedish government, media, and citizens in the defense against information operations.[184] Election systems have now been included as part of critical infrastructure and fall under the authority of crisis preparation and response within the Civil Contingencies Agency.[185] With this agency's authority, directive, and budget, Sweden conducts threat analysis of election systems and targeted training of civil servants to detect and respond to information operations.[186] Sweden also has created an interagency forum between its security agencies to coordinate future elections. With stronger coalitions among agencies, Sweden's government has sought to optimize and synchronize its agencies' collective power, enhancing the speed and quality of decision-making to improve signaling and manage risk.

In another example, after suffering a massive cyberattack from Russia in 2007, Estonia has adapted its infrastructure to withstand future cyberattacks. It maintains a "data embassy" in Luxembourg that houses copies of the country's data.[187] Most strikingly, Estonia has highly advanced voting protection systems that allow voters to vote online by using their personal identification digital signatures.[188]

The Latvian government adapted its State Defense Concept in 2016 to incorporate total defense and "social resilience" as an integral component to its national security strategy.[189] Such language makes clear that the Latvian government seeks to deter gray zone or "hybrid" threats "to increase and improve the population's ability to resist all forms of hybrid threats."[190] ■

Information Sharing and Action

Fusion centers provide important outlets to develop policy, strategy, and resilience from ongoing and emerging threats. Estonia is home to NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE). Per its mission, the CCDCOE conducts research; convenes the International Conference on Cyber Conflict and trainings and exercises like the Cyber Coalition; and develops policy and strategy in the fields of cybersecurity for members of the alliance and its partners.[191] In practice, its contributions have been strongest in providing research and analysis. Per the organization of NATO, the CCDCOE is concerned with one functional element of the gray zone: cyber defense.

More broadly, the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE), based in Finland, is a "neutral facilitator between the EU and NATO" for all hybrid threats.[192] Like the CCDCOE, Hybrid COE convenes strategic discussions, exercises, and research for the development and sharing of best practices for hybrid threats like information operations, energy infrastructure security, economic coercion, and others.[193] Such a model is pragmatic, as many gray zone threats are interrelated.

These centers of excellence are strong sources of coordinated research, exercises, policy, and campaign strategy. The United States is a participant in both the CCDCOE and Hybrid COE and would do well to expand its adoption of the COEs' recommendations and advocate for other participating countries to adopt recommendations, as the United States develops its own strategic and operational approach. ■

Private-Sector Efforts to Fuse Collective Information Sharing and Action

After facing multiple cyberattacks, banks in the United Kingdom like Lloyds, Barclays, Deutsche Bank, Santander UK, and Standard Chartered joined a London-based cyber security group called the Cyber Defense Alliance (CDA).[194] The CDA serves as a platform for the banks to share information about best practices and lessons learned from past cyberattacks.[195] These banks fund the CDA by paying for access to research and shared information.[196] Under this model, the CDA is a private-sector-led solution that provides incentives to other private enterprises to improve their cybersecurity systems. ■

ty at the White House has some drawbacks. Executive branch leadership will need to help the NSC staff target their efforts at the strategic level, given the propensity across multiple administrations to incentivize a focus on meeting near-term presidential needs. Absent such direction, an NSC-led model of synchronization could risk furthering a largely tactical, tit-for-tat approach to rivals' strategies.[199]

Key elements of this *interagency driver model* include:

- Meeting statutory direction to designate an NSC senior director for gray zone challenges, akin to similar-level focus for counterterrorism and countering weapons of mass destruction;
- Defining and driving priorities for foreign and domestic policy, in support of regional and global competitive strategies, such as by contributing to strategy and policy processes focused on China and Russia;
- Driving key lines of interagency alignment through a Gray Zone Action Group (GZAG), akin to the Counterterrorism Security Group (CSG), in areas such as:
  - Specific directions and role clarity for agencies, with a regularized (e.g., monthly) deputies and principals committee process;
  - Strategic narrative in coordination with DHS, DoS, DoD, Intelligence Community (IC), and other implementing agencies;
  - Strategy, with implementing agencies, for allied and partner engagement and multilateral burden sharing;
  - Strategy, with implementing agencies, for private-sector engagement;
  - Particular focus on the nexus of cyber and information operations; and
  - Encouragement for innovation and monitoring of progress and accountability.
- Receiving support from an interagency task force that ties information to strategy and operations (see details in Intelligence and Warning recommendations)
- Organizing and proactively engaging in a legislative strategy, with implementing agencies, to ensure effective and constitutional oversight.

INTELLIGENCE AND WARNING

The fluidity of gray zone challenges tests the U.S. intelligence and warning system. Information integration tools can advantage analysts, helping to make sense of seemingly disparate data points through the integration of a range of information sources into a cohesive, actionable product. Through a common information-integrated picture, all actors—ranging from multiple interagency entities to the United States' various allies and partners—could be on the same page before initiating both defensive and offensive approaches. Further, significant amounts of quality open-source information are now available and should be leveraged to build products and analysis prior to problem prioritization in the areas of observation, attribution, and intent.[200]

Competing in the gray zone also involves active cooperation, between allies and partners as well as public and private actors to share information. Best practices have arisen from coordinating responses with allies and partners. Collaboration with private-sector companies has resulted in guidance to companies on how to guard against the cyber threat. Multilateral coordination between governments victimized by gray zone economic coercion has enabled a strong condemnation by the international community in response to illicit behavior. Successfully distinguishing the gray zone campaign signal through the global noise requires action through the entirety of the national security community. Policy, process, and tools must all adapt and evolve to detect, discern, and act upon a new type of signal. A full description of this approach is included in Appendix A.

To achieve greater alignment and integration of information, strategy, and operations, the United States needs a common and adaptive picture of the environment and warning features for policymakers and operators. Multiple models exist for how to achieve this end: the National Counterterrorism Center (NCTC), the Cyber Threat Intelligence and Integration Center (CTIIC), and the Joint Interagency Task Force-South (JIATF). The CSIS study team ultimately drew on the best aspects of each for its recommendations to improve intelligence fusion and connectivity "upstream" to decisionmakers and "downstream" to operators.

The National Counterterrorism Center.

NCTC integrates counterterrorism (CT) intelligence and operations across government agencies. The 9/11 Commission recommended the NCTC's formation to help close information sharing gaps in matters pertaining to terrorism. The commission recommended a "civilian-led, unified, joint command for counterterrorism," modeled after the CIA's Terrorist Threat Integration Center.[201] Through executive action, the NCTC was stood up in 2004 and has been the primary organization to integrate and analyze intelligence relating to terrorism and counterterrorism.[202]

NCTC is aligned under the Director of National Intelligence (DNI). The NCTC director is appointed by the president and confirmed by the Senate. The NCTC director reports to the DNI as the national intelligence manager for counterterrorism and serves as the DNI's principal adviser on intelligence operations relating to CT. The NCTC director reports directly to the president for CT strategic operational planning activities.[203]

To coordinate and present holistic information regarding terror threats, the NCTC has authority over strategic operational planning as it integrates intelligence from a multitude of sectors, including diplomatic, financial, military, homeland security, and law enforcement.[204] The NCTC also coordinates with foreign allies and partners to further improve intelligence. The NCTC assigns roles and responsibilities to other federal agencies, leads interagency terrorism task forces, and hosts the interagency Joint Counterterrorism Assessment Team, which creates intelligence products for all levels of the government (federal, state, and local) as well as the private sector.[205] Centralizing these activities within the NCTC aims to ensure that strategic operational planning for counterterrorism is efficiently organized and uniform. These centralized efforts also aim to facilitate information and intelligence sharing and distribution across relevant U.S. agencies. This organization decreases opportunities for duplication and improves the agility of U.S. action by clarifying roles and responsibilities and encouraging the flow of relevant intelligence.

Critiques of the NCTC's effectiveness point primarily to two issues.[206] The first relates to the relatively unclear objectives of its strategic and operational planning element, which can be dependent on leadership personality. Second, inspector general reports from the IC, DHS, and DoJ have asserted that clearer guidance is needed for information sharing through NCTC that "accounts for the roles and responsibilities agencies have according to statute."[207]

The Cyber Threat Intelligence and Integration Center.

Another existing intelligence fusion source is the Cyber Threat Intelligence and Integration Center (CTIIC). Established in 2015 by presidential memorandum under the DNI, the CTIIC produces coordinated IC analysis of cyber threats from abroad to U.S. interests. CTIIC's mission is to ensure that information is shared among the federal cyber community, and that it enables operators, analysts, and policymakers to make timely decisions about cyber threats and actors. However, much as with critiques of NCTC, tensions and lack of role clarity between CTIIC and agencies with cyber and intelligence missions can limit CTIIC's effectiveness.

Joint Interagency Task Force South (JIATF South) Model.

JIATF South is a preeminent example of a joint interagency task force model. With the rise of Colombian drug cartels nearly 40 years ago, the Reagan administration and Congress identified the operational gaps of traditional law enforcement and saw the need to amend law and pass directives to give DoD greater legislative authority in matters pertaining to narcotics trafficking. In 1981, Congress amended the Posse Comitatus Act, allowing the DoD to support civilian law enforcement agencies and the Coast Guard. President Reagan later granted DoD greater authority through the National Security Decision Directive 221 in 1986, which elevated narcotrafficking to a national security threat.[208] As counter-narcotics efforts continued to fail over several decades, Congress and the executive branch experimented with increased authority and resourcing granted to DoD efforts, ultimately resulting in JIATF South.[209]

With requisite authority, resourcing, tolerance for experimentation, and inclusion of joint, interagency, and international partners, JIATF South is able to execute its mission of detection and monitoring operations pertaining to illicit trafficking.[210] Under the leadership of the U.S. Southern Command and receiving directives and priorities from departments and agencies involved in the interagency process, JIATF South relies on the fusion of cross-functional teams to leverage intelligence and operational and tactical advantages to better achieve strategic priorities. As a result, JIATF South has centralized strategic priorities through greater mission understanding and strategic campaigning. In practice, this means the DoD supplies detection and monitoring operations, as well as other tactical and resourcing advantages, and allies and partners expand the scope of intelligence. Synchronizing these elements across agencies and partners, law enforcement has better intelligence to proceed with arrests to increase successful prosecutions.[211]

Even as JIATF South receives significant praise for its success as an organizational model, important questions remain about the overall effectiveness of U.S. counter-narcotics efforts. Similarly, a U.S. approach to the gray zone that succeeds tactically may well fall short at the strategic level absent shifts in strategic culture, smart policies, and investments in needed capabilities.

Fusing Intelligence and Improving Warning: Aiding Virtuous Strategy-to-Operations Cycles

The U.S. government must align the priority and applicability of its intelligence and warning efforts alongside improvements in strategy and operations. Many pieces of a solution set exist today, but the United States does not yet have a viable architecture. The National Intelligence Council (NIC) should have responsibility for the intelligence fusion effort. Overcoming public-private and foreign-domestic barriers to information sharing is vital for effectiveness in the face of modern-day gray zone tactics. Relative to other parts of the U.S. intelligence community, the NIC has developed a culture of outreach and engagement to parties beyond the U.S. government. It also has requisite authority to sanitize intelligence for sharing with allies and partners and can speed similar intelligence sanitization for other actors, such as U.S. companies. Assignment at the NIC is career-enhancing for intelligence officers, making it an ideal place to draw the best and brightest across the many intelligence disciplines and generate the expertise required by the gray zone challenge.

It will not be enough to simply fuse intelligence. As described above, campaigning effectively requires a continual feedback loop from strategy to operations. Intelligence plays a vital role in creating this virtuous cycle, ensuring decision-makers and operators have the information they need to adjust nimbly. This is particularly valuable when it allows U.S. actors, allies, and partners to act in advance of threats or to seize emergent opportunities. The national intelligence officer (NIO) for gray zone challenges should thus be a key participant in the GZAG process, along with other major interagency strategists and operators, notably including the NIO for counterintelligence. Moreover, the United States will need to revitalize the covert aspects of its strategy through a body akin to the Cold War-era active measures working group, hosted by the CIA and linked to the NSC staff, departments, and agencies via the GZAG.[212] The NIO would also serve on this covert active measures working group.

Especially in its initial stages, fully linking intelligence to strategy and operations will require greater institutional horsepower than a single NIO and NSC senior director can provide. Borrowing from the JIATF South model, the CSIS study team recommends that the NSC senior director oversees a small interagency intelligence-operations task force assigned to develop the gray zone campaign plan and serve as the core staff element for its implementation through the GZAG process.

In all, improving intelligence and warning and creating a virtuous feedback cycle with decision-makers and operators includes:

- Creating a NIO for gray zone threat fusion, reporting to the director of National Intelligence, working closely with the NIO for counterintelligence, and serving as a principal member of the GZAG. This officer:
  - Provides a common intelligence picture for U.S. national security agencies on gray zone challenge sets and is responsive to the president and DNI taskings on priority areas;
  - Is responsible for gray zone information synthesis, including input from across the IC, DHS, DoD, DoS, DoE Treasury Department, FBI, and law enforcement agencies;
  - Engages private-sector operational experts for planning and execution through an established process;
  - Develops and refines a framework for a warning system for gray zone activities;
  - Briefs the Committee on Foreign Investment in the United States working group on emerging economic and technological threats; and
  - Establishes two-way information sharing with the private sector on shared threats, including both a classified mechanism for cleared

    individuals and an unclassified mechanism for broader information sharing.

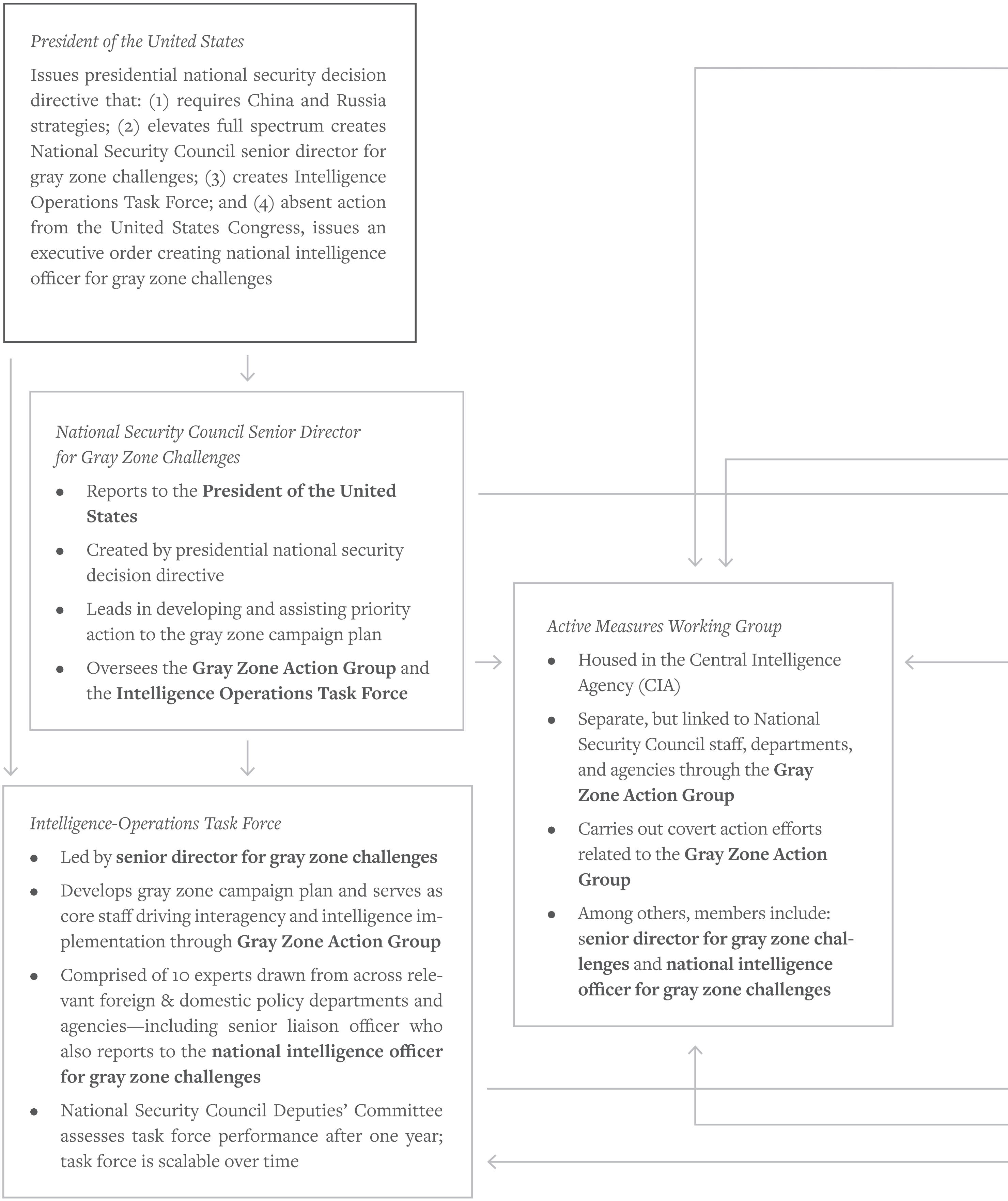
- Leveraging the authorities, capabilities, and products of the existing NCTC, the CTIIC, and other like bodies;
- Revitalizing an active measures working group, led by the CIA and with the participation of the NIO and NSC senior director for gray zone challenges, to strategize and coordinate covert aspects of the U.S. gray zone campaign plan;
    - Key department and agency leaders, such as assistant secretary-level participants in the GZAG, should be cleared for access on the group's efforts.
- Establishing an intelligence-operations task force (of no more than 10 people) under the direction of the NSC senior director for gray zone challenges, linked to but distinct from the active measures working group.

The gray zone intelligence-operations task force should:

- Be led by the NSC senior director for gray zone challenges, who should be a senior civilian with career intelligence and operational experience;
- Comprise no more than 10 experts drawn from across the relevant domestic- and international-facing national security departments and agencies, with performance appraisals conducted by the NSC senior director during their tenure on the task force;
    - This includes a senior liaison officer who also reports to the NIO for gray zone challenges.
- Provide weekly briefings in the GZAG process to guide implementation and synchronize interagency action;
    - The task force should be hosted in the White House executive office buildings to facilitate support to the GZAG, Deputies Committee, and Principals Committee.
- Employ adaptive feedback mechanisms and integration to inform the intelligence-to-operations cycle, with the advice of the NIO for gray zone challenges, enabling decision-making agility; and
- Coordinate and synchronize action with U.S. embassy country teams, in coordination with the State Department.

The NSC Deputies Committee, meeting through the GZAG process, should assess the performance of the task force after its first year, with clearly defined outcomes, objectives, and metrics for success, in coordination with task force members and the senior director and NIO. Task force roles and capabilities could be scaled over time, depending on active or projected threat streams and U.S. activities.

REORGANIZING FOR THE GRAY ZONE



President of the United States

Issues presidential national security decision directive that: (1) requires China and Russia strategies; (2) elevates full spectrum creates National Security Council senior director for gray zone challenges; (3) creates Intelligence Operations Task Force; and (4) absent action from the United States Congress, issues an executive order creating national intelligence officer for gray zone challenges

National Security Council Senior Director for Gray Zone Challenges

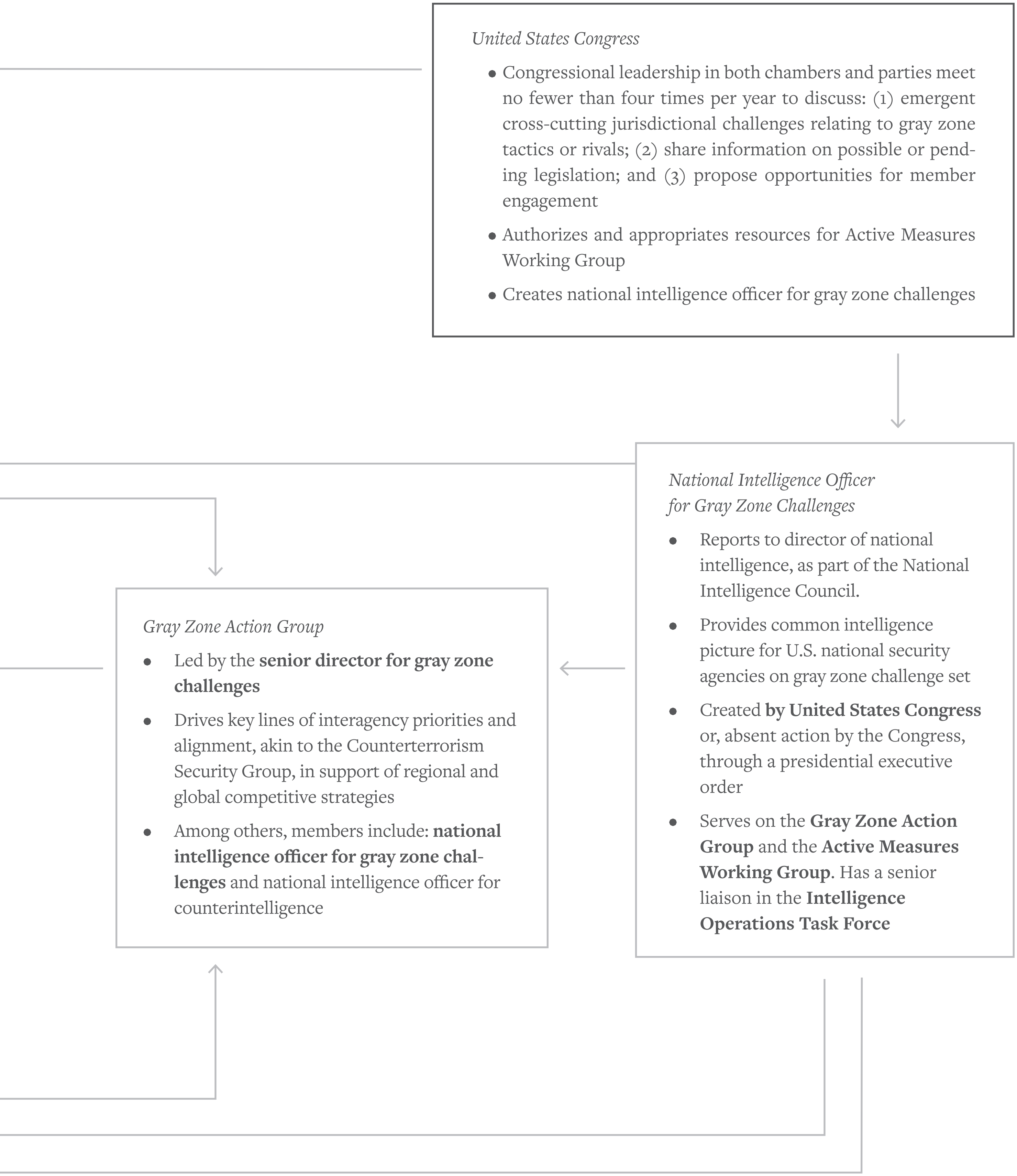
- Reports to the **President of the United States**
- Created by presidential national security decision directive
- Leads in developing and assisting priority action to the gray zone campaign plan
- Oversees the **Gray Zone Action Group** and the **Intelligence Operations Task Force**

Intelligence-Operations Task Force

- Led by **senior director for gray zone challenges**
- Develops gray zone campaign plan and serves as core staff driving interagency and intelligence implementation through **Gray Zone Action Group**
- Comprised of 10 experts drawn from across relevant foreign & domestic policy departments and agencies—including senior liaison officer who also reports to the **national intelligence officer for gray zone challenges**
- National Security Council Deputies' Committee assesses task force performance after one year; task force is scalable over time

Active Measures Working Group

- Housed in the Central Intelligence Agency (CIA)
- Separate, but linked to National Security Council staff, departments, and agencies through the **Gray Zone Action Group**
- Carries out covert action efforts related to the **Gray Zone Action Group**
- Among others, members include: s**enior director for gray zone challenges** and **national intelligence officer for gray zone challenges**



United States Congress

- Congressional leadership in both chambers and parties meet no fewer than four times per year to discuss: (1) emergent cross-cutting jurisdictional challenges relating to gray zone tactics or rivals; (2) share information on possible or pending legislation; and (3) propose opportunities for member engagement
- Authorizes and appropriates resources for Active Measures Working Group
- Creates national intelligence officer for gray zone challenges

National Intelligence Officer for Gray Zone Challenges

- Reports to director of national intelligence, as part of the National Intelligence Council.
- Provides common intelligence picture for U.S. national security agencies on gray zone challenge set
- Created **by United States Congress** or, absent action by the Congress, through a presidential executive order
- Serves on the **Gray Zone Action Group** and the **Active Measures Working Group**. Has a senior liaison in the **Intelligence Operations Task Force**

Gray Zone Action Group

- Led by the **senior director for gray zone challenges**
- Drives key lines of interagency priorities and alignment, akin to the Counterterrorism Security Group, in support of regional and global competitive strategies
- Among others, members include: **national intelligence officer for gray zone challenges** and national intelligence officer for counterintelligence

RECOMMENDATION

Reform the U.S. policy process to achieve strategic action and better link operations to strategy

Actions for the U.S. Administration

- Issue a presidential national security decision directive to elevate the full spectrum of competition, including its gray zone elements and its importance as a national priority. Define U.S. desired outcomes, priority lines of effort, role clarity for U.S. agencies, and an interagency process to drive innovation and accountability through regular monitoring and evaluation of performance. The directive should:
    - Specifically call for the creation and continual assessment and updating of comprehensive, cost-imposing U.S. strategies for China and Russia, prioritizing a China strategy first.[213]
    - Create an NSC senior director for gray zone challenges to coordinate and monitor action across the interagency, in support of the China and Russia strategies and broader policy development. This would be consistent with and could fulfill the existing statutory requirement to appoint a coordinator for combating malign foreign influence operations and campaigns.[214] The senior director would put priority on leading development of the gray zone campaign plan with its three lines of effort and priority action areas.
    - Specify the responsibility of the NSC senior director to oversee an interagency GZAG, akin to the Counterterrorism Strategy Group.
    - Establish an intelligence-operations task force, reporting directly to the newly established NSC senior director. It would require the NSC senior director to report within 365 days of their appointment on recommended mechanisms for improving the link between intelligence and operations within the task force's scope of interest. It should specify the need for the director's evaluation to include assessments of JIATF-like models and mission manager authorities for specified high-priority mission sets.[215]
- Identify and assign up to 10 detailees from across the interagency to staff the task force. Require that appropriate private-sector experts are identified and cleared for consultation as needed.
    - This should be incentivized as a rotation that links to career advancement to attract the best talent.

→ AUTHORITY, ORGNANIZATION, AND POLICY CHANGE

Actions for the U.S. Congress

- Require the president to submit with the proposed FY2021 budget: a strategy for China and a strategy for Russia, both of which include supporting documentation that links departments' and agencies' submitted budgets to the strategy.
- Require the president to submit updates to both strategies, inclusive of budget crosswalks, in FY2022.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Congressional leadership of both parties and across both chambers should meet no fewer than four times per year to achieve the following objectives: (1) raise emergent cross-cutting jurisdictional challenges relating to evidenced gray zone tactics or rivals (domestic and foreign); (2) share information on possible or pending legislation relevant to the challenge set; and (3) propose opportunities for member engagement in the issue space.
    - The Senate's bipartisan National Security Working Group should address these same three objectives, expanding membership as needed to ensure strong representation and linkages across domestic security, foreign, and defense committees.
    - The leadership of the House of Representatives should establish a bipartisan National Security Working Group, similar to that in the Senate, and include within its mandate the need to achieve the three objectives cited above.

⟶ **AUTHORITY AND RESOURCE CHANGE**

RECOMMENDATION

Improve intelligence and warning to close the action-reaction gap

Actions for the U.S. Administration

- Absent Congressional action (see below), issue an executive order to create a NIO for gray zone threat fusion.
    - The NIO should have an emphasis on warning for gray zone developments, including three key attributes: information integration and data visualization; a feedback mechanism to improve the action/reaction cycle; and the ability to leverage cooperation with the private sector and with allies and partners.

⟶ **AUTHORITY, ORGNANIZATION, POLICY, AND CAPABILITY CHANGE**

- Appoint a senior official with substantial career intelligence experience to the NIO position.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Deconflict and research efficiencies that could be gained through shared expertise and mechanisms at the NCTC and the CTIIC in creating a new NIO for gray zone.

⟶ **POLICY CHANGE**

- Establish an interagency active measures working group, separate but linked to the GZAG, focused on covert action efforts, making the NSC senior director and NIO for gray zone fusion members of the group.

⟶ **AUTHORITY AND RESOURCE CHANGE**

Actions for the U.S. Congress

- Authorize the creation of an NIO for gray zone threat fusion within the NIC.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Require the administration to report on what deconfliction and efficiencies can be achieved in sharing expertise and mechanisms with NCTC and CTIIC.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Authorize and appropriate resourcing for a new, interagency active measures working group, hosted by the CIA and linked to the GZAG, with requisite authorities and resourcing for information operations programming, convening authority, and for working group operating costs.

⟶ **AUTHORITY AND RESOURCE CHANGE**

PRIORITIZING KEY CAPABILITY INVESTMENTS

U.S. government capabilities will need to be honed to address the unique gray zone challenges that competitors present. Two capability areas merit substantial investment and alignment of concerted action: strategic communications and national cyber capabilities.

Strategic Communications

The U.S. government must bring policy, organizational, and resourcing focus to elevating information as a critical domain of statecraft. Recent advances in data-driven technologies have elevated information as a source of power to influence the political and economic environment, to foster economic growth, to enable a decision-making advantage over competitors, and to communicate securely and quickly.[216] As a result, the U.S. approach must shift from reactive to proactive. A new approach to strategic communications should infuse guiding principles of transparency, unity of effort, and avoiding the tyranny of over-classification or holding back information to use for bureaucratic or institutional advantage. The NSC senior director for gray zone challenges should assign clear roles and responsibilities to drive the strategic communication effort, in accordance with department and agency statutes and thinking beyond traditional national security agencies and tools. Priority should be placed on facilitating the sharing of relevant information with the American public and mobilizing private-sector engagement. The U.S. government should also open engagement with civil society as an independent check on government action and messaging. It should seek to coordinate and synchronize narrative themes with allies and partners while calibrating action in cases where elements in these countries may have been co-opted by U.S. competitors.

The NSC senior director should run an interagency process (via the GZAG described above) aligning both domestic and national security policy efforts to further this strategic communications effort with three major lines of effort. First, DHS should lead overall coordination with other departments and agencies on the domestic effects of foreign operations to influence U.S. territories and constitutional institutions. Key initiatives across the domestic-facing interagency should include coordinated messaging themes warning of foreign influence operations at home, providing civic education and media literacy grants, and developing recommendations for how to regulate social media. Second, DoS should lead overall coordination with other departments and agencies on the effects of foreign information operations overseas and promulgating messaging abroad. Third, the administration should re-establish a form of the active measures working group as a U.S. interagency committee hosted by the CIA and linked to the GZAG to drive investigation and exposure of disinformation and to conduct information and covert action operations abroad (as described above).

Strategic Communications Gap. The United States has long struggled with a gap in building a public narrative about national security challenges at home and abroad to counter foreign disruptive messaging and disinformation. The Eisenhower administration created the U.S. Information Agency (USIA) in 1953 to direct and operate many of the U.S. government's activities intended to inform and influence foreign audiences. Its objectives were to convey the U.S. government perspective, counter propaganda, develop local capacity to counter disinformation, increase transparency, and engender a desire for democratic freedom. It sponsored educational exchanges among public- and private-sector experts and provided support to libraries, book publishing, and speaking tours. It produced media, operated news services (e.g., Voice of America), and helped the private sector and the U.S. media reach audiences abroad. At the end of the Cold War, as its mission became less clear, as its effectiveness was debated, and as budget efficiencies were sought, Congress dissolved the USIA and broke it into parts, some of which reside within DoS.[217] Its broadcasting functions were spun off into the separate Broadcasting Board of Governors, which still operates today as the U.S. Agency for Global Media, but only has a narrow mandate.[218]

Today, the Global Engagement Center (GEC) within the Department of State fulfills part of the USIA mandate, with a focus on countering propaganda and disinformation from both state and non-state actors. GEC's efforts have suffered from the mismatch of U.S. priorities and responsibilities with foreign and domestic efforts. While the GEC has legislative authority to combat information operations and narratives that run counter to U.S. interests abroad, similar domestic efforts currently have no clear lead nor an allocated funding stream. Furthermore, the GEC has not received adequate funding until recently, and even then, its annual process to justify and access funds from DoD is arduous. In addition, its vetting and accountability standards for grantees could be improved, so as not to inadvertently compromise or target legitimate information sources. A final challenge to the GEC is the overall weakness of U.S. indicators and warning for gray zone tactics, which hampers the speed and quality of follow-on messaging efforts.

Leveraging Lessons from Allies and Partners.

Australia, Sweden, France, and Latvia are positive examples of countries that have implemented measures to improve public awareness of gray zone activities. One popular measure is incorporating media literacy and electoral education into education systems. The Australian government has created general information operations awareness by sponsoring a free museum called the National Electoral Education Centre in Canberra that is devoted to informing the public about voting processes.[219] Sweden has implemented media literacy into its elementary and high school curriculum.[220] France's Education Ministry has added an elective on media literacy to national high school curriculum, with many calling for the courses to be mandatory.[221] These courses teach students how to judge content on sites like Twitter and YouTube, how to check facts, and even the basics of journalism (how they gather and confirm facts) to rebuild students' trust in the media.[222]

Latvia has been a leader in promoting civic awareness of gray zone challenges. Because younger Latvian generations were born after the fall of the Soviet Union and do not have the memory of living under the presence of an oppressive foreign power, the Latvian government has addressed this generational gap by including themes of resilience and civic responsibility in school curriculums for subjects like history, political science, and human security.[223] Furthermore, schools inform students about current security news, like why NATO has troops stationed in Latvia, and facilitate meetings with the troops of NATO's Enhanced Forward Presence, located at the Adaži military base.

By providing outreach to its school-aged populations, Australia, Sweden, France, and Latvia strengthened their narrative in gray zone competition and built up the resilience of its citizens against information operations and attacks on its electoral systems. This government-led initiative can provide a model for similar U.S. government-led projects that can build resiliency against gray zone threats such as information operations.

While Australia's museum and Sweden's new curriculum additions are strong examples of generalized awareness campaigns, some experts believe broad and generalized awareness campaigns of information operations are not as effective as targeted education of stakeholders, like those conducted by Sweden's Civil Contingencies Agency.[224] Because Sweden lists elections as a component of critical infrastructure, Sweden has effectively delegated authority and readily available funds to provide targeted trainings and informational sessions, like those for political party leaders, to better train and inform vulnerable groups.[225] Yet, scaling from such models for the U.S. population might be difficult.

Although government-led initiatives and international organization centers have produced important research, policy recommendations, and resilience efforts, civil society can play a vital role in providing an independent, third-party perspective. Because gray zone tactics are designed to sow doubt in the norms, values, and political procedures of the United States and its allies, unbiased and third-party research and projects have a legitimate role to play as they avoid accusations of political partisanship. Ukraine is one such country that faces a toxic political landscape aggravated by Russian information operations and political coercion. Ukraine mitigates these threats with a strong culture of civil society organization. The Ukraine Crisis Media Center counters information operations by providing news programs on television and online that are fact-checked for disinformation and misinformation by third-party journalists.[226] StopFake is another civil society group that posts reports on Russian false news, research on how to identify news as false or originating from Russia, and trends in Russian disinformation campaigns.[227] The Baltic Centre for Investigative Journalism brings together Latvian and other Baltic journalists to investigate "socially-disruptive issues such as corruption, non-transparency, money laundering, and press intimidation" to provide the public with objective reports to diminish the power of information operations seeking to divide social groups.[228] By offering the public multiple sources of unbiased news and research about Russian disinformation campaigns and false news, citizens have a stronger base to better inform themselves of the gray zone threats around them. ■

RECOMMENDATION

Elevate information as a critical domain of statecraft

Actions for the U.S. Administration

- As part of the presidential national security directive, designate the NSC senior director for gray zone challenges as the lead coordinator for the national security elements of strategic communications, with DHS as the lead agency to drive domestic efforts and DoS as the lead agency for overseas efforts. This effort should:
    - Ensure DHS's critical infrastructure protection efforts include information elements, especially regarding targets in the U.S. democratic and economic systems, and leverage intelligence from the new aforementioned fusion center to enable information sharing and resiliency investments in U.S. businesses;
    - Invest in research to determine which strategic communications techniques and methods are most useful at home and abroad;
    - Boost overseas engagement on countering disinformation and election security with allies, including with the Hybrid COE and in the Asia Pacific (e.g., Australia); and
    - Conduct information operations, leveraging intelligence and warning from the fusion center to be proactive.

⟶ **AUTHORITY, ORGNANIZATION, POLICY, RESOURCE, AND CAPABILITY CHANGE**

- Develop stronger standards within DoS for vetting and accountability for GEC grantees to prevent misuse and mistargeting of information campaigns.

⟶ **POLICY AND RESOURCE CHANGE**

- Develop coordinated information operations for DoD and the IC to reinforce overt DoS messaging and in support of the active measures working group.

⟶ **POLICY AND RESOURCE CHANGE**

- Leverage intelligence and warning from the fusion center to inform counterintelligence and law enforcement efforts in the FBI. The FBI and DHS should also continuously improve reporting mechanisms for the private sector, universities, political campaigns, and general public to access hotlines and public service announcements in the event of threats.

⟶ **POLICY AND RESOURCE CHANGE**

- Promote states' civic education and media literacy best practices and grant opportunities for U.S. public schools, community groups, and other elements of civil society via the Department of Education; DoD should promote civics education in DoD Education Activity schools.

⟶ **AUTHORITY, ORGNANIZATION, POLICY, RESOURCE, AND CAPABILITY CHANGE**

Actions for the U.S. Congress

- Authorize DHS as the lead domestic agency to counter information operations and disinformation affecting U.S. territories and constitutional institutions, in collaboration with other interagency actors; appropriate research and grant funding to enable operations; and designate a specific head for these activities within DHS. The FBI will retain its leading role for counterintelligence.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Increase appropriations for DOS overseas engagement, including for the GEC and for international education and exchanges, with priority resourcing for countering China and Russia.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Clarify authorities for strategic communications at home and abroad, given threats to U.S. territory and institutions; include a review of authorities for U.S. information operations and messaging abroad.

⟶ **AUTHORITY CHANGE**

- Develop social media regulation, including:
    - Formalizing information sharing mechanisms between the U.S. government and social media companies, using the "Global Internet Forum to Counter Terrorism" as a possible model;[229]
    - Improving information sharing with the IC. Information provided by social media platforms should be part of an all-source intelligence cycle;
    - Funding public research into countering evolving disinformation threats (e.g., integration of AI

systems into machine-driven communications tools for use in propaganda—MADCOMs, synthetic video, and personalized phishing, among others);

- Providing financial incentives for social media platforms to develop counter-disinformation tools that can be built into platforms or distributed to individual users at scale, like the Defense Advanced Research Projects Agency's media forensics program; and
- Establishing a social media oversight board, like the Privacy and Civil Liberties and Oversight Board, tasked with evaluating social media algorithms, misinformation, and disinformation based on common guidelines or policies. The board could provide independent oversight while protecting privacy equities and platforms' intellectual property.

→ **AUTHORITY, ORGNANIZATION, POLICY, RESOURCE, AND CAPABILITY CHANGE**

- Fully fund the already-passed Serve America Act to increase national service opportunities from 75,000 to 250,000 and review the forthcoming findings and recommendations of the National Commission on Military, National, and Public Service for further opportunities to improve civic engagement. [230]

→ **RESOURCE CHANGE**

- Authorize and appropriate resourcing for Department of Education grants on civic education and media literacy.

→ **AUTHORITY AND RESOURCE CHANGE**

- Authorize the Department of Education to require civic education and media literacy inclusion in grades K-12 or on standardized tests.
- Broaden authorities for U.S. Agency for Global Media to operate in media-competitive regions.

→ **AUTHORITY AND RESOURCE CHANGE**

National Cyber Capabilities

Although the United States has taken significant strides to recognize, organize, and resource for cyber challenges, greater policy prioritization, alignment with broader strategy, and resourcing is needed. These internal U.S. government challenges are not unique to competition and its gray zone elements but currently compound the U.S. government's present inability to fully align and leverage cyber capabilities in a campaign approach. Cyber challenges present a particularly pernicious source of gray zone activity, particularly when used in combination with information operations, and must be a central concern for adapting the U.S. government's approach.

RECOMMENDATION

Bolster national cyber capabilities

Actions for the U.S. Administration

- Appoint a cyber coordinator on the NSC staff to facilitate interagency collaboration and deconfliction, prioritizing homeland defense;

⟶ **ORGANIZATION AND AUTHORITY CHANGE**

- Prioritize and align cyber strategy and operations with competitive strategies and request additional resourcing from Congress for addressing the cyber and information operations nexus.

⟶ **ORGANIZATION, AUTHORITY, AND RESOURCE CHANGE**

- Align offensive cyber action with information operations and counter disinformation approaches, where appropriate.

⟶ **POLICY AND CAPABILITY CHANGE**

- Develop capabilities for offensive cyber operations for the defense of U.S. territory and institutions to deter and prevent adversaries from hacking in the first place.[231]
  - Guided by policies and procedures, these capabilities could include erasing computers at scale; disabling accounts and credentials used by attacking hackers; cutting off access to services; and making it harder to compromise innocent systems to conduct adversary attacks.[232]

⟶ **CAPABILITY AND RESOURCE CHANGE**

- Establish a set of norms for cyber policy that accounts for the domain's evolving complexity. Emphasize development of a holistic approach and create a code of conduct for offensive and defensive capabilities.

⟶ **AUTHORITY AND POLICY CHANGE**

- Buttress cyber alliances and partnerships abroad to share information, coordinate action, and build resilience, particularly on the nexus of cyber and information and disinformation operations.
  - Develop a common approach for 5G security.

⟶ **POLICY AND RESOURCE CHANGE**

- Develop mechanisms and incentives for collaboration and intelligence sharing with the private sector, building upon the Section 9 cybersecurity and Financial Services Information Sharing and Analysis Center examples.

⟶ **ORGANIZATION, POLICY, AND RESOURCE CHANGE**

- Ensure U.S. companies can continue to innovate and produce advanced technologies to compete overseas through supportive policies and grants.

⟶ **POLICY AND RESOURCE CHANGE**

Actions for the U.S. Congress

- Authorize and appropriate additional resourcing for offensive cyber capabilities.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Authorize and appropriate sustained resourcing for election cybersecurity, specifically for personnel and organization of DHS's Election Task Force, to prepare for the 2020 elections and long-term election security at the federal and local levels.[233]

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Authorize and appropriate additional resourcing for cyber strategy and operations in the gray zone, and particularly the cyber and information operations nexus.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Authorize and appropriate research and development resourcing for advanced technologies and for grants for the private sector. At the same time, aid government and the private sector in building resilience with "analog" back-up mechanisms.

⟶ **AUTHORITY AND RESOURCE CHANGE**

COALITION BUILDING WITH ALLIES AND PARTNERS AND THE PRIVATE SECTOR

Inducements for Allies, Partners, and Third Parties

The United States has significant, untapped potential inducements for other countries and third parties with which it wishes to collaborate on common competitive approaches. Although the United States is unlikely to match China's global investments, bolstering inducements for allies, partners, and third parties can activate networks to focus on common priorities and build resiliency in ways that will enable other lines of the U.S. campaign plan. Key tools for allied, partner, and third-party engagement abroad include: international trade and free trade agreements; targeted international development and stabilization assistance in fragile and contested spaces; use of the forthcoming U.S. International Development Finance Corporation (USDFC) (from the BUILD Act) to spur growth in competitive regions; providing security-sector assistance to priority allies and partners; accelerating targeted energy resilience programming to critical countries; and broadly, creating bilateral and multilateral compacts to induce change and commitment to common approaches that directly or indirectly reduce global competitive space, making countries more resilient to penetration by competitors.

RECOMMENDATION

Build and leverage inducements for allies, partners, and third parties

Actions for the U.S. Administration

- Reinvigorate goodwill toward the multilateral approaches necessary for gray zone competition. Leverage allied and partner advantages in the gray zone as part of U.S. strategy to fill gaps and offset risk. Buttress tools for allied, partner, and third-party engagement, including:
  - International and free trade agreements;
  - Targeted international development and stabilization assistance;
  - Strategic investments in security cooperation and security-sector assistance to increase interoperability, enable access, and build partner capacity and resiliency;
  - Accelerated implementation of the BUILD Act and stand up of the USDFC; and
  - Bilateral and multilateral compacts to induce change and commitment to common approaches that directly or indirectly compete with actors that deploy gray zone tools, reduce competitive space, and increase resiliency to gray zone penetration.

⟶ **POLICY, CAPABILITY AND RESOURCE CHANGE**

- Collaborate with allies and partners to develop their own Committee on Foreign Investment in the United States-like mechanisms to block investments by competitors that have backdoor capabilities to threaten critical infrastructure or have nefarious intent, including via foreign government ownership or leverage that could be used to disrupt supplies and services. Share information among allies and partners to inform decision-making.

⟶ **POLICY, CAPABILITY AND RESOURCE CHANGE**

Actions for the U.S. Congress

- Authorize and appropriate resourcing for targeted development, stabilization, and security-sector assistance.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Authorize and appropriate new and agile DoS and DoE programming for allied and partner energy resiliency.

⟶ **AUTHORITY AND RESOURCE CHANGE**

Mobilizing U.S. Citizens, Civil Society, and the Private Sector

On the domestic front, the U.S. government should elevate strategic investments in partnerships across businesses, universities and schools, civil society, and the broader public to spur innovation to maintain America's competitive edge. The federal government should look to research and development grants, scholarships, and as previously described, information and intelligence sharing on common threats to inform planning.

Increasing partnerships and engagement with the private sector will be critical to ensuring the resilience of the U.S. economy to gray zone penetration, harnessing innovations and best practices for countering harmful gray zone activities, and bolstering U.S., allied, and partner competitiveness in foreign markets. This approach requires trust. It could well be in tension with some elements of the private sector which prize their independence, doubt U.S. government motives, have incentives to work with and within competitor markets (especially China), and do not wish to be treated as surrogates of the U.S. government. While some European allies to the United States have far different relationships with their private sector—as demonstrated by EU actions against social media companies in response to privacy concerns and hate speech—and though the U.S. government has historically successfully worked and supported private-sector industry to encourage mutual growth and innovation, today's environment is more complicated.[234] However, cooperative examples like DHS's Section 9 cybersecurity initiative and the Financial Services Information Sharing and Analysis Center provide compelling demonstrations of partnerships with the private sector, as discussed earlier in this report.

RECOMMENDATION

Build and leverage partnerships within U.S. society

Actions for the U.S. Administration

- Offer incentives for U.S. businesses, educational institutions, and civil society to invest in and catalyze U.S. innovation. Prime areas for investment include:
  - Federal research and development in critical technological areas;
  - Public-private collaboration efforts aimed at creating opportunities for private-sector initiatives to reduce known weaknesses to gray zone tactics, including providing greater transparency on foreign sources of social media posts;
  - Cyber defense incentives—including information and intelligence sharing—for companies that report malign influence, like social media platforms; and
  - Support for science, technology, engineering, and math (STEM) education, including scholarships and H1B visas for highly skilled workers.

⟶ **POLICY, CAPABILITY AND RESOURCE CHANGE**

- Review and expand the definition for what constitutes critical infrastructure to include priority targets in the private sector from nation-state competitors and include threats from information operations.

⟶ **POLICY CHANGE**

- Expand existing partnerships with key sectors, particularly energy and telecommunications companies. Increase inducements and declassify more intelligence or privileged information important for critical infrastructure security to inform risk-based scenario planning and common playbooks for prevention and response.

⟶ **AUTHORITY, POLICY, CAPABILITY, AND RESOURCE CHANGE**

Actions for the U.S. Congress

- Authorize and appropriate resources to DHS to support grant and information sharing and collaborative partnership opportunities, including on joint incident response, with the private sector.

⟶ **AUTHORITY AND RESOURCE CHANGE**

- Authorize and appropriate resourcing for federal research and development in critical technological areas, incentives and grants for the private sector, grants and scholarships for STEM education, and H1B visas for highly skilled workers from abroad.[235]

⟶ **AUTHORITY AND RESOURCE CHANGE**

Conclusion

Rivals may seek to undermine the foundations of U.S. strength. However, the United States has strategic asymmetries to compete and push back—if these are matched with political leadership to recognize the gravity of this moment and to undertake necessary reforms. Changes to U.S. organization, authorities, policies, and capabilities must be prioritized to catalyze innovation, harness strategic action, build coalitions, and bolster institutional resilience. Concerted bipartisan leadership and action is needed now to affect these reforms. No less than the strength of U.S. institutions, economic vitality, and influence abroad is at stake.

CASE STUDY: WARNING FOR THE GRAY ZONE

by Lindsey Sheppard and Matthew Conklin

Identifying and assessing the true nature of gray zone threats is intrinsically the intelligence mission, guided by the policy priorities set at the national level.[236] Gray zone campaigns are challenging given that warning requires detection of a weak signal through global noise and across threat vectors and regional boundaries. Such activity exists below the threshold of armed conflict but within the bounds of competition, obscuring intent, capability, and impact. Gray zone activity is most effective when malign activity is executed within legal boundaries so as not to set off any alarms or cross traditional warning trigger points, further weakening the signal.[237] Thus, warning in the gray zone means identifying and assessing new patterns throughout new sources of data.

This paper will discuss how intelligence, and particularly geospatial intelligence, can be collected, analyzed, and applied to better identify and enable the United States to anticipate and respond to gray zone challenges. It details past examples in which the United States effectively applied tools to monitor and respond to gray zone challenges. Key examples highlighted include China's reef dredging in the South China Sea and Russia's use of non-uniformed combatants in Ukraine. Interviews with representatives from the private sector, government agencies, and nonprofit organizations contextualize these examples.

Attributes of Warning

The need to assess the threat and proactively compete in the gray zone shapes how, when, and where a tool or set of tools is used. That is, providing mission value is the core guiding principle in adapting the concept of warning, policy, and intelligence processes to drive an actionable product. However, the type of information needed for gray zone warning is often different from traditional concepts of warning. Many warning problems are often tied to the use of force. When the order of battle is known, such as intent indicated by force mobilization in armed conflict, warning indicators provide a path to an expected future state or outcome. While uncertainty and questions of confidence have always been a staple of warnings and indicators, competing in the gray zone brings a new "order of battle" through competition in political, economic, energy, cyber, space, and information domains. As the United States increasingly finds itself confronting foreign threats in each of these spaces, policymakers will need to define new red lines, trigger points, and timelines. Critically, political and military leaders will need to sort through unprecedented amounts of intelligence to determine how to counter gray zone activities. As intelligence scholar Aaron Brantly describes, "Virtually every form of Technical Intelligence from SIGINT, MASINT, and IMINT (now GEOINT) to include the emerging fields of CYBINT and SOCINT (Social Media Intelligence) are expanding at near exponential rates. The signal to noise ratio within this data is very low, and vast collections of data make analysis extremely difficult."[238]

The overarching challenge finding the signal through the noise is posed by three interconnected gray zone elements: *temporality, attribution, and intent*. First, gray zone threats are *temporal* in nature. The nature of gray zone threats truly requires a "big picture view" over long timescales and across regions and functional topics. Identifying gray zone activity involves pattern identification. On their own, individual events are difficult to distinguish from one-off actions, statecraft, or diplomacy. This means that classifying an aggressive activity as gray zone is dependent on and informed by the analysis of aggregated data over a specified time period. For example, a seemingly routine diplomatic visit by a Russian official to a European capital might not be enough to raise suspicion about Russia's potentially malign interests in the country. Yet, if that instance of diplomatic activity is part of a larger trend or is the first visit of a broader pattern of future visits with similar characteristics, such as coercive economic dealmaking, diplomatic activity could be analyzed as a metric of gray zone behavior. Heather Conley, author of *Kremlin Playbook 2: The Enablers*, describes how Russia has strategically extended its coercive influence through financial and political networks over the years:

> *Austria, by cultivating its posture as a space between East and West, has exploited its unique position to make itself a crucial hub for Russian investments in Europe over the past fifteen years. It has attracted the presence and riches of many of the former Soviet Union party and secret service apparatchiks-turned-businessmen. Under the current chancellor, Sebastian Kurz, the Austrian government has protected and grown its economic relationship with Moscow. Chan-*

> *cellor Kurz visited Moscow in March 2018, and Vladimir Putin made his first post-reelection European visit to Vienna in June of the same year.*[239]

The temporality of gray zone threats requires the synthesis of observation with contextual understanding early in the identification and assessment process. Even rapidly advancing techniques, such as machine learning, are not well tailored to produce the necessary insight from time series data without the contextual knowledge and awareness of a human analyst. While machine learning may find the otherwise impossible to find insights and patterns, the human must make sense of whether that is a fair pattern worth exploration.[240] However, given the dual needs of temporal assessment, the promise of geospatial analysis is rooted in the "signal over time" nature of consistent earth observation. Earth observation provides one mechanism for addressing the time series element of certain activities to normalize variance by sampling a target area or region over time that may then be enriched with other sources of information. Capturing the temporal nature of gray zone activities provides one means to build a clearer picture around attribution and intent once HUMINT or SIGINT have directed the target region for observation. We will discuss in later sections how the availability and sophistication of commercial geospatial capability provides a means for addressing the need for high-quality imagery to assist the intelligence analysis process.

Second, *attribution* of an activity to an actor serves both to enable policy and operational decisions as well as public attribution. In support of policy and operational decisions, attribution often comes at a cost. Requiring an "almost certain(ly)" or "nearly certain" analytic assessment before acting costs time and analytic effort.[241,242] The cost of attribution for both policy and public purposes is heightened by the fact that much of the data needed to inform historical pattern analyses of large quantities of cyber-related information is owned by private companies.[243]

Further, while direct observation enables attribution, direct observation of gray zone activity rarely occurs. Consider the example of Russia's unidentified "little green men" in Crimea. While it was possible for analysts to infer from local commentary and on-the-ground reporting that the soldiers without insignia were Russian special forces, the judgment that Russia was covertly intervening in Ukraine involved contextualizing the

Cyber Attribution

The weak signal nature of gray zone activity presents challenges for attribution. As an example, the 2018 Office of the Director of National Intelligence (ODNI) Guide to Cyber Attribution addresses the difficulties of (cyber) attribution for policy and operational purposes:

> Establishing attribution for cyber operations is difficult but not impossible. No simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability. In some instances, the [intelligence community] can establish cyber attribution within hours of an incident, but the accuracy and confidence of the attribution will vary depending on available data.[246]

The ODNI report goes on to say: "The three primary indicators are tradecraft, infrastructure, malware, and intent. We also rely on indicators from external sources, such as open-source reports from the private cybersecurity firms."[247] Nonetheless, when the government does decide to publicly attribute a cyberattack to a foreign power, there is little evidence that denouncing a country that uses gray zone tactics will achieve the desired deterrent effect.[248]

presence of "little green men" within a larger trend pattern of Russia's strategic behavior.

However, while the intelligence community has become much better at attribution to inform policy decisionmakers of gray zone activities, making that attribution public is not the sole mechanism to deter adversaries that use gray zone tools.[244] As mentioned in the 2019 Worldwide Threat Assessment, the growing commercial availability of advanced cyber capabilities contributes to the noise of unattributed cyber activities in which ambiguous gray zone behavior thrives.[245]

In some cases, the investment in human and technological resources needed to reach a confident claim of attribution can be prohibitive. Denied or restricted areas may entirely prevent direct observation by civilian or military personnel.[249] Different units across the interagency maintain varying standards about the level of certainty needed to attribute gray zone activity to a foreign state. Across interagency units, the perception that 95 to 99 percent certainty in attribution is needed to authorize a U.S. response suggests an unrealistically high standard, especially in the dynamic and ambiguous context of the gray zone environment. Lessons learned from high conflict scenarios indicate that a lower threshold such as 80 percent certainty could be a suitable baseline for gray zone attribution. According to the ODNI: "No simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability."[250]

Public attribution may not be worthwhile in every instance, and more efficient mechanisms may be needed to ensure an agile response while also pursuing approaches that allow for direct observation sooner.[251] For example, although the Federal Bureau of Investigation (FBI) continues to release cyber advisory warnings to industry partners that attribute malign activity to North Korean cyber agents, the advisories state that such attribution is unlikely to deter future cyber operations.[252] "In conceding that attribution will not change North Korea's calculus in cyber space," writes Sean Lyngaas, "the FBI is reiterating what is widely recognized in the cybersecurity industry: that Kim Jong Un's regime is too brazen to care about being called out for its hacking."[253]

Third, the challenges associated with temporality and attribution directly influence the *judgement of adversarial intent* to conduct gray zone activity. Indeed, the purpose of countering gray zone threats is to deter an adversary from fulfilling its intent to act. Yet, making a determination about actor intent is a purely retrospective assessment based on the collective analysis of various indicators. While attribution is one piece of the puzzle, closing the space around intent often means synthesizing multiple relevant indicators and warnings, including the state's geopolitical ambitions, military ties, trade and investment, level of corruption, and media landscape, among others.

The process of characterizing adversarial intent is illustrated in the case of China's reef dredging in the South China Sea, where geospatial imagery revealed that Chinese vessels were building islands in contested waters. Publication of these findings brought pressure on the Chinese government to respond to international questioning. Consequently, China's official statement in response was widely interpreted as evidence of the government's expansionary ambitions. This response is an example of the U.S. reliance on "naming and shaming" adversaries that use gray zone tools as a deterrence technique. It is important to note that the applicability of the traditional indicators and warning metrics depends on the local environment. For example, among some military analysts, indicators and warnings are thought to be less applicable to maritime gray zone activity. Instead, qualitative measures may be more useful for policymakers in the maritime domain.[254] According to intelligence studies scholar James Wirtz, one such example would be the observable effects generated by a military's decision to mobilize forces on a large scale. "The movement of forces from a day alert to a generated alert status," Wirtz writes, "often creates a string of observable actions that can be detected by the collection efforts of oppositional intelligence agencies."[255]

As two notable examples of gray zone activity, China's reef dredging in the South China Sea and Russia's military intervention in Crimea highlight the various challenges inherent in the three themes of temporality, attribution, and intent. Chinese and Russian objectives and execution differed in these cases, but their tactics—leveraging ambiguity to delay response and ensuring that their activities fall short of direct conflict with the United States or regional countries—are largely the same, underscoring the presence of a persistent dilemma for U.S. policymakers and operators.

Challenges and Constraints

Adapting to the challenges of gray zone warning requires addressing constraints within both policy and intelligence processes. The constantly shifting and ambiguous nature of gray zone threats exposes vulnerabilities in the U.S. toolkit. For example, the applicability of geospatial data to predicting emerging gray zone threats assumes that geospatial imagery of the specific region is strategically important to the gray zone mission. In other words, for the United States to excel in the gray zone, it must first know what it is looking for. It is therefore crucial for defense and foreign policy practitioners to apply a shared analytical framework—or common threat picture—to identify, analyze, and respond to gray zone threats. However, process flow, lack of communication, unclear policy direction, and structural silos are barriers to cohesive interagency coordination and shared threat assessments and priorities.[256]

Policy Challenges and Constraints

Through gray zone activities, actors seek to gradually change the competition environment. This incremental approach to competition often resembles the "boiling frog" fable, resulting in the United States acclimatizing to a new normal. This poses challenges to warning over long-simmering timeframes and across sectoral boundaries. When addressing gradual or incremental changes in the competition environment, the United States often confronts competing priorities in near-term gains versus long-term strategy goals or threats within a political structure that favors the near-term. Particularly when legal boundaries are not clearly violated, discerning the true nature of gray zone activity as well as the appropriate response similarly puts the near-term and long-term at odds, while also crossing public-private and foreign and domestic policy boundaries. Economic gray zone activity by China demonstrates the challenges of resolving near-term priorities with the recognition of a long-term campaign; addressing Chinese intellectual property theft, the Belt and Road Initiative, and growing dominance in the telecommunication market risks upsetting the balance of trade and other existing relations. When responses are undertaken, a gap exists in policy and process between U.S. strategic intent to compete in the gray zone—as articulated through the National Security Strategy and the National Defense Strategy—and the plans, tasks, and activities that various U.S. government organizations are undertaking. As a result, U.S. efforts may be uncoordinated and stove-piped and may miss opportunities to be proactive. The result is unclear prioritization and resource allocation for driving intelligence prioritization, collection, and analysis.

While timely and meaningful analysis of gray zone activities means the intelligence community must utilize new sources and methods, the process of addressing these collection needs can be accelerated when there is a clear policy priority. Problem prioritization can be a strong driver of maturing analytic methods. In the absence of clear policy prioritization along the chain of command, however, elements across the interagency tend to remain in their familiar context and problem-specific domain. While the post-9/11 dominance of the counterterrorism mission incentivized interagency units to justify their relevance in terms of combating terrorism, the centrality of a single mission highlights the need for leadership at the management level of the national security enterprise. While the counterterrorism mission was elevated to functional management to address similar challenges, for instance, it is at present less clear how agencies should compete in the gray zone.

Intelligence Process Challenges and Constraints

Gray zone campaigns challenge the intelligence community's organizational structure as well as tried and true processes. Effectively addressing the gray zone through the intelligence process necessitates adapting the existing practices and processes to the nature of the activity. New data requires new sources, methods, and collection. Evidence of gray zone campaigns often exists in open-source environments or within the private sector. Particularly in the case of economic warfare, the intelligence community is not well positioned to assess activity. The collection infrastructure built up during the Cold War, designed to siphon state secrets over decades, is ill-suited to provide similar value in the economic gray zone.

Regardless of gray zone activity type, addressing the three gray zone warning elements—temporality, attribution, and intent—requires data visualization, the fusing of multiple sources, and mechanisms to make a reasonable judgement in uncertain circumstances. No single intelligence method, source, or analytic package may completely solve this puzzle—each is one tool in the toolbox, the suite needed to provide mission value. The modality of the indicators inherently impacts the efficacy and applicability of a toolkit. For example, while geospatial data may provide a means for assessing indicators with geographic and time-based significance, it requires other means to incorporate the relevant cultural context. Without tailoring the tools and process to the nature of the threat, a generic toolkit is otherwise applied blindly. For cyber and related technical analysis in particular, it is easy to overemphasize a tool's technological capabilities at the expense of the user's relevant cultural knowledge. When making analytical inferences based on satellite imagery, it may be critical to incorporate local cultural knowledge about the geography under examination.

Further, the guiding process itself must evolve around the sources, methods, and analytic techniques. Like the gray zone threat, the process must similarly be dynamic. It must be flexible, adaptable, and iterative, and it should continuously experiment, test boundaries, and incorporate lessons learned to achieve outcomes. Process and analysis must reach across single threat vectors to look holistically across functional areas, technologies, and regions to surface the emergent issues to inform and shift resources. Moreover, for analysts to evaluate whether an activity under observation does in fact constitute gray zone behavior, they rely on an established set of classification types (e.g., people, activities, and traits) that correspond with collection and analytic priorities detailed in strategic documents like the National Intelligence Priorities Framework.

Unfortunately, long-established processes are not sufficiently elastic to adapt to the different kinds of data and information. Collection emphasizes tried and true sources and methods, but misses shifts toward open-source commercial research, development, and innovation. To be sure, radar engineers or nuclear scientists still have access to important state secrets. However, capability is increasingly built in the open through publicly available data sets, algorithms, and software. Further, the editorial structure of analysis may be well-suited for explaining the political behaviors of an individual or country, but it is not well-suited to conveying or exploiting rapid computational advances requiring a technical background—a significant constraint in the Information Age. The process to review and elevate analytic products may rely on regional silos, generic language for a broad audience, and a management structure unfamiliar and uneasy with technical terms and concepts. For example, an analytic product assessing Chinese economic activity in telecommunications and semiconductors crosses regional boundaries and requires an understanding of next generation telecommunication infrastructure, a complex technical topic. Restricting analysis to one region and excluding the engineering nuance to increase accessibility to a general audience paints only one part of the larger, richer picture required to bring the gray zone campaign into focus.

Further, it may be difficult for GEOINT or SIGINT analysts to know what they are observing is a priority—or more importantly if it might be salient to an incipient gray zone threat—because the analysts detecting change on the ground are not always privy to the higher-level discussions between the Director of National Intelligence, Defense Intelligence Agency (DIA), or the Central Intelligence Agency (CIA) that establish collection and analytic priorities. This challenge relates to the inherent obstacle of collection lag time in the intelligence cycle. If analysts do not have the assets they need, analysts need the ability to take initiative in thinking what relevant assets and resources could assist their mission and how to obtain them. In light of this, it is important for analysts to know what they are looking for if the United States is to mount a credible response to gray zone threats and to be able to fuse intelligence across sectors and agencies.

Global Trends Constraining Gray Zone Warning

The increasing utility of competition below the threshold of armed conflict is amplified by global technology trends. The globalization of priority technology means that adversaries, allies, and partners alike have easy access to highly capable, relatively affordable technology. While the United States strives to maintain a persistent technical advantage, other states are building more robust and diverse technology portfolios. While learning to adapt to the threat posed by gray zone adversaries, the United States must simultaneously strive to keep its lead on research and development and, perhaps most importantly, deployment. The agility of gray zone threats requires a response that operates and evolves on similar time scales. Technology trends directly affect gray zone warning, as warning also requires new sources of data and new methods to find timely and meaningful indicators. For example, the steady forward march of fifth generation (5G) wireless and the Internet of Things has strategic competitors facing off in regulatory and standards-setting bodies while free market economies contend with aggressive semi-state-backed corporations. As nations exert influence in regulatory bodies, assessing the electromagnetic spectrum needs of wireless devices with spectrum allocation may reveal intent and expected capability in a future with ubiquitous internet. In this instance, the gray zone signal is found through analysis of highly technical yet open source standards.

Meanwhile, further complicating a credible U.S. response is the varying degrees to which *allies and partners* perceive foreign adversaries as posing a gray zone threat. Actors and effects are entangled in economic and political structures, posing difficulties in identifying problems. For example, variance across ally and partner perceptions of Russia's gray zone activities or the transregional nature of Chinese economic coercion may impede a unified effort to track gray zone actions. Further, there is a growing uncertainty among foreign policy commentators about the degree to which future interallied gray zone responses will be possible due to disparities in common understanding of threatening activity and lack of strong national narratives on gray zone challenges.

Finally, distrust between the private and public sector can undermine cooperation on gray zone warnings. Collaboration with the private sector requires rebuilding relationships between a national security enterprise and privately-sector innovation base that are deeply skeptical of one another. Positive engagement is critical to counteracting the damage from leaks and opaqueness of activity. For those entities actively willing to support the national security mission, coordination through non-traditional contracting mechanisms and active investment in application provides the necessary support to private-sector firms. However, active cooperation between public and private actors also requires highlighting the risks now facing many companies in the global economic and security environments. While early 2019 exposed questionable applications of facial recognition technology in China, it similarly brought to light the dangers facing U.S.-based entities who wish to conduct research and business in China. Microsoft Research Asia, a Beijing-based Microsoft research organization, faced scrutiny in April 2019 on its decision to partner with a Chinese military-run university for research in artificial intelligence (AI) that could further human rights abuses of the ethnic minority Uighur population in Xinjiang.[257] Further, awareness of alleged sanctions violations by Huawei Technologies and ZTE Corp led the Massachusetts Institute of Technology to sever ties with the Chinese-based telecommunications firms.[258]

Framework for Gray Zone Warning

The reality is that not every question worth answering has unlimited resources, and the fidelity of information is not consistent across all regions or functional areas. The availability of quality open-source information provides an opportunity to build products and analysis prior to problem prioritization. As the value and availability of information has increased significantly, observation, attribution, and intent increasingly may be based on open-source information.[259] In fact, commercially available open-source satellite imagery has provided an avenue for identifying and assessing gray zone campaigns and then aligning national resources to refine the understanding of events, attribution, and intent.

One key criterion for gray zone warning frameworks is to *integrate disparate sources of information into a cohesive, actionable product*. Data visualization combining various sources of such information allows for the understanding of broad sets of activity on an ongoing basis to support a reasoned assessment. Data analytics and visualization evolved alongside the counterterrorism mission throughout U.S. involvement in the Middle East following the events of September 11, 2001. While analysts early in the conflicts cobbled together their own interfaces and visualizations to layer the necessary information, the mission value drove the creation of various data integration and visualization platforms. Geospatial analysis is in similar early stages. Satellite imagery of North Korea's nuclear test sites and previously undeclared missile locations has brought GEOINT front and center to mainstream audiences. Open-source geospatial information combined with additional sources provides an accessible mechanism to close the space around attribution and intent of adversary actions in the gray zone. According to a recent annual assessment of the GEOINT community:

> *"The consumption of GEOINT data, products, and services should be self-service, because all produced intelligence, along with the source information that went into it, can be found on the platform. Operators would not need to wait for the finished report; they could just pull the raw information from the platform and filter for available GEOINT analytic reports."*[260]

Through a common information-integrated picture, all actors—ranging from multiple interagency entities to various U.S. allies and partners—could be on the same page before initiating both defensive and offensive gray zone approaches. Quickly integrated and widely-shared information enabled one of the most effective responses to gray zone action to date: the multinational response by Western governments to the March 2018 Skripal poisoning attacks.[261] Usefully, U.S. Southern Command is sharing best practices with other combatant commands on how it leverages analytic toolkits like the Joint Improvised Threat Defeat Organization's VOLTRON suite to identify, monitor, and evaluate threats in their area of operations.[262]

Information integration tools provide an advantage to analysts with their capacity to make sense of seemingly disparate data points. Information integration and data visualization tools are especially effective ways to differentiate the signal from the noise in complex, unfamiliar spaces conducive to gray zone activity. For example, in the domain of economic coercion, flows of foreign capital, particularly those from state-backed corporations, could be used to infer the science and technology priorities of strategic competitors investing in firms abroad. Identifying which companies are offered even seemingly small investments from state-affiliated entities is a nontrivial signal of the state's strategic interests. Recently, researchers published an impressive online transparency platform that exemplifies the potential for open-source research to complement the government intelligence process. "Mapping China's Tech Giants," an initiative of the Australian Strategic Policy Institute, tracks the global expansion of 12 Chinese technology companies. The interactive map features an extensive database of information documenting China's involvement in overseas 5G networks, smart cities, and university and research partnerships. Through bringing together disparate sources of information to reach a judgement of intent, the report's authors conclude that Chinese internet and technology companies are not exclusively commercial actors, due to the public-private ties with the Chinese Communist Party.[263]

Data integration tools help analysts understand who and what matters most to a gray zone operation area and why. For example, several years' worth of satellite imagery could help determine the health of local crops. Combining imagery analysis with HUMINT cultural knowledge of interpersonal connections could be visualized through lines of relation between people, activities, and economic information. These models could allow policymakers to conceptualize connections that were otherwise not readily apparent. The point is that combining HUMINT with GEOINT and SIGINT for a geographic area would assist the analyst and local operations in understanding a particular gray zone context.

A second key criteria of a gray zone warning framework is a *feedback mechanism to close the action-reaction cycle*. Feedback loops adapt to the culture and context of the threat activity. Intelligence observes and assesses; separate organizations execute action. A feedback mechanism allows for the evaluation of how well the response is addressing the threat action and to adjust if necessary. The gray zone threat is by definition adaptable and flexible, meaning feedback is necessary to adapt the response accordingly. Once the product feedback loop is closed, U.S. interagency actors may become more proactive, as opposed to reactive, shifting the mindset from purely defense to driving the cycle through offense.

Feedback throughout the action-reaction cycle must also occur within sustained, tailored activity. Information operations demonstrate the necessity of context-specific responses, rather than a "one size fits all" approach. As an example, Russian tactics in Serbia are not equivalent to Russian tactics in Ukraine. While Finland's highly educated population and centralized whole-of-society defense make it resilient to Russian disinformation, state corruption in Ukraine and Georgia present opportunities for malign disinformation tactics.[264] Finland, ranked the third-least corrupt country in the world, is also less susceptible to Russian disinformation compared to former Soviet states with large Russian-speaking populations. In other words, a country's specific social, cultural, and political profile shapes which tactics the aggressor state will employ in the gray zone.[265] While existing programs are tailored, the process of refining based on the cultural context must be improved. Further, current operations build in doctrinal vulnerability by deemphasizing the sustainment: drop-offs or halts in proactive messaging create an information void that may then be filled by an adversary. Incorporating feedback throughout a counter-disinformation campaign while also using persistent messaging—leveraging the realities of human cognitive biases—has demonstrated results in successfully protecting populations against disinformation.

Finally, *effective warning in the gray zone involves active cooperation*, between allies and partners as well as public and private actors. The combined response to the Russian attack on the Skripals in the United Kingdom demonstrates the efficacy of collective responses and actions from allies and partners. Best practices have arisen from coordinating responses with allies and partners. Nordic partners on the front lines of Russian influence are well positioned to share toolkits and educate politicians on countering and preparing their citizens for disinformation campaigns. The December 2018 international condemnation of China's cyber theft of sensitive information from private companies and foreign governments required multilateral coordination and active cooperation. In cooperation with the U.S. indictment of Chinese hackers, the UK National Cyber Security Centre (NCSC) similarly attributed the illicit cyber activity to an organization affiliated with the Chinese Ministry of State Security.[266] Earlier in 2017, the NCSC collaborated with private-sector companies to identify the Chinese hacker group and provide guidance to companies on how to guard against the cyber threat. Multilateral coordination between governments victimized by China's intellectual property theft—including U.S. allies such as Germany, Australia, Canada, and Japan—enabled a strong multilateral condemnation by the international community of China's illicit behavior.

Technology is fast moving, particularly when functionality is based in software, and collaboration with private entities allows for better awareness of and access to outside innovation. In the months following Russia's 2014 invasion of the Crimea, private-sector researchers demonstrated the potential of using open-source geospatial data from social media to establish the identity and location of Russian soldiers in Ukraine. Bellingcat—a research and investigative journalism organization—and the Atlantic Council Digital Forensics Lab disseminated open-source research on Russia's intervention in Crimea for public consumption.[267] According to one government agency, collaboration with think tank researchers on projects such as the CSIS Asia Maritime Transparency Initiative represents the type of partnerships that can effectively raise public education about gray zone threats.

Successfully distinguishing the gray zone campaign signal through the global noise requires action through the entirety of the national security community. Adversarial tactics to gradually change the security environment are advantaged by a system that is better suited to clear incursions and violations of boundaries, borders, and laws. Policy, process, and tools must all adapt and evolve to detect, discern, and act upon a new type of signal. The same global technology trends challenging the United States present opportunities to succeed in gray zone competition. Leadership in public- and private-sector research, development, and innovation positions the United States to maintain the persistent technical advantage necessary for gray zone warning.

CASE STUDY: THE U.S. GOVERNMENT IN THE COLD WAR

by Alice Friend and Joseph Kiernan

Context and Background

The Cold War has been called "a 45-yearlong Gray Zone struggle," making an examination of how the U.S. government (USG) organized itself for competition during that era a critical case study.[268] Five of the seven contemporary gray zone activities identified in this study were major action areas during the Cold War: political coercion, economic coercion, information operations, military and paramilitary activities, and proxy support. Congress and the presidency shared responsibility for organizing and reorganizing gray zone-like approaches, although they did so as part of the overall Cold War effort, making gray zone-like activities a kind of campaign-within-a-campaign.

From 1947 to 1989, the United States used four distinct structural approaches to the Cold War, into which gray zone-like missions and organizations were integrated.

1. The *"genesis" phase* (1947–1953) witnessed the post-World War II reorganization of the entire national security enterprise. Driven by the Congress and corresponding to the demands of the emergent "Containment" doctrine, four major legislative events shaped the organizational structure for U.S. gray zone operations during the Cold War: the National Security Act of 1947, the Foreign Assistance Act of 1948, the Smith-Mundt Act of 1948, and the CIA Act of 1949.[269] The major aims of these statutes were "centralized information gathering and analysis, and more unified military decision making."[270] Together they established institutions for U.S. economic influence overseas, information operations and white propaganda, covert action, counterintelligence, and political warfare.
2. In the *"consolidation" phase* (1953–1969) the Eisenhower and Kennedy administrations reorganized national security institutions to execute their competing foreign policy visions of "New Look" and "Flexible Response," respectively.[271] Underneath both approaches, the USG prioritized reforming its covert and clandestine instruments as front-line tools to support anticommunist proxies and conduct paramilitary activities against the Soviet Bloc.[272] Dependence on covert action particularly enhanced the Central Intelligence Agency's (CIA) powers. Overt political and economic coercion were also retooled. Building on the European Recovery Program (ERP), also known as the Marshall Plan, the United States tested lead-agency and collaborative interagency organizational forms to deliver military, economic, and technical assistance to allies, partners, and proxies.[273] These efforts, and the organizational centralization needed to conduct them, peaked during the Vietnam war.
3. The *"constraint" period* (1969–1979) paralleled popular resentment toward the Vietnam War. Congress and the executive restrained gray zone offensive activities, particularly of the covert/clandestine variety, reducing resources and demanding unprecedented transparency. Institutionally, the Nixon administration centralized its foreign policy and national security decisionmaking within the person of the Assistant to the President for National Security Affairs (APNSA), with the consequence that the Department of State's (DoS) policy formulation role was reduced.[274] By the middle of the decade the Congress and President Ford were also cutting resources for the Department of Defense (DoD). Yet the transition away from conventional responses to Soviet aggression did not mean a commensurate augmentation of gray zone activities to compensate.[275] By the late-1970s, it was apparent to non-détente-minded political officials that the gray zone-like USG infrastructure needed revitalizing.[276]
4. The *"resurgence" period* (1979–1989) was an era of redoubling efforts against the Soviet Bloc, driving renewed investment in the full range of conventional and gray zone competitive mechanisms. Not only did DoD budgets grow again, but President Reagan repositioned the secretary of state as his "principal foreign policy advisor" and attempted to reconstruct the National Security Council (NSC) to coordinate whole-of-government strategy.[277] However, navigating the statutory restrictions that had been imposed in the 1970s required greater collaboration with Congress on broader institutional reforms—some of which, like the Goldwater-Nichols Department of Defense Reorganization Act, were resisted by the administration. Especially where gray zone-like activities were concerned, the Reagan White House gravitated toward ad hoc arrange-

ments. What we would today call the gray zone was itself the subject of some controversy during this period, with powerful entities in DoD, DoS, and Congress making strident arguments about the growing importance of so-called low-intensity conflict, while others focused on nuclear arms control and conventional buildup. Such debates were still unresolved when the Soviet Union finally began to collapse in 1989.

Findings: Patterns of Organizational Experimentation

The four phases present a pattern of experimentation in terms of both direct organizational choices and policies with organizational implications. These choices were primarily driven by the range of strategic approaches presidential administrations took over time. Generally, the United States progressed through approaches in the following order:

1. Prioritizing Western political cohesion and military capacity;
2. Supporting broader intervention and counter-intervention in pro-Western and pro-Soviet states, respectively, coupled with economic and military assistance to the former;
3. Pursuing détente and fewer U.S. entanglements in peripheral states;
4. Using comprehensive pressure on Moscow.

Despite this strategic variation, persistent roles in strategy formulation and implementation emerged early in the Cold War and persisted until its conclusion. These included: alliance and proxy relations; assistance; trade and development; intelligence; propaganda and psychological operations; and pro- and counterinsurgent support. Although these roles were surprisingly stable, role assignments migrated across and within agencies, and redundancy was a key feature of USG organization. Just because a gray zone-like role fell under the statutory responsibilities of an agency did not necessarily result in that role staying exclusively in that agency. In fact, in terms of gray zone-like efforts, authorities and resources for covert/clandestine activities grew more flexible over time; this flexibility then made covert and clandestine activities increasingly appealing to presidential administrations. Conversely, the more overt or transparent an effort, the more scrutiny its activities and budgets received. Consequently, oversight tended to be greater for overt lines of effort until the constraint period, when Congress moved to extend more control over covert and clandestine programs.

Coordination and reporting relationships were also highly variable over time. The degree of centralization preferred by the president and the ways the president used the NSC drove the level of interagency cooperation and communication. As more Cold War presidents centralized decisionmaking and policy direction or turned to just a few agencies and advisers, less coordination occurred between agencies and bureaucracies competed harder for influence. This effect was frequently mitigated by the administrative styles of the presidents. This process was just one indicator that leadership, particularly the president's, had an enormous influence over organizations and their uses.[278] Assertive agency leaders, such as the CIA's Director for the Office of Policy Coordination Frank Wisner and the Federal Bureau of Investigation Director J. Edgar Hoover, succeeded in accruing authority for their respective organizations while minimizing oversight.[279] However, as the national security bureaucracies grew in size and complexity, coordination also became more complicated, and presidents were increasingly constrained by institutional interests and resulting inertia.

Lessons Learned and Best Practices

The range of organizational approaches to gray zone-like competition during the Cold War generated a rich array of lessons for modern use. Overall, seven major organizational *lessons* for gray zone competition emerged from the Cold War:

- Cold War gray zone-like government organization was shaped by a mix of statutory and executive action. In the 1940s, Congress created and modified the principal organs of national security policymaking and execution. Thereafter, energy for organization and reorganization was generally driven by the executive branch, with some important but sporadic exceptions as noted above. In the late 1940s, national security institutional designers had creative license. The drastic reductions in national security institutions at the end of World War II were comparatively free of extensive institutional infrastructure and legal impediments much beyond the U.S. Constitution. The conditions were not a completely clean slate—the military departments, State Department, and the precursor to the CIA were all well-established and capable of weighing in on reform debates. But novel organizational design and redesign was possible.

- On the foundations of the National Security Act, Cold War organization for gray zone-like activities was remarkably elastic and responsive to presidential administrative styles. Repeated executive reorganization allowed the USG to adapt to both external threats and internal demands. However, institutional destruction proved much harder than institutional reorganization and creation, making the entire governing apparatus more complex over time.[280]
- Nevertheless, the pre-Cold War foreign policy organizations were forced to adapt or be threatened continually with irrelevance. Although granted direction over aspects of economic, information, and covert operations during the genesis phase, the DoS struggled to execute gray zone-like competition on the scale and with the flexibility expected by most presidents. From "genesis" to "constraint" it shed gray zone-like responsibilities to a litany of novel, specialized organizations such as the U.S. Agency for International Development, the U.S. Information Agency, or the CIA. DoD, meanwhile, was continually subjected to reconfiguration pressures, but their unique military expertise prevented significant "spin-off" effects as occurred with the State Department. The only significant replication of DoD responsibilities was the creation of the CIA's Special Operations Group.[281]
- The Cold War witnessed a pronounced migration of gray zone-like responsibilities toward covert and clandestine activities, with implications for role assignments, centralization, authorities, and budgets. Empowering agencies or divisions of agencies with covert or clandestine missions was appealing for two interdependent reasons: sustainability and insulation from oversight. Keeping institutional activities covert or clandestine reduced internal debate and dissent as well as public scrutiny, making policies less likely to be interrupted by dint of bureaucratic competition or external oversight. Restrictions of access to information associated with covert and clandestine activities could offer presidents a menu of instruments with legal flexibility and were shielded from targeted appropriations cuts thanks to black budgets. These powerful incentives created a feedback loop of growing responsibilities and resources and permitted organizational autonomy unprecedented in the U.S. system. But compartmentalization could also breed a pernicious form of myopia and inertia and increase the difficulties of halting or redirecting such programs. Only serious Congressional and public political mobilization could blunt the aggregation of covert powers. Such restraint was also quickly attenuated by the geostrategic demands of the Cold War, leading to a 45-year-long ebb and flow in the degree to which gray zone competition meant covert action.[282]
- The desire for unity of effort tended to drive presidents toward centralized organization. By positioning the NSC and the White House at the center of national security decisionmaking, especially on sensitive gray zone-like activities, presidents could surmount the impediments of departmental independence and interagency complexity. Centralization also limited debate to expedite decisions and conferred greater responsiveness to presidential direction. In contrast, the desire for informational synthesis and expertise—and sometimes deniability—drove presidents to delegate authority. The more specialized the expertise, the harder it was for the president or any other agency to replicate it. This also helps explain why the State Department suffered from more competitive organizations than the DoD.
- Before the intensification of the Vietnam War, the preponderance of Congressional oversight focused on foreign assistance. In the 1970s, Congress took greater interest in reviewing and restricting the activities, authorities, and budgets of agencies involved in covert and clandestine actions. This marked a level of congressional influence and interference unseen since the genesis period. Congress itself organized committee structures to reflect the major departments and agencies established by statute, an impediment to reorganization in general and to oversight when interagency task forces and other ad-hoc arrangements were the primary mechanisms of policy execution.

From these lessons, we derive four best practices for organizing for gray zone competition:

- *Organizational reforms should remove layers, encourage organizational initiative, and eliminate anachronisms:* A sclerotic decisionmaking and execution system is a major vulnerability in gray zone competitions. The more complex the interagency system becomes, the greater the costs of interagency coordination and the more difficult unity of effort becomes, driving presidents toward centralization and secrecy that only exacerbates other problems, including unhealthy interdepartmental competition and policy inertia. Moreover, institutions can outlive their usefulness, absorbing resources and political energy. Although it takes political capital to close institutions and realign organizations, doing so frees up human and financial resources. Identifying and seizing opportunities to remove unnecessary layers and organizations is crucial to overcoming institutional inertia, fighting excessive restrictions on information and decisionmaking, and speeding response times to gray zone activities.

- *Gray zone competition takes a coalition:* Gray zone competition takes place in multiple domains across the globe and cannot be conducted without allies and partners with influence over those domains. Soviet political and economic containment, military and paramilitary activities, and all-source intelligence gathering were contingent on cooperation between U.S. institutions and their counterparts across the West and beyond.[283] This was true not only between governments but also between government and the private sector, whose collaboration on information operations, for example, was a major element of Western solidarity.
- *Treat oversight like an enabler, not an impediment:* Persistent oversight allows for incremental organizational adjustments and prevents strategic myopia and disruptive episodes of public backlash as occurred in the 1970s regarding covert activities. Rather than impeding executive flexibility, it actually sustains organizational autonomy by insuring the republic against the overreach that can accompany institutional power. Balancing between exigency and values-based legal constraints, particularly in the realm of covert and clandestine operations, is crucial to contemporary gray zone competition. Robust oversight mechanisms operating from both Congress and the executive branch, in mutual communication on both sides of the veil of state secrecy, are imperative to ensuring operational efficacy and constitutional controls.
- *Recognize that threats manifest in very different ways that may require very different organizational approaches:* During the Cold War, the United States restructured its national security state to compete with a single enemy but made myriad institutional adjustments over time as the threat from that adversary evolved. The contemporary United States is competing and countering multiple adversaries, and so must be even more organizationally nimble. The task force model, drawing on the resources of existing institutions but with direct lines of control from senior leaders and with a narrow focus or objective, frequently succeeded during the Cold War. Task forces may evolve into a new institution or may outlive their usefulness after a short period of time, but they are an example of the kind of rebalancing of human capital and lines of authority necessary to conduct a long-term, ever-changing campaign.

CASE STUDY: ISRAEL'S COMPETITION WITH IRAN, 1991–2015

by Michael Matlaga

Context and Background

Iran and Israel, once partners with warm relations diplomatically and militarily, have never engaged in direct military confrontation. In the aftermath of the Iranian revolution in 1979, Iran and Israel severed official diplomatic ties, and relations between the two states quickly deteriorated into a decades-long gray zone competition, one that continues today.[284] This case examines organizational and policy shifts made by Israel between the First Gulf War and the implementation of the 2015 national defense strategy, with particular emphasis on the 2006 Israel-Lebanon War.

The end of the First Gulf War defined what Israeli defense officials saw as a new security environment where state-based conflict was likely to be replaced by short, low-intensity conflict that involved the public on the home front more than ever before. The end of the war thus resulted in a period of organizational and procedural change, notably for the Israeli Defense Forces (IDF) with the creation of a new regional Home Front Command.[285] It also prompted changes for the IDF's intelligence arm, Aman, with the introduction of systemic analysis, which focuses on "systems" with cross-functional and multi-country portfolios rather than teams focused exclusively on specific countries or regions.[286]

The 2015 IDF national defense strategy, prepared by IDF Chief of the General Staff Gadi Eisenkot, was Israel's first public document of its kind and marked a turning point in how Israel views the threat from Iran and views strategy itself.[287] The document reflects three key lessons for Israel from the preceding decades: (1) there is a need for a renewed focus on interagency integration in tackling gray zone competition, occurring during "campaigns between wars;"[288] (2) Iran poses a strategic-level threat to Israel and thus merits a strategic response; (3) Israel's mode of competing with Iran remains at the tactical and operational levels. The contradiction of some of the lessons from the defense strategy suggests that organizational forms can impose constraints on national purpose.[289]

The relevant actors during these shifts have been the Prime Minister's Office (PMO) and the relevant cyber domain oversight authorities, the Ministry of Strategic Affairs and Public Diplomacy (formerly *Hasbara* Ministry and Ministry of Public Diplomacy), the IDF and Aman (military intelligence), and Mossad (foreign intelligence). Of the gray zone activities identified in this study, the most prevalent in this case were Israeli efforts to counter Iranian proxies and state-backed forces, as well as information and cyber operations. The role of the political domain, especially with Israel expanding its diplomatic relationships with Sunni Arab states in the region, was largely muted but played an increasingly important role toward the end of the period.

Findings

The period examined in this case study is perhaps best defined by the culture of decentralized experimentation and widespread aversion to strategy and long-term planning throughout the various agencies within the Israeli defense and foreign policy establishments. Acting autonomously from each other with little central direction, each of Israel's relevant agencies were and continue to be in a constant state of assessment of their performance, analyzing failures and looking for ways to better meet their priorities and compete with other agencies for influence despite clear divisions in areas of responsibility. Most changes occurred by adapting their individual approaches to the shifting security environments but also occasionally by making internal structural changes themselves. These organizational changes mostly involved expanding the number of internal structures or increasing funding for existing, lesser-funded units. A key commonality was a priority on the short term over the long term. While it is never explicitly stated as such by civilian officials or agency heads, this short-term tactical and operational focus is perhaps the driving force behind why, despite frequent self-assessments of agency organizational approaches and plans, meaningful organizational expansion or restructuring was infrequent. The creation of the Ministry of Public Diplomacy is one notable exception to this trend.

The PMO,[290] relying heavily on public opinion to lend it political power over agencies, held more influence over other civilian bodies than the defense and intelligence communities and primarily sought to carve out control over emerging dimensions of gray zone policy, asserting control with reassignment and some active roles in the information space and oversight in the cyber domain.[291] It also pushed for cooperation with traditionally hostile Arab neighbors in an effort to combat Iranian influence in the region.[292]

Organizational changes to the defense and intelligence establishments were rarely prescribed or ordered by the PMO, the Knesset, or other civilian leaders. Rather, the PMO defined the *roles* of each of the agencies broadly (e.g., defense, foreign intelligence, information operations, and oversight) and occasionally articulated the need for new roles—as was necessary with the emergence of modern telecommunications technology and the cyber domain—but otherwise the PMO did not dictate organizational policies or activities.[293] The relative independence of the agencies led to consistency in role assignments between them, as the civilian authorities generally lacked the political influence and, as it relates to the intelligence community, meaningful legal authority to force change or reassignment. The military and military intelligence concerned themselves with the real-time military demands of combatting Iran's proxies—Hezbollah and Hamas—albeit in multiple domains.[294] Mossad was the dominant force in covert action and targeted assassinations and led in intelligence collection and offensive cyber operations against Iran.[295] The PMO and the Ministry of Strategic Affairs and Public Diplomacy—formerly the Hasbara Ministry and Ministry of Public Diplomacy—took control of the information space (information and disinformation).[296] Meanwhile the PMO seized the initiative in the regulation of the cyber domain and cyber defense through its subservient bureaucracies—in this case, offices like the National Cyber Bureau and eventually the National Cyber Security Authority.[297]

This decentralized, delegated form of control led the individual agencies to take responsibility for and to institute their own organizational changes at all levels, as well as to take cues for the need for change from different stimuli. Change in the IDF depended on the public perception, both of the IDF itself and of the competence of civilian leadership.[298] Aman, relatively insulated within the IDF, adapted based on its own perceptions of the changing security environment.[299] Mossad's direction was mostly defined by the agency leadership but was occasionally forced to contend with bad publicity.[300] Yet, the agencies generally decided that long-term strategic plans were not well-suited to the current security environment, choosing instead to focus on the operational and tactical levels. While civilian authorities generally did not force change on the agencies, they were each subject to the public opinion of a well-informed and involved civilian population and sometimes implemented changes when faced with intense scrutiny and failure.

After the 2006 war with Lebanon, the defense establishment contended with intense public scrutiny over its performance—leading to a number of important personnel changes like the IDF chief of staff and the minister of defense.[301] While overall funding continued to decline, damage to the civilian sector spurred a renewed interest in the need for a robust Home Front Command.[302] These constraints and the public failures during the campaign also led the IDF and Aman to shift focus from special operations and airpower to fighting "hybrid" enemies like Hezbollah that, in their assessment, fell between low-intensity and high-intensity conflict.[303] This chiefly involved the re-expansion of IDF ground forces with a renewed focus on maneuverability.[304] The acknowledged strategic threat from Iran served mostly as an overture for the more real-time threats Israel faced through Iran's proxies.

Mossad largely operated with a level of secrecy beyond that of any comparable Western intelligence agency. Behind this veil of secrecy, Mossad enjoyed near limitless autonomy. However, highly public cases like the assassination of Hamas leader Mahmoud al-Mabhouh,[305] the suicide of Mossad agent Ben Zygier,[306] the exposure of Mossad agents using British and New Zealand passports, and a report by the state comptroller exposing abuses did cause promises of internal reorganization, adaptation, and personnel changes to appease calls for greater oversight of the spy agency.[307]

One significant organizational change, however, occurred due to internal pressure on then-Mossad chief Meir Dagan to increase cooperation with foreign intelligence agencies. In response, he transformed and expanded the traditionally decrepit Tevel foreign liaison unit to meet these demands.[308] Oversight by the PMO or any other arm of the government was essentially non-existent, allowing the agency to pursue its goals relatively free of constraints. Mossad consistently recognized Iran as the greatest source of concern for both their counterterrorism and counterproliferation priorities, but its fixation on the operational and tactical levels prioritized weakening Iran's influence over Hezbollah, Hamas, and the proxies themselves.

The decentralized command structure, the diminished importance of civilian leadership over the agencies, and the clear lines between responsibility for the various aspects of modern gray zone competitions not only meant that the agencies were largely responsible for instituting their own changes but also resulted in a general lack of coordination across them and, in fact, competition between them. The IDF, which had its own intelligence service in Aman that aligned with the needs of the military, did not frequently need to enlist the assistance of the PMO or Mossad in executing its mission. In fact, the involvement of the civilian leadership in military decisions fluctuated with public opinion about foreign policy. After the 2006 war, civilians largely blamed the political leadership for its lack of military expertise despite numerous internal reports about IDF failures.[309] Mossad's unparalleled secrecy and independence in choosing its own missions meant that it rarely conducted operations that required cooperation with the military or the PMO.

These characteristics all meant that strategy was not defined in a centralized process by the country's leadership but at best evolved out of an accretion of independent activities directed by autonomous agencies. However, the end results were less than the sum of their parts, not strategies so much as a series of specialized operational plans. Even the 2015 national defense strategy largely focuses on the interim operational national defense concerns.[310] This aversion to long-term planning and focus on the short term produced relatively static organizational structures with highly malleable organizational plans and internal roles.

Lessons Learned

Israel's organizational approaches to gray zone-like competition with Iran between the end of the First Gulf War and the implementation of the first official, public national defense strategy in 2015 provided several lessons that could be useful for application in the United States. Overall, six major lessons emerged:

- *Since organization was decentralized, and strategy not defined, each agency's priorities and adaptations were shaped by factors specific to the nature of the organization rather than the gray zone threat itself.* Agencies prone to secrecy like Mossad react strongly to high-profile failures that bring media attention and threats of additional oversight. IDF and other military decisions, while also often effected by high-profile failures, are chiefly constrained by historically risk- and cost-averse organizational cultures. It also leads organizations to focus on what is in front of them—operations and tactics—like preparing for protracted conflict with Hezbollah or carrying out covert operations against non-strategic enemies. This reactive approach successfully mitigates known threats but is vulnerable to adversary adaptation at the strategic level.
- *Nevertheless, organizational autonomy leads to extremely effective tactical and operational responses to gray zone threats. Weak interagency coordination still held the line against adversary (Iranian) activities without strategically reducing them.* With the agencies sticking to their specialized expertise and lines of effort, specific tasks can be closely monitored and feedback loops tight. Even without highly coordinated interagency efforts, the IDF can conduct responsive operations, the PMO can generate relatively positive messaging about Israeli foreign policy aims and goals in the region, and Mossad can chip away at Hezbollah, Hamas, and Iranian command structures through covert operations. This will produce effective results in the short term but likely will not shift the overall advantage to Israel or allow it to compel a change in Iranian behavior. The United States might be able to learn from the tactical and operational successes of Israeli agencies while applying its own principles about the interagency process in an attempt to produce results at the strategic level.
- *Limited institutional constraints encouraged experimentation, self-regulation, and cultural consistency but also resulted in a lack of coordination and strategic direction.* Without meaningful civilian oversight, primarily from the PMO, the agencies were generally left to pursue their engrained mission sets under their own direction and implement changes largely as they saw fit, undergoing internal cultural change only when driven by internal factors. This led to strong internal organizational cultures and a willingness to make changes on their own, something that is not necessarily characteristic of U.S. bureaucracies. However, without overarching direction from civilian leadership, these agencies often worked in silos and pursued their lines of effort without meaningful cooperation across agencies. Without institutionalized interagency cooperation or mission reassignment from civilian leadership, agencies had very little incentive to work across offices beyond an ad hoc basis.
- *Excessive agency autonomy increased the power of outside pressure.* Even with decentralized control, other factors can constrain organizational decisions, reducing government control over agencies further. Despite the PMO's lack of meaningful influence

over the organizational decisions of gray zone-related agencies, the IDF, Mossad, and others were not completely immune to outside pressures. For the IDF, public opinion determined the degree of autonomy they had for decisionmaking as well as the degree of blame they received for blunders. This was particularly evident after the 2006 war, when public opinion surrounding the relatively unsuccessful operations called for military adaptation but laid blame on the civilian leadership for its lack of expertise and encouraged the military to be largely responsible for its own adjustments. Mossad has enjoyed unparalleled secrecy within the government and in the public eye, but high-profile failures or abuses—like the death of Ben Zygier, the highly publicized Dubai operation to assassinate Hamas leader Mahmoud al-Mabhouh, which was caught on video, or the abuses exposed by the comptroller's office—force the organization to react in ways that the public or other parts of the government would otherwise not be able to force.

- *Even with strong institutional reforms and structures, individuals and their backgrounds dictated organizational direction, public discourse, and the viability of oversight.* Oversight by civilian authorities of foreign policy and national security agencies—which in the case of Israel was mostly political and not institutional in nature—can be weakened by a perceived lack of expertise of the civilian leadership. This can also be further derailed by the political behavior of agency officials, both current and former, whose expertise often carries more weight in public discourse. The 2015 defense strategy, in addition to its productive calls for better interagency cooperation and recognition of gray zone challenges, also seemed to serve a political role of shifting potential future responsibility and blame to civilian leadership, a common theme after the 2006 war and the wars with Gaza that followed. These dynamics can be further amplified by the presence of officials with such expertise in politics, as is overwhelmingly the case in Israel. Party leaders, Knesset members, and ministers with career agency and military experience can bring their institutional biases to civilian positions and complicate political discourse and oversight.
- *Unique expertise protected organizational autonomy.* One of the primary factors that undermined civilian control over the national security departments and agencies responsible for conducting and defending against gray zone activities was public perceptions about expertise. That is, the public generally perceived civilian leadership as lacking sufficient expertise to exercise oversight or drive change within the agencies, and even often placed blame on civilian leadership for agency failures. The general population and each of the agencies largely considered the expertise of Mossad and the IDF/Aman to be specific to the organization and unique to those who serve over the long term. This resulted in broad organizational autonomy across several lines of effort, including proxy conflict and relations, offensive information operations, covert operations, and countering some types of disinformation. The most notable gray zone tool that could be replicated or distributed throughout the different agencies and sectors, cyber security, was *not* claimed by or isolated to a single agency. Additionally, the expertise of the Ministry of Foreign Affairs in *hasbara* and public diplomacy was not considered unique, and the PMO was able to stand up a new agency dedicated to the information domain. This has drastically weakened the role of the MFA overall.

Best Practices

- *Strategic gray zone competition takes a coalition:* As illustrated in the Cold War case study in this report, gray zone competition cannot be conducted without allies and partners with influence over the variety of domains and locations where such competition takes place. This case study further builds out this point from difficult lessons that Israel learned not only about working with international partners, particularly international intelligence partners, but also across government agencies. Without a coherent, widely accepted strategy, Israeli agencies pursued tactical-level objectives with the utility of success not extending beyond the tactical or operational level. Israel was moderately successful at beating back Iranian gray zone activity at the tactical level—fighting Iranian proxies, justifying Israeli foreign policy positions with information campaigns, and countering disinformation from Iranian proxies. It was not, however, able to roll back Iranian influence or broader foreign policy goals that it sought to achieve through the gray zone in ways that serve larger Israeli security interests in the region. While Israel has not suffered any meaningful military losses to Iran in Gaza or Lebanon, local populations in the Palestinian territories and Lebanon deeply distrust Israeli intentions following these interventions. In combination with local governance failures and other factors, this creates favorable conditions for Iranian-backed proxies, investments, and influence to persist. In fact, Iran's broader regional footprint has only grown.[311] So just as gray zone competition takes a coalition of allies and partners, strategic-level success in the gray zone also takes a well-integrated interagency effort.

- *Build in flexibility for initiative without losing organizational and strategic principles:* Israel's organizational approach and the autonomy of the agencies encouraged internal-, operational-, and tactical-level experimentation. This type of initiative would likely be more difficult in a more cumbersome, bureaucratic entity like the USG, but there are ways the USG could look to replicate some of the flexibility afforded to agencies in Israel without changing the organizational and strategic principles of U.S. foreign and defense policy. Chiefly, civilian and political oversight of the national security apparatus is not mutually exclusive with looking for ways for agencies to experiment at the tactical and operational levels. This could encourage the type of experimentation that, in Israel, led to the establishment of a new regional command, the decisions within Mossad to work more closely with international intelligence partners, and the IDF ultimately adjusting its forces to deal with more hybrid enemies like Hezbollah. In the U.S. system, this type of freedom would still see civilian political leadership exercising control and setting the strategic direction of U.S. gray zone activities while allowing for agencies with unique expertise to adjust operational and tactical approaches that might allow the United States to more effectively pursue its desired outcomes in the gray zone.

CASE STUDY: FIRST SOLAR, 2006–2012

by Joseph Federici and Joseph Kiernan

Context and Background

In 2007, the U.S. solar power industry seemed poised for strong and sustainable growth.[312] However, in only four short years, a number of challenges emerged that threatened the continued viability of many U.S. solar power companies. One of those companies was First Solar, Inc. This case study examines the organizational and structural decisions made by First Solar between 2006–2012 and explains why First Solar continued to be viable in a volatile market.

In the early 2000s, new policies, primarily in Europe, made solar energy more commercially competitive with traditional fossil fuels. These came largely in the form of subsidy programs that encouraged the large-scale purchasing of solar panels by guaranteeing owners an above-market price for the energy they produced. U.S. firms took advantage of this state-supported demand and profited through sales to Europe.[313]

First Solar forged its place in the industry as the largest U.S. manufacturer of photovoltaic (PV) solar panels, or modules. Its proprietary cadmium telluride thin-film technology "made it the largest and lowest-cost producer for nearly a decade."[314] In fact, it became the first solar company in the world to manufacture solar panels that could generate power at less than $1.00 per watt.[315] In 2007, backed by high profits and strong growth that stemmed almost exclusively from European markets, First Solar expanded production internationally to keep up with global demand by building a manufacturing facility in Germany to complement its research/development/manufacturing plant in Ohio. Between 2007 and 2011, First Solar announced plans to expand its capabilities by opening new manufacturing centers in both Malaysia and Vietnam.[316] To support this expansion, the company's workforce grew more than fourfold, from almost 1,500 employees in 2007 to 7,000 by the end of 2011.[317]

Additionally, in 2007, First Solar purchased Turner Renewable Energy, a system integrator company. This acquisition allowed First Solar to "vertically integrate" its operations, meaning that First Solar now controlled the "engineering, procurement, construction, operations, maintenance, and development of solar power plants."[318] Rather than only designing and producing solar panels, vertical integration allowed First Solar to begin operating a "systems business" segment of the company that focused on the construction of large, utility-scale projects. [319]

Vertical integration aside, focusing on utilities made sense for First Solar, and in 2011 the company announced a transition away from rooftop solar installations, which had previously been a significant portion of its sales portfolio.[320] While the company's proprietary thin-film technology was cost competitive—able to produce more energy for less money—it was less geometrically efficient than its competitors. Therefore, its solar panels were best suited to compete in large-scale utility projects where space constraints were not a prominent factor.[321] Increasing the scale of its sales allowed the company to optimize its competitive advantage in the market.

By 2011, however, two major challenges emerged that threatened the continued viability of the U.S. solar industry in general and First Solar in particular. First, in the wake of the Great Recession and the subsequent wave of austerity policies, European governments began scaling back the subsidy programs which had sustained the demand for renewable energy on the continent.[322] Second, this shrinking demand was met with a global oversupply of solar panels, manufactured in large part by Chinese firms able to sell at or below cost due to financial support from Beijing.[323] Due to this decrease in demand and increase in supply, by the end of 2011, a series of high-profile U.S. companies comprising one-fifth of the U.S. solar industry had closed operations or declared bankruptcy.[324]

Between FY2007 and FY2010, First Solar had seen its operating income expand more than fivefold, from $137 million to almost $750 million. Facing these new market challenges, however, First Solar experienced its first net operating loss in seven years, losing $68 million in FY2011.[325] Nevertheless, the company was able to avoid the fate of much of its competition across the U.S. solar industry, avoiding bankruptcy and rebounding to compete more robustly in the years ahead. Within two years, both its sales and revenue were growing firmly, and by FY2015 the company had a positive operating income of over $500 million, with sales revenue surpassing those in FY2010 by over $1 billion.

Findings

First Solar seems to have managed multiple challenges and remained a viable company for two reasons. First, the company responded quickly to global market changes and recognized the need to reverse its previous course of expansion, instead scaling back production to align its supply with shrinking global demand. Second, it was able to stay afloat by relying on pre-existing contracts for its utility systems project, which offered a degree of continuing demand and acted as a buffer against global market fluctuations.[326]

While these two factors helped First Solar to survive in the short term, the company began to orchestrate a longer-term strategic plan that would allow it to succeed amid evolving market realities. It seems to have understood that its previous dependence on heavily subsidized European markets was unsustainable, so it began seeking new markets where demand for solar energy would be more sustainable and less dependent on policy fluctuations. Largescale utility projects in emerging markets across Asia, the Middle East, and North Africa would take up an increasing share of First Solar's sales going forward.[327]

The organizational elements of this successful strategy are straightforward. First Solar appears to operate as a private-sector company with a traditional centralized hierarchical structure in which major company decisions are made at the executive level and passed downwards. While individual divisions of the firm may have some leeway to manage themselves for localized efficiency, they are nonetheless executing directives from above. There is no obvious lateral engagement between divisions. The incentive structure for the company, both the whole and its parts, is presumably one of seeking to maximize profits. Accountability to this end is centered around the board of directors, which selects the CEO and is designed to effectively represent the interests of the company's shareholders.[328]

In the short term, this case demonstrates how an organization was able to remain viable amid a rapidly changing strategic environment by reallocating resources away from suboptimal pursuits and by leveraging competitive advantages that it had previously cultivated.

Even though First Solar's strategy shifted, the roles within the different segments of First Solar seem to have remained static. As per the 2009 Annual Report, First Solar began formally operating its business in two segments. The first is the component's segment, which involved research, development, engineering, manufacturing, and sales. The second, the systems segment, included project development, engineering, procurement, construction, operations and management, and project finance.[329] These roles were seemingly unaffected by changes in strategy.

The role assignments, however, did seem to shift as the strategy changed. It appears that this was less a function of assignments shifting within a segment or between segments and more about assignments being scaled down and up. This was most pronounced in the component segment in manufacturing. By 2011, the company had recognized a "structural imbalance between supply and demand," in which production significantly exceeded global demand.[330] With fewer panels being sold, the company's existing manufacturing facilities were only producing 1.7 gigawatts worth of modules, 68 percent of its manufacturing capacity of 2.5 gigawatts.[331] In response, the company began to scale back its operations in late 2011, cancelling plans for a new plant in Vietnam, idling four existing production lines in Malaysia, and fully shuttering manufacturing operations in Germany.[332] This strategic restructuring seems to have led to a more efficient allocation of resources and left the firm producing an appropriate quantity of solar panels to match global demand.

Between 2009 and 2013, the company was led by three different CEOs: Robert Gillette (2009–2011), Michael Ahearn (Interim CEO, 2011–2012), and James Hughes (2012–2016).[333] Based on publicly available documents, it is difficult to ascertain the extent to which the personalities of these leaders affected the company's success. However, one can see that: the end of Gillette's tenure coincided with the marked downturn of First Solar's operations; Ahearn oversaw the introduction of the company's tactical and strategic responses to those challenges; and Hughes led the company through the stabilization of its market performance.

Lessons Learned

First Solar's organizational and structural decisions between 2006–2012 provided the study team with several lessons that could be useful for application to the United States government. Those lessons include:

- *An organization should identify risks and invest in opportunities to hedge against those risks.* Beginning as early as 2006, First Solar seemed to understand that its focus on producing modules in a highly subsidized European market was subject to, "changes in general economic and political conditions in the countries in which [it] operated."[334] Rather than hoping that the economic realities in Europe would remain static, the purchase of Turner Renewable Energy in 2007 allowed First Solar to vertically integrate and invest in a pipeline for the construction of large, utility-scale projects. According to First Solar, the contracted North American pipeline was to act as "a buffer against demand uncertainties."[335] Indeed, when European demand fell in 2011, the pipeline seemed to help shield the firm from the worst consequences of Europe's market volatility.

- *Responsiveness to the evolving strategic environment is determined by incentives as well as organization and culture.* First Solar's strategic plan prior to the Great Recession sought to optimize its performance given certain market realities that ceased to be true once European governments began scaling back their subsidy programs and global demand shrank. Rather than continuing to pursue the same plan under new conditions, the company seemed to recognize the need to reallocate its resources and realign its priorities to the evolving needs of the market. In an ostensibly diametric shift from its previous plans to expand manufacturing capacity, First Solar wisely scaled back production to align itself with the newly emerging market imbalance, all while beginning to seek more sustainable emerging markets. Accordingly, the company reduced its workforce by 30 percent, going from 7,000 employees in 2011 to only 4,850 by the end of 2013.[336] This reduction seemingly helped limit duplication and allowed for an optimized allocation of resources.
- *An organization that recognizes and exploits those areas where it has a competitive advantage can build resiliency to multi-vector challenges.* First Solar understood that its strategic edge in the global market came from its proprietary thin-film technology. It seems as though it's best chance to establish and preserve its place in the industry was to reorient towards segments of the market that were best suited for its particular panels, relative to the competition. Early on, a significant portion of First Solar's sales portfolio included rooftop installations, where its modules' cost efficiency was somewhat counteracted by its relative geometric inefficiency.[337] With the company's evident transition into a more exclusive focus on the utility segment of the solar market, where large-scale projects were not confined by the same size restrictions, First Solar was able to optimize its product's unique advantage.[338]
- *An organization that continuously refines and resources its competitive advantages will increase its chances of survival.* While First Solar seemingly recognized how to best take advantage of its technological edge, it also understood that it could not take that advantage for granted. In a dynamic market, competitors vying for First Solar's market share were developing solar technology that could potentially reach or surpass the cost efficiency of its CdTe thin-film modules.[339] To maintain its position, the company put additional and more focused resources into the development of its technology, and as a result, the quality and efficiency of the product continued to grow and stay well above the competition.[340]
- *A centralized organization can implement decisions quickly.* Once it became clear to First Solar that demand in Europe had dropped and that Chinese companies were oversupplying the market, First Solar needed to move quickly to stay afloat. In the course of essentially one year, First Solar rapidly adjusted its entire business model. In this traditional top-down hierarchical structure, as opposed to a more bureaucratized model, it appears that decisions were implemented quickly, and First Solar was able to effectively respond to changes in the market.
- *A division-of-labor structure, as opposed to role redundancy, can perform efficiently.* The operations of the two main business segments of First Solar, components and systems, are distinct from one another with seemingly minimal direct interaction. However, they are both inextricably connected with one another in their common pursuit of maximizing the company's profits and market share. The development and success of one seemingly complements the other's ability to succeed. For instance, the manufacturing and technological improvement of solar modules takes place under the auspices of the components segment, but the viability of full-scale systems projects relies on the quality and efficiency of those very modules.
- *An organization should be proactive in developing a long-term strategic plan.* First Solar announced its long-term strategic plan in December 2011, when its financial losses made clear that the company

needed to radically reorient its strategy. However, financial reports acknowledged as early as 2006 the risks associated with the company's dependence on a few European customers whose demand was contingent on government subsidies.[341] While the investment in its North American utility pipeline project was structured in part to act as a buffer against market volatility, First Solar nonetheless waited until its sales began to fall in Europe before it unveiled its transition towards new developing markets. While an outside observer cannot know the internal strategic calculus within First Solar's leadership, the company may have been better equipped to mitigate the impact of and respond to the loss of European demand had it been more proactive in changing course *before* the Great Recession.

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 at 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.

Melissa Dalton is a senior fellow and deputy director of the CSIS International Security Program (ISP) and director of the Cooperative Defense Project (CDP). Her CDP research focuses on reinforcing the principled foundations of U.S. defense policy and military operations. She also frequently conducts research and writes on security cooperation with allies and partners and U.S. defense policy in the Middle East. As deputy director, she advises the ISP director on a broad range of strategic and management issues. She manages the daily operations of ISP, including a team of 50 resident staff and an extensive network of nonresident affiliates. Prior to joining CSIS in 2014, Ms. Dalton served in a number of positions at the U.S. Department of Defense (DoD) in the Office of the Under Secretary of Defense for Policy from 2007 to 2014. She most recently was a senior adviser for force planning, where she contributed to the 2014 Quadrennial Defense Review and DoD's planning guidance. Previously, she served as special assistant to the under secretary of defense for policy, as policy adviser to the commander of the International Security Assistance Force in Kabul, Afghanistan and as country director for Lebanon and Syria. In 2012, she was a visiting fellow at the Center for a New American Security. Prior to her DoD service, she taught English to middle and high school students in Damascus, Syria in 2006. From 2003 to 2005, she served as an intelligence analyst at the Defense Intelligence Agency. Ms. Dalton holds a BA in foreign affairs from the University of Virginia and an MA in international relations from the Johns Hopkins University School of Advanced International Studies. She is a member of the Council on Foreign Relations and was an international affairs fellow at the Council on Foreign Relations.

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 & Russia, both from Stanford University.

Alice Hunt Friend is a senior fellow in the International Security Program at 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 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.

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.

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.

Joseph Federici is a research associate and program manager with the International Security Program at CSIS, where he works on a variety of projects 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.

Matthew Conklin was a research intern with the International Security Program at CSIS, where he provided 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 returned to the University of Chicago to pursue a PhD in political science with a concentration in international relations.

Joseph Kiernan was a research intern with the International Security Program at CSIS. He currently serves as research assistant to Dr. Henry A. Kissinger in New York. He received his MPhil in international relations and politics from the University of Cambridge where he was a Thouron Scholar and his BA in diplomatic history and political science from the University of Pennsylvania.

Endnotes

[1] White House, *National Security Strategy of the United States* (Washington, DC: December 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; Department of Defense, *National Defense Strategy of the United States of America* (Washington, DC: 2018), 2, https://DoD.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[2] Also referred to as hybrid threat, political warfare, malign influence, sharp power, and competition, the phenomenon of the gray zone is well-researched and analyzed by scholars. For further discussion of definitional issues, see *By Other Means Part I*.

[3] Catherine Porter, "Chinese Dissidents Feel Heat of Beijing's Wrath. Even in Canada." *New York Times*, April 1, 2019, https://www.nytimes.com/2019/04/01/world/canada/china-dissident-harassment-sheng-xue.html.

[4] Michael Eisenstadt, "Information Warfare: Centerpiece of Iran's Way of War," in Katherine Hicks et al., *Deterring Iran After the Nuclear Deal* (Washington, DC: CSIS, March 2017), https://www.csis.org/analysis/deterring-iran-after-nuclear-deal.

[5] "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," U.S. Department of Justice – Office of Public Affairs, February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[6] Jonathan Landay and Mark Hosenball, "Russia, China, Iran Sought to Influence U.S. 2018 Elections: U.S. Spy Chief," Reuters, December 21, 2018, https://www.reuters.com/article/us-usa-election-interference/russia-china-iran-sought-to-influence-u-s-2018-elections-u-s-spy-chief-idUSKCN1OK2FS.

[7] DHS and its partners have leveraged relationships with social media companies to find private-sector-led solutions, like taking down misinformation about election processes in time for the 2018 U.S. midterm elections.

[8] Department of Defense, "Department of Defense Directive: Irregular Warfare (IW), 3000.07," May 12, 2017, 3, https://fas.org/irp/DoDdir/DoD/d3000_07.pdf.

[9] Ibid.

[10] Office of the Under Secretary of Defense (Comptroller), *European Deterrence Initiative – U.S. Department of Defense Budget Fiscal Year (FY) 2019* (Washington, DC: February 2018), https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/fy2019_EDI_JBook.pdf.

[11] Marc Santora and Julian E. Barnes, "In the Balkans, Russia and the West Fight a Disinformation-Age Battle," *New York Times*, September 16, 2018, https://www.nytimes.com/2018/09/16/world/europe/macedonia-referendum-russia-nato.html.

[12] Sebastian Bay et al., *The Current Digital Arena and Its Risks to Serving Military Personnel* (Riga, Latvia: NATO Strategic Communications Center of Excellence, January 2019), https://www.stratcomcoe.org/current-digital-arena-and-its-risks-serving-military-personnel.

[13] Natalia Drozdiak and Ott Ummelas, "NATO Readies for Cyber Threats on Russian Doorstep," Bloomberg, November 29, 2018, https://www.bloomberg.com/news/articles/2018-11-29/nato-readies-for-cyber-threats-with-wargames-on-russian-doorstep.

[14] "The National Security Agency: Missions, Authorities, Oversight and Partnerships," National Security Agency, August 9, 2013, https://fas.org/irp/nsa/nsa-story.pdf.

[15] Katie Lange, "Cybercom: How DOD's Newest Unified 'Cocom' Works," U.S. Department of Defense, October 12, 2018, https://www.defense.gov/explore/story/Article/1660928/cybercom-how-dods-newest-unified-cocom-works/.

[16] Julian E. Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *New York Times*, October 23, 2018, https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html.

[17] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 26, 2018, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.1fcc76530cc2.

[18] Ellen Nakashima, "U.S. Cyber Force Credited with Helping Stop Russia from Undermining Midterms," *Washington Post*, February 14, 2019, 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=.b572ea329ada.

[19] White House, *National Security Strategy*.

[20] "Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections," Director of National Intelligence, October 19, 2018, https://www.dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections.

[21] White House, *National Security Strategy*, 35.

[22] Of note, the Department of Justice charged 13 Russian individuals and 3 Russian businesses for deploying information warfare against U.S. electoral systems during the 2016 U.S. presidential election. It also indicted Russian intelligence officers for deploying disinformation campaigns against anti-doping organizations.

[23] White House, *National Security Strategy*.

[24] Julian Borger, "U.S. Cuts Funds for Anti-Propaganda Group that Trolled Activists," *Guardian*, May 31, 2019, https://www.theguardian.com/us-news/2019/may/31/us-cuts-funds-for-anti-propaganda-group-that-trolled-activists.

[25] Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms."

[26] Ibid.; Sheera Frenkel, Kate Conger, and Kevin Roose, "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.

[27] Ryan Henry, Stacie L. Pettyjohn, and Erin York, *Portfolio Assessment of the Department of State Internet Freedom Program* (Santa Monica: Rand Corporation, 2014), 59, https://www.rand.org/pubs/research_reports/RR794.html.

[28] "U.S. Department of State Announced Competition to Promote Internet Freedom in Ukraine," UNIAN, March 9, 2019, https://www.unian.info/economics/10473681-u-s-department-of-state-announces-competition-to-promote-internet-freedom-in-ukraine.html.

[29] Heather Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: CSIS, October 2016), xi, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf; Heather Conley et al., *The Kremlin Playbook 2: The Enablers* (Washington, DC: CSIS, March 2019), 12, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190326_KPII_WEB%20FINAL.pdf.

[30] Heather Conley, "Putin's Playbook: The Kremlin's Use of Oligarchs, Money and Intelligence in 2016 and Beyond," written statement before the House Permanent Select Committee on Intelligence, March 28, 2019, 5.

[31] 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.

[32] 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.

[33] 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.

[34] "Key Takeaways – Worldwide Telecom Equipment Market 2018," Dell'Oro Group, http://www.delloro.com/delloro-group/telecom-equipment-market-2018.

[35] James Andrew Lewis, "5G: To Ban or Not to Ban? It's Not Black or White," CSIS, *Commentary*, April 24, 2019, https://www.csis.org/analysis/5g-ban-or-not-ban-its-not-black-or-white.

[36] Matthew P. Goodman, "Predatory Economics and the China Challenge," CSIS, *Global Economics Monthly* 6, no. 11 (November 2017), https://www.csis.org/analysis/predatory-economics-and-china-challenge; Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, *China's Use of Coercive Economic Measures* (Washington, DC: Center for New American Security, June 2018), https://www.cnas.org/publications/reports/chinas-use-of-coercive-economic-measures.

[37] Edward Wong and Ben Hubbard, "Pompeo's Anti-Iran Tour Faces Obstacles of a Fractious Middle East" *New York Times*, January 14, 2019, https://www.nytimes.com/2019/01/14/world/middleeast/pompeo-iran-middle-east-coalition.html.

[38] RFE/RL Balkan Service, "Montenegrin Court Convicts All 14 Defendants of Plotting Pro-Russia Coup," May 9, 2019, https://www.rferl.org/a/montenegro-court-convicts-14-on-terrorism-charges-/29930212.html.

[39] Programs include free and fair elections support, youth empowerment, and general democratic governance.

40 “U.S. at U.N. Takes Aim at China’s Belt and Road Initiative,” *Straits Times*, March 16, 2019, https://www.straitstimes.com/asia/east-asia/us-at-un-takes-aim-at-chinas-belt-and-road-initiative.

41 “OPIC to Begin to Transition to the U.S. International Development Finance Corporation,” OPIC, https://www.opic.gov/build-act/overview.

42 “Mission Statement,” U.S. Department of Commerce – Bureau of Industry and Security, https://www.bis.doc.gov/index.php/about-bis/mission-statement.

43 Ian F. Fergusson and Paul K. Kerr, *The U.S. Export Control System and the Export Control Reform Initiative* (Washington, DC: U.S. Congressional Research Service, April 2019), https://fas.org/sgp/crs/natsec/R41916.pdf.

44 Ibid., 2.

45 Ibid.

46 “Export Administration Regulations (EAR),” U.S. Department of Commerce – Bureau of Industry and Security, https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

47 “Two Indictments Unsealed Charging Iranian Citizen with Violating U.S. Export Laws and Sanctions Against Iran,” U.S. Department of Justice, press release, June 4, 2019, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2404-two-indictments-unsealed-charging-iranian-citizen-with-violating-u-s-export-laws-and-sanctions-against-iran/file.

48 “BIS 2019 Annual Conference on Export Controls,” U.S. Department of Commerce – Bureau of Industry and Security, 2019, https://www.bis.doc.gov/index.php/compliance-a-training/export-administration-regulations-training/annual-conference-2019.

49 Fergusson and Kerr, “The U.S. Export Control System and the Export Control Reform Initiative.”

50 James K. Jackson and Cathleen D. Cimino-Isaacs, “CFIUS Reform: Foreign Investment National Security Review,” Congressional Research Service, August 22, 2018, https://fas.org/sgp/crs/natsec/IF10952.pdf.

51 Ana Swanson and Keith Bradsher, “Trade Disputes Between U.S. and China Deepens as Beijing Retaliates,” *New York Times*, May 13, 2019, https://www.nytimes.com/2019/05/13/us/politics/us-china-trade-tariffs.html.

52 “China, Mongolia & Taiwan,” United States Trade Representative, https://ustr.gov/countries-regions/china-mongolia-taiwan.

53 United States Trade Representative, *2017 Report to Congress on China’s WTO Compliance* (Washington, DC: January 2018), https://ustr.gov/sites/default/files/files/Press/Reports/China%202017%20WTO%20Report.pdf.

54 “Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies,” U.S. Department of Justice – Office of Public Affairs, October 10, 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

55 “Chinese National Charged with Committing Theft of Trade Secrets,” U.S. Department of Justice – Office of Public Affairs, December 21, 2018, https://www.justice.gov/opa/pr/chinese-national-charged-committing-theft-trade-secrets.

56 Daniel R. Coats et al., “Open Hearing on Worldwide Threats,” U.S. Senate Select Committee on Intelligence, February 13, 2018, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0.

57 “Collateral Damage? Research Collaboration in an Age of U.S.-China Competition,” CSIS – Simon Chair in Political Economy, Washington, DC, June 4, 2019, https://www.csis.org/events/collateral-damage-research-collaboration-age-us-china-competition.

58 Alexandra Yoon-Hendricks, “Visa Restrictions for Chinese Students Alarm Academia,” *New York Times*, July 2018, https://www.nytimes.com/2018/07/25/us/politics/visa-restrictions-chinese-students.html.

59 Helene Cooper and Eric Schmitt, “U.S. Spy craft 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.

60 “About the FTC,” U.S. Federal Trade Commission, https://www.ftc.gov/about-ftc/what-we-do.

61 Ibid.

62 “Cmr. Phillips participates in G7 panel on Digital Innovation and Competition in Paris,” U.S. Federal Trade Commission, June 3, 2019, https://www.ftc.gov/news-events/events-calendar/cmr-phillips-participates-g7-panel-digital-innovation-competition-paris; “Cmr. Phillips gives opening keynote at Global Antitrust Economics

Conference," U.S. Federal Trade Commission, May 31, 2019, https://www.ftc.gov/news-events/events-calendar/cmr-phillips-gives-opening-keynote-global-antitrust-economics-conference.

63 "What We Do," U.S. Securities and Exchange Commission, https://www.sec.gov/Article/whatwedo.html.

64 "Enforcement." U.S. Securities and Exchange Commission. 27 Dec 2016. https://www.sec.gov/litigation.shtml

65 U.S. Congress, Senate, *Asia Reassurance Initiative Act of 2018*, S. 2736, 115th Cong., 2nd sess., became Public Law December 31, 2018, https://www.congress.gov/bill/115th-congress/senate-bill/2736/text#toc-H6013C5BE3DA34822B-CCA1E905EE1BDCC.

66 U.S. Congress, House, *Ukraine Freedom Support Act of 2014* H.R.5859, 113th Cong., 2nd sess., December 18, 2014, https://www.congress.gov/bill/113th-congress/senate-bill/2828/.

67 "Bureau of Energy Resources," U.S. State Department, 2019, https://www.state.gov/bureaus-offices/under-secretary-for-economic-growth-energy-and-the-environment/bureau-of-energy-resources/.

68 U.S. Congress, *Ukraine Freedom Support Act of 2014*.

69 "U.S. – Ukraine Energy Cooperation," U.S. Department of Energy, Office of International Affairs, https://www.energy.gov/ia/international-affairs-initiatives/us-ukraine-energy-cooperation.

70 "Supporting Development of Natural Gas Markets and LNG Options," U.S. Department of Energy, Office of International Affairs, https://www.energy.gov/ia/downloads/supporting-development-natural-gas-markets-and-lng-options.

71 U.S. Congress, *Asia Reassurance Initiative Act of 2018*.

72 Matthew P. Goodman et al., *The Higher Road: Forging a U.S. Strategy for the Global Infrastructure Challenge* (Washington, DC: CSIS, April 2019), 2, https://www.csis.org/higherroad.

73 Ibid., 23.

74 Todd Moss and Erin Collinson, "USDFC Monitor: Why Is the White House Scuttling its Biggest Development Win? Four Hidden Daggers Pointed at the Heart of the New USDFC," Center for Global Development, April 2, 2019, https://www.cgdev.org/blog/why-white-house-scuttling-its-biggest-development-win-four-hidden-daggers-pointed-heart-new.

75 Ibid.

76 U.S. Congress, *Asia Reassurance Initiative Act of 2018*.

77 Peter, Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, *China's Use of Coercive Economic Measures*, (Washington, DC: Center for New American Security, June 2018), https://www.cnas.org/publications/reports/chinas-use-of-coercive-economic-measures.

78 "EU Adopts Investment Screening Regulation," Lexology, March 6, 2019, https://www.lexology.com/library/detail.aspx?g=e781e37f-1c60-4384-9f21-c93edba2f114.

79 Scott Harold, 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; Ibid.; 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; "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," U.S. Department of Justice – Office of Public Affairs, March 23, 2018, https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary.

80 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; 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.

81 Ibid.

82 Joseph Berger, "A Dam, Small and Unsung, is Caught Up in an Iranian Hacking Case," *New York Times*, March 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html; Nicole

Perlroth and David E. Sanger, “Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says,” New York Times, March 15, 2018, https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html.

83 Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2019* (Washington, DC: CSIS, April 2019), 7, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf.

84 For a more detailed summary of the attributes of counterspace weapons, see ibid., 6-7.

85 Ibid., 23-24.

86 “About CISA,” U.S. Department of Homeland Security, https://www.dhs.gov/cisa/about-cisa. Other DHS initiatives of note are the Science and Technology Directorate (S&T), the Cyber Risk Economics Program (CYRIE), and the Cyber Crimes Center (C3).

87 “About CISA,” U.S. Department of Homeland Security.

88 “About Us – National Cybersecurity and Communications Integration Center,” U.S. Department of Homeland Security – Cyber Emergency Response Team, https://www.us-cert.gov/about-us.

89 “Cyber Crimes Cases – How NPPD Protects the U.S. from Cyber Attacks,” U.S. Department of Homeland Security, https://www.dhs.gov/cyber-crime-cases.

90 “Statement from CISA Director Krebs on Election Security,” U.S. Department of Homeland Security – CISA, February 14, 2019, https://www.dhs.gov/cisa/news/2019/02/14/statement-cisa-director-krebs-election-security.

91 “NATO’s Role in Cyberspace,” *NATO Review Magazin*e, February 12, 2019, https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm.

92 Wassenmaar Arrangement Secretariat, *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (Vienna: December 2018), https://www.wassenaar.org/app/uploads/2018/12/WA-DOC-18-PUB-001-Public-Docs-Vol-II-2018-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-18.pdf; “Budapest Convention and Related Standards,” Council of Europe, 2018, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

93 David E. Sanger, Eileen Sullivan, and David D. Kirkpatrick, “Russia Targeted Investigators Trying to Expose Its Misdeeds, Western Allies Say,” *New York Times*, October 4, 2018, https://www.nytimes.com/2018/10/04/us/politics/russia-hacks-doping-poisoning.html.

94 “Department of Energy Statement on Chinese Hacking of Global Managed Service Providers,” U.S. Department of Energy, December 20, 2018, https://www.energy.gov/articles/department-energy-statement-chinese-hacking-global-managed-service-providers.

95 “DOE Announces $40 Million for Grid Modernization Initiative,” U.S. Department of Energy, January 24, 2019, https://www.energy.gov/articles/doe-announces-40-million-grid-modernization-initiative.

96 DoE contributes to the IC through its Offices of Cybersecurity, Energy Security, and Emergency Response and its Office of Intelligence and Counterintelligence.

97 “U.S.-Ukraine Energy Cooperation,” U.S. Department of Energy – Office of International Affairs.

98 Ellen Nakashima, “With New Indictment, U.S. Launches Aggressive Campaign to Thwart Economic Attacks,” *Washington Post*, November 1, 2018, https://www.washingtonpost.com/world/national-security/with-new-indictments-us-launches-aggressive-campaign-to-thwart-chinas-economic-attacks/2018/11/01/70dc5572-dd78-11e8-b732-3c72cbf131f2_story.html?utm_term=.a3fa576945f2.

99 Department of Justice, *Report of the Attorney General’s Cyber Digital Task Force* (Washington, DC: July 2, 2018, https://www.justice.gov/ag/page/file/1076696/download.

100 Ibid.

101 “Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System,” U.S. Department of Justice – Office of Public Affairs; “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,” U.S. Department of Justice – Office of Public Affairs, July 13, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

102 “Cybersecurity,” National Security Agency, https://www.nsa.gov/what-we-do/cybersecurity/.

103 For a recent example, see Warren P. Strobel, “Bolton Says U.S. is Expanding Offensive Cyber Operations,” *Wall*

Street Journal, June 11, 2019, https://www.wsj.com/articles/bolton-says-u-s-is-expanding-offensive-cyber-operations-11560266199.

104 "National Cyber Investigative Joint Task Force," FBI, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

105 "Who We Are," Cyber Threat Intelligence Integration Center – The Office of the Director of National Intelligence, https://www.dni.gov/index.php/ctiic-who-we-are.

106 "National Cyber Investigative Joint Task Force," FBI; ibid.

107 U.S. Congress, House, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, 115th Cong., became Public Law August 13, 2018, https://www.congress.gov/bill/115th-congress/house-bill/5515/text#toc-H0114859E2D0F-4DEFA6D32D714EF75F80.

108 Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms."

109 "National Security Agency, Cybercom Defend Against Election Meddling," U.S. Department of Defense, August 2, 2019, https://DoD.defense.gov/News/Article/Article/1592000/national-security-agency-cybercom-defend-against-election-meddling/.

110 Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms"; Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections."

111 David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?searchResultPosition=1.

112 "Research," CCDCOE, https://ccdcoe.org/research/; "CyCon," CCDCOE, https://ccdcoe.org/cycon/; "Interactive Cyber Law in Practice: Interactive Toolkit," CCDCOE, https://cyberlaw.ccdcoe.org/wiki/Main_Page; "Exercises," CCDCOE, https://ccdcoe.org/exercises/.

113 "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," U.S. Department of Justice – Office of Public Affairs, October 4, 2018, https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

114 Jackson and Cimino-Isaacs, "CFIUS Reform."

115 Ibid.

116 U.S. Congress, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*; Dan Stumpf and Kate O'Keeffe, "U.S. Blocks Some Exports from Huawei's Silicon Valley Unit," *Wall Street Journal*, https://www.wsj.com/articles/u-s-blocks-some-exports-from-huaweis-silicon-valley-unit-11547119803.

117 "The President's National Spectrum Strategy Will Give America a Boost in 5G," U.S. Department of Commerce, October 25, 2018, https://www.commerce.gov/news/blog/2018/10/presidents-national-spectrum-strategy-will-give-america-boost-5g.

118 Cecilia Kang and David E. Sanger, "Huawei is a Target as Trump Moves to Ban Foreign Telecom Gear," *New York Times*, May 15, 2019, https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html.

119 Ibid.

120 "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," White House, May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

121 Kang and Sanger, "Huawei is a Target as Trump Moves to Ban Foreign Telecom Gear"; Ibid. Regarding assessments and reports, the Director of National Intelligence and secretary of DHS are to deliver "periodic" assessments of threats and vulnerabilities to the United States with concern to relevant technologies. The secretary of DHS, "in consultation as appropriate with the Secretary of the Treasury, the Secretary of Homeland Security, Secretary of State, the Secretary of Defense, the Attorney General, the United States Trade Representative, the Director of National Intelligence, and the Chairman of the Federal Communications Commission," will deliver a report to the president on the progress this EO has made in blocking harmful technologies in the United States.

122 "Communications Security, Reliability, and Interoperability Council," Federal Communications Commission, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

123 "Annex 3-14 Counterspace Operations," Curtis E. Lemay Center for Doctrine Development and Education, August

27, 2018, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-14/Annex-3-14-Counterspace-Ops.pdf.

124 "Text of Space Policy Directive-4: Establishment of United States Space Force," White House, Presidential Memoranda, February 19, 2019, https://www.whitehouse.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/.

125 Todd Harrison, "Why We Need a Space Force," CSIS, Commentary, October 3, 2018, https://www.csis.org/analysis/why-we-need-space-force.

126 White House, *National Cyber Strategy* (Washington, DC: 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

127 Ibid., p. 7.

128 Kang and Sanger, "Huawei is a Target as Trump Moves to Ban Foreign Telecom Gear."

129 "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," White House.

130 Interview conducted by authors on January 16, 2019..

131 Michael Sulmeyer, "How the U.S. Can Play Cyber-Offense," *Foreign Affairs*, March 22, 2018, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.

132 "President Donald J. Trump is Unveiling an America First National Space Strategy," White House, March 23, 2018, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.

133 Text of Space Policy Directive-4: Establishment of the United States Space Force," White House, Presidential Memoranda, February 19, 2019, https://www.whitehouse.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/.

134 Kaitlyn Johnson, "Space Force or Space Corps?" The Center for Strategic and International Studies, June 27, 2019, https://www.csis.org/analysis/space-force-or-space-corps.

135 Erin Banco and Betsy Woodruff, "Trump's DHS Guts Task Forces Protecting Elections From Foreign Meddling," Daily Beast, February 13, 2019, https://www.thedailybeast.com/trumps-dhs-guts-task-forces-protecting-elections-from-foreign-meddling; William A. Carter, *CSIS 2018 Election Security Scorecard: The Outlook for 2018, 2020, and Beyond* (Washington, DC: CSIS, October 2018), https://www.csis.org/analysis/csis-election-cybersecurity-scorecard-outlook-2018-2020-and-beyond.

136 Kathleen J. McInnis and Stephen M. McCall, "'Space Force' and Related DoD Proposals: Issues for Congress," Congressional Research Service, April 8, 2019, https://crsreports.congress.gov/product/pdf/IF/IF11172.

137 Johnson, "Space Force or Space Corps?"

138 Ibid.

139 Joseph Marks, "The Cybersecurity 202: Here's how the military's hacking arm is gearing up to protect the 2020 election," *Washington Post*, May 8, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/05/08/the-cybersecurity-202-here-s-how-the-military-s-hacking-arm-is-gearing-up-to-protect-the-2020-election/5cd23177a7a0a46cfe152c7e/?utm_term=.73b9f5b8b314.

140 "Presidential Policy Directive – U.S. Cyber Incident Coordination/PPD-41," White House, July 26, 2016, https://fas.org/irp/offdocs/ppd/ppd-41.html.

141 Suzanne Spaulding and Ted Schlein, "Does the U.S. Need a Cabinet-Level Department of Cybersecurity?" *Wall Street Journal*, June 3, 2019, https://www.wsj.com/articles/does-the-u-s-need-a-cabinet-level-department-of-cybersecurity-11559586996.

142 Ibid.

143 Government Accountability Office , "Defense Space Acquisitions: Too Early to Determine If Recent Changes Will Resolve Persistent Fragmentation in Management and Oversight," July 26, 2016, https://www.gao.gov/assets/680/678697.pdf; McInnis and McCall, "'Space Force' and Related DoD Proposals."

144 Ibid.

145 Thomas Gibbons-Neff, "How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/world/middleeast/american-commandos-russian-mercenaries-syria.html.

146 Asia Maritime Transparency Initiative, “China Island Tracker,” CSIS, https://amti.csis.org/island-tracker/china/#Spratly%20Islands.

147 Ibid.

148 Michael Schwirtz, “A Year After Skripal Poisoning, Russia Offers Defiant Face to Britain and the West,” *New York Times*, March 4, 2019, https://www.nytimes.com/2019/03/04/world/europe/russia-skripal-poisoning-britain.html; Joshua Berlinger, “U.S. Sanctions North Korea After Blaming Country for Kim Jong Nam’s Killing,” CNN, March 7, 2018, https://www.cnn.com/2018/03/07/politics/kim-jong-nam-sanctions-intl/index.html.

149 The Leahy Law prevents the United States from partnering with security forces that have committed human rights violations. Countries like Iran and Russia do not have these same limitations, frameworks of oversight, and responsibility for accountability. This will continue to be a capability advantage for adversaries, as the United States cannot sacrifice its rules, norms, and values for human rights protections. “U.S. Code 2378d. Limitation on Assistance to Security Forces,” Legal Information Institute,Cornell Law School, https://www.law.cornell.edu/uscode/text/22/2378d.

150 Seth G. Jones, “War by Proxy: Iran’s Growing Footprint in the Middle East,” CSIS, *CSIS Brief*, March 2019, 4-5, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190312_IranProxyWar_FINAL.pdf; Seth G. Jones and Maxwell B. Markusen, “The Escalating Conflict with Hezbollah in Syria,” CSIS, *CSIS Brief*, June 2018, 2, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180620_JonesMarkusen_EscalatingConflict_FINAL.pdf?hLyKL-4vUoURgwuGdWHooVx9Q6A_sKRta.

151 Jones, “War by Proxy,” 10.

152 The Office of Terrorism and Financial Intelligence and OFAC are both within the Department of Treasury and can enforce sanctions against Iranian and Russian gray zone activity. The Department of Treasury is also a member of the Financial Action Task Force (FATF), an international organization that sanctions terrorist organizations.

153 U.S. House Committee on Armed Services, “Statement of General Curtis M. Scaparrotti, Commander, United States European Command,” March 28, 2017, https://www.armedservices.senate.gov/imo/media/doc/Scaparrotti_03-05-19.pdf.

154 Paul Zukunft, “Navigating the Fourth Coast,” in *Shifting Currents in the Arctic: Perspectives from Three Artic Littoral States* (Washington, DC: CSIS, May 2019), p. 4, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190501_NorthernConnections.pdf.

155 Pat Towell and Aras D. Kazlauskas, “The European Deterrence Initiative: A Budgetary Overview,” Congressional Research Service, August 8, 2018, https://fas.org/sgp/crs/natsec/IF10946.pdf.

156 U.S. Congress, *Ukraine Freedom Support Act of 2014*.

157 “Department of Defense Directive: Irregular Warfare (IW), 3000.07,” U.S. Department of Defense, May 12, 2017, 2, https://fas.org/irp/DoDdir/DoD/d3000_07.pdf.

158 Andrew Feickert, “Army Security Force Assistance Brigades (SFABs),” Congressional Research Service, October 24, 2018, https://fas.org/sgp/crs/natsec/IF10675.pdf.

159 “Ref Book – Department of Defense Title 10 Authorities,” Office of the Director of National Intelligence, https://www.dni.gov/index.php/ic-legal-reference-book/department-of-defense-title-10-authorities.

160 “U.S. Code: Title 22. Foreign Relations and Intercourse,” Cornell Law School – Legal Information Institute, https://www.law.cornell.edu/uscode/text/22.

161 “Iran Sanctions,” U.S. Department of Treasury, https://www.treasury.gov/resource-center/sanctions/programs/pages/iran.aspx; Berlinger, “U.S. Sanctions North Korea After Blaming Country for Kim Jong Nam’s Killing.”

162 “Statement from the President on the Designation of the Islamic Revolutionary Guard Corps as a Foreign Terrorist Organization,” White House, April 8, 2019, https://www.whitehouse.gov/briefings-statements/statement-president-designation-islamic-revolutionary-guard-corps-foreign-terrorist-organization/.

163 Thomas Gibbons-Neff, “How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria.”

164 Andrew E. Kramer, “Ukraine’s President Appeals for NATO Support After Russia Standoff,” *New York Times*, November 29, 2018, https://www.nytimes.com/2018/11/29/world/europe/ukraine-russia-nato.html; Ihor Kabanenko, “Strategic Implications of Russia and Ukraine’s Naval Clash on November 25,” *Eurasia Daily Monitor* 15, no. 167 (November 2018), https://jamestown.org/program/strategic-implications-of-russia-and-ukraines-naval-clash-on-november-25/.

165 U.S. Congress, *Asia Reassurance Initiative Act of 2018*.

166 Ibid.

167 DoD, Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region (Washington, DC: June 2019), https://media.defense.gov/2019/May/31/2002139210/-1/-1/1/DOD_INDO_PACIFIC_STRATEGY_REPORT_JUNE_2019.PDF.

168 Judy Dempsey, "NATO Just Turned 70 – and It's Showing Its Age," *Washington Post*, April 4, 2019, https://www.washingtonpost.com/opinions/2019/04/04/nato-just-turned-its-showing-its-age/?utm_term=.681267d95762.

169 Amy F. Woolf, "Russian Compliance with the Intermediate Range Nuclear Forces (INF) Treaty: Background and Issues for Congress," Congressional Research Service, February 8, 2019, 2, https://fas.org/sgp/crs/nuke/R43832.pdf.

170 David. Oakley, "The Problems of a Militarized Foreign Policy for America's Premier Intelligence Agency," War on the Rocks, May 2, 2019, https://warontherocks.com/2019/05/the-problems-of-a-militarized-foreign-policy-for-americas-premier-intelligence-agency/.

171 See for example, Project on National Security Reform and the Center for the Study of the Presidency, *Forging a New Shield* (Washington DC: November 2008) or the Beyond Goldwater-Nichols Project, (Center for Strategic and International Studies, 2004–2008).

172 A case study on the U.S. "45-Year Long Gray Zone Struggle" in the Cold War, 1947–1989, is in Appendix B; a case study on Israel-Iran competition, 1991–2015, is in Appendix C; and a case study from the private sector, First Solar, 2006–2012, is in Appendix D.

173 "[Intelligence agencies] collect a staggering amount of information, synthesize reports from secret and open sources, and try to distill it into digestible analytical products for policymakers, diplomats, and military officers." Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (New York: Cornell University Press, 2011), p.vii.

174 For challenges with Russian legal warfare (lawfare), see Mark Voyger, "Russian Lawfare–Russia's Weaponisation of International and Domestic Law: Implications for the Region and Policy Recommendations," *Journal on Baltic Security* 4, no. 2 (2018), https://content.sciendo.com/abstract/journals/jobs/ahead-of-print/article-10.2478-jobs-2018-0011.xml.

175 "Analytic Standards," Office of the Director of National Intelligence, Intelligence Community Directive, January 2, 2015, https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

176 Ibid.

177 "It has become harder for Western countries to spy on places such as China, Iran, and Russia and easier for those countries' intelligence services to spy on the rest of the world." Edward Lucas, "The Spycraft Revolution," *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/."

178 On the challenges posed by process flow/integrating information into a coherent product, see the discussion on filtering data here: The United States Geospatial Intelligence Foundation, *The State and Future of GEOINT 2018* (Virginia, 2018), p. 4, https://usgif.org/system/uploads/5489/original/2018_SaFoG_PDF_Final.pdf?1518125527.

179 Economic gray zone activity by China demonstrates the challenges of resolving near-term priorities with the recognition of a long-term campaign; addressing Chinese IP theft, the Belt and Road Initiative, and growing dominance in the telecommunication market risks upsetting the balance of trade and other existing relations.

180 As two notable examples of gray zone activity, China's reef dredging in the South China Sea and Russia's military intervention in Crimea highlight the various challenges inherent in the three themes of temporality, attribution, and intent. Chinese and Russian objectives and execution differed in these cases, but their tactics—leveraging ambiguity to delay response and ensuring that their activities fall short of direct conflict with the United States or regional countries—are largely the same, underscoring the presence of a persistent dilemma for U.S. policymakers and operators.

181 Nicole Perloth and David E. Sanger, "White House Eliminates Cybersecurity Coordinator Role," *New York Times*, May 15, 2018, https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html.

182 Suzanne Spaulding, Devi Nair, and Arthur Nelson, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System* (Washington, DC: CSIS, 2019), 35, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf.

183 "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," White House, Executive Order, May 11, 2017, https://www.whitehouse.gov/presidential-actions/presiden-

tial-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

184 Gabriel Cederberg, *Catching Swedish Phish: How Sweden is Protecting its 2018 Elections* (Cambridge, MA, The Belfer Center, Harvard Kennedy School, August 2018), 1, https://www.belfercenter.org/sites/default/files/files/publication/Swedish%20Phish%20-%20final2.pdf.

185 Ibid., 1

186 Ibid., 13.

187 Elizabeth Schulze, "How a tiny country bordering Russia became one of the most tech-savvy societies in the world," CNBC, February 8, 2019, https://www.cnbc.com/2019/02/08/how-estonia-became-a-digital-society.html.

188 "Internet Voting in Estonia," National Democratic Institute, https://www.ndi.org/e-voting-guide/examples/internet-voting-in-estonia.

189 Ojars Eriks Kalnins, "Resilience of Necessity in the Baltics," Royal United Services Institute, January 31, 2019, https://rusi.org/commentary/resilience-necessity-baltics.

190 Ibid.

191 "About Us," CCDCOE, https://ccdcoe.org/about-us/.

192 "What is Hybrid COE?" European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/what-is-hybridcoe/.

193 Ibid.

194 "Lloyd Joins New British Banking Cyber Defense Alliances: Sources," Reuters, February 9, 2017, https://www.reuters.com/article/us-lloyds-cyber/lloyds-joins-new-british-banking-cyber-defense-alliance-sources-idUSKBN15O28O.

195 Ibid.

196 Ibid.

197 Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Washington, DC: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR1772.html.

198 "50 U.S. Code § 3021.National Security Council," Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/uscode/text/50/3021.

199 Critiques of an overly powerful NSC should be heeded, particularly when it constrains agency innovation.

200 "The sources of information overload are not singular in nature. Instead they comprise collections from across all major intelligence agencies. The volume of every form of intelligence increased markedly in the post war era and was not confined to SIGINT. Virtually every form of Technical Intelligence from SIGINT, MASINT, and IMINT (now GEOINT) to include the emerging fields of CYBINT and SOCINT (Social Media Intelligence) are expanding at near exponential rates." Aaron F. Brantly, "When everything becomes intelligence: machine learning and the connected world," *Intelligence and National Security* 33, no. 4 (2018): 566.

201 Michael E. DeVine and Heidi M. Peters, "National Counterterrorism Center (NCTC)," Congressional Research Service, July 11, 2018, https://fas.org/sgp/crs/intel/IF10709.pdf.

202 "Who We Are," National Counterterrorism Center – Office of the Director of National Intelligence, https://www.dni.gov/index.php/nctc-who-we-are.

203 National Counterterrorism Center, *Today's NCTC* (McLean, VA: August 2017), https://www.dni.gov/files/NCTC/documents/features_documents/NCTC-Primer_FINAL.pdf.

204 DeVine and Peters, "National Counterterrorism Center (NCTC)."

205 Ibid.

206 "National Counterterrorism Center," Congressional Research Service, July 11, 2018, https://fas.org/sgp/crs/intel/IF10709.pdf.

207 Ibid.

208 Evan Munsing and Christopher J. Lamb, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success* (Washington, DC: National Defense University Press: June 2011), 7-9, https://ndupress.ndu.edu/portals/68/documents/stratperspective/inss/strategic-perspectives-5.pdf.

209 Ibid., 11; Bill Flavin ed., *Stabilization: A New Approach to Whole of Government Operational Planning and Execution*

(Carlisle, PA: U.S. Army Peacekeeping and Stability Operations Institute, June 2018), https://publications.armywarcollege.edu/pubs/3540.pdf.

210 "About Us," Joint Interagency Task Force South, U.S. Southern Command, https://www.jiatfs.southcom.mil/About-Us/.

211 Munsing and Lamb, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*, 34–35.

212 The Active Measures Working Group was a "part-time interagency committee established in the 1980s to counter Soviet disinformation effectively accomplished its mission. The group successfully established and executed U.S. policy on responding to Soviet disinformation. It exposed some Soviet covert operations and raised the political cost of others by sensitizing foreign and domestic audiences to how they were being duped. The group's work encouraged allies and made the Soviet Union pay a price for disinformation that reverberated all the way to the top of the Soviet political apparatus. It became the U.S. government's body of expertise on disinformation and was highly regarded in both Congress and the executive branch." See Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference* (Washington, DC: National Defense University's Institute for National Strategic Studies, June 2012), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.

213 The Senate Armed Services Committee has included a provision in the draft FY2020 National Defense Authorization Act requiring a report from DoD on its cost imposition strategies for both China and Russia. See U. S. Congress, Senate, *National Defense Authorization Act for Fiscal Year 2020*, S. 1790, 116th Cong., 1st sess., https://www.congress.gov/116/bills/s1790/BILLS-116s1790rs.pdf; A similar recommendation was made in National Defense Strategy Commission, *Providing for the Common Defense: The Assessment and Recommendations of the National Defense Strategy Commission* (Washington, DC: United States Institute of Peace, November 2018), https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf; The XX NDAA has also already required the creation of these strategies, but the administration has not yet published either.

214 "50 U.S. Code § 3021.National Security Council," Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/uscode/text/50/3021.

215 For more on the advantages of creating mission managers, see Christopher J. Lamb, "National Security Reform," in R.D. Hooker, Jr. ed., *Charting a Course: Strategic Choices for a New Administration* (Washington, DC: National Defense University Press, December 2016), 84–88, https://inss.ndu.edu/Portals/68/Documents/Books/charting-a-course/charting-a-course.pdf?ver=2016-12-08-154300-120.

216 Eric Rosenbach and Katherine Mansted, "The Geopolitics of Information," Belfer Center for Science and International Affairs, Harvard Kennedy School, May 28, 2019, https://www.belfercenter.org/publication/geopolitics-information.

217 Those that wish for the re-creation of the USIA may miss that even at its height, the USIA did not have the personnel, funding, support, training, or mandate to match the massive Soviet propaganda machine. In addition, the USIA operated at a time where information traveled through more limited means and was able to cover and access many foreign media markets. The current information environment is much different: vast, open to all, and atomized. Advocates of recreating the USIA may also be wishing for a whole-of-government strategy, not only a way to communicate it effectively.

218 The USAGM cannot convey political messaging, engages countries that have limited press, and cannot compete in spaces where Western media operate.

219 "Visit Us – The National Electoral Education Centre," Australian Electoral Commission, https://education.aec.gov.au/visit-us/.

220 "Stärkt digital kompetens i skolans styrdokument," Regeringen, March 9, 2017, https://www.regeringen.se/contentassets/acd9a3987a8e4619bd6ed95c26ada236/informationsmaterial-starkt-digital-kompetens-i-skolans-styrdokument.pdf.

221 Adam Satariano and Elian Peltier, "In France, School Lessons Ask: Which Twitter Post Should You Trust," *New York Times*, December 13, 2018, https://www.nytimes.com/2018/12/13/technology/france-internet-literacy-school.html.

222 Ibid.

223 Kalnins, "Resilience of Necessity in the Baltics."

224 "New Version of Handbook for Communicators – Countering Information Influence Activities," Swedish Civil Contingencies Agency, https://www.msb.se/en/Tools/News/New-version-of-handbook-for-communicators--Counter-

ing-information-influence-activities-/; "Training Exercises," Swedish Civil Contingencies Agency, https://www.msb.se/en/Training--Exercises/; Steven Lee Meyers, "'E-Stonia' Accuses Russia of Computer Attacks," New York Times, May 18, 2007, https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjawKvDmf7i-AhWNgVwKHb1LBVAQFjAAegQIABAB&url=https%3A%2F%2Fwww.nytimes.com%2F2007%2F05%2F18%2F-world%2Feurope%2F18cnd-russia.html&usg=AOvVaw0s-W_1_FCTqUMMndxzRzk6.

225 "Risk of Interference in Swedish Elections 2018," Säkerhetspolisen, Swedish Security Service, January 24, 2018, www.sakerhetspolisen.se/en/swedish-security-service/about-us/press-room/current-events/news/2018-01-24-risk-of-interference-in-swedish-elections-2018.html.

226 "About Us – Ukraine Crisis Media Center," Ukraine Crisis Media Center, http://uacrisis.org/about.

227 "About Us – StopFake," StopFake.org, https://www.stopfake.org/en/about-us/.

228 Kalnins, "Resilience of Necessity in the Baltics"; "About Us," Baltic Centre for Investigative Journalism, re:Baltica, https://en.rebaltica.lv/about-us/.

229 "About Our Mission," Global Internet Forum to Counter Terrorism, https://www.gifct.org/about/; Also, see Michael McFaul, *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Elections and Beyond* (Palo Alto: Stanford University, June 2019), https://cyber.fsi.stanford.edu/securing-our-cyber-future.

230 Stanley McChrystal, "Every American Should Serve for One Year," *Time*, June 20, 2017, http://time.com/naitonal/year-national-service-americorps-peace-corps/.

231 Michael Sulmeyer, "How the U.S. Can Play Cyber-Offense," *Foreign Affairs*, March 22, 2018, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.

232 Ibid.

233 McFaul, *Securing American Elections*.

234 Adam Satariano, "Europe is Reigning in Tech Giants. But Some Say It's Going Too Far," *New York Times*, May 6, 2019, https://www.nytimes.com/2019/05/06/technology/europe-tech-censorship.html.

235 Rosenbach and Mansted, "The Geopolitics of Information."

236 "[Intelligence agencies] collect a staggering amount of information, synthesize reports from secret and open sources, and try to distill it into digestible analytical products for policymakers, diplomats, and military officers." Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithica, New York: Cornell University Press, 2011), p.vii.

237 For challenges with Russian legal warfare (lawfare), see Mark Voyger, "Russian Lawfare – Russia's Weaponisation of International and Domestic Law: Implications for the Region and Policy Recommendations," *Journal on Baltic Security* 4, no. 2 (2018), https://content.sciendo.com/abstract/journals/jobs/ahead-of-print/article-10.2478-jobs-2018-0011.xml.

238 Aaron F. Brantly, "When everything becomes intelligence: machine learning and the connected world," *Intelligence and National Security* 33, no. 4 (2018): 566. Regarding the acronyms used in this sentence, they stand for the following: SIGINT (signals intelligence), MASINT (measurement and signature intelligence), IMINT (imagery intelligence), GEOINT (geospatial intelligence), and CYBINT (cyber intelligence). These acronyms are used throughout this paper.

239 Heather Conley et al., *The Kremlin Playbook 2: The Enablers* (Lanham: Rowman & Littlefield, 2019), 56.

240 "Many of the complex questions fielded by intelligence agencies often reside within sub-populations and outside of easily accessible information sources. It is extremely difficult to capture historical data in the present, whether by survey on what an individual's perceptions of an event, particular policy, law, practice, or decision were, yet big data is increasingly building a historical repository of data on these perceptions in the form of social media posts, news archives, recorded emails, web-traffic logs and much more. Information captured in stream and stored for later use such as email communications, forums, chat logs, browser histories, and many other types of data can help to inform future analysis when novel questions and their subsequent informed hypotheses are developed." Brantly, "When everything becomes intelligence."

241 Office of the Director of National Intelligence, "Analytic Standards," Intelligence Community Directive 203, https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

242 Ibid.

243 Shawn Powers and Markos Kounalakis, eds., *Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation* (Washington, DC: Advisory Commission on Public Diplomacy, 2017), 29, https://www.state.gov/documents/organization/271028.pdf.

244 On the potential downsides to publicizing an adversary's illicit behave, see Allison Carnegie and Austin Carson, "The Spotlight's Harsh Glare: Rethinking Publicity and International Order," *International Organization* 72, no. 3 (2018): 627–657.

245 Office of the Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," written statement of Daniel R. Coats, January 29, 2019, 7, https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

246 Office of the Director of National Intelligence, "A Guide to Cyber Attribution," September 14, 2018, 2, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.

247 Ibid., p. 2–3; Two additional sections in the ODNI report that are relevant to this discussion are "Best Practices for Determining Attribution" and "Best Practices for Presenting Attribution Analysis." See ibid., 3–4.

248 Sasha Romanosky and Benjamin Boudreaux, *Private Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government* (Santa Monica, CA: RAND Corporation, 2019), 28, https://www.rand.org/pubs/working_papers/WR1267.html.

249 "It has become harder for Western countries to spy on places such as China, Iran, and Russia and easier for those countries' intelligence services to spy on the rest of the world." Edward Lucas, "The Spycraft Revolution," *Foreign Policy*, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/.

250 Office of the Director of National Intelligence, "A Guide to Cyber Attribution."

251 Policymakers must also be sensitive to the possibility that using public attribution to "name and shame" adversaries may unintentionally lead to negative political backlash. For an EU example, see Michael Peel, Mehreen Khan, and Max Seddon, "EU attack on pro-Kremlin 'fake news' takes a hit," *Financial Times*, April 2, 2018, https://www.ft.com/content/5ec2a204-3406-11e8-ae84-494103e73f7f.

252 Sean Lyngaas, "FBI to private industry: Attribution won't deter North Korean hacking," Cyber Scoop, October 26, 2018, https://www.cyberscoop.com/fbi-north-korea-hacking-wont-stop-tlp-green/.

253 Lyngaas, "FBI to private industry: Attribution won't deter North Korean hacking."

254 For a theoretical explanation and in-depth case studies on why policymakers and intelligence analysts value different indicators/warnings when assessing adversaries, see Keren Yarhi-Milo, "In the Eye of the Beholder: How Leaders and Intelligence Communities Assess the Intentions of Adversaries," *International Security* 38, no. 1 (2013): 7–51, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00128.

255 James J. Wirtz, "Indications and Warning in an Age of Uncertainty," *International Journal of Intelligence and Counter-Intelligence* 26, no. 3 (2013): 552, https://core.ac.uk/download/pdf/36739628.pdf.

256 On the challenges posed by process flow and integrating information into a coherent product, see the discussion on filtering data here: The United States Geospatial Intelligence Foundation, *The State and Future of GEOINT 2018* (Virginia: 2018), 4, https://usgif.org/system/uploads/5489/original/2018_SaFoG_PDF_Final.pdf?1518125527.

257 Murgia, Madhumita and Yuan Yang, "Microsoft Worked with Chinese Military University on Artificial Intelligence," *Financial Times*, April 10, 2019, https://www.ft.com/content/9378e7ee-5ae6-11e9-9dde-7aedca0a081a.

258 Kanishka Singh, "Elite U.S. school MIT cuts ties with Chinese tech firms Huawei, ZTE," Reuters, April 4, 2019, https://www.reuters.com/article/us-usa-huawei-tech-zte/elite-u-s-school-mit-cuts-ties-with-chinese-tech-firms-huawei-zte-idUSKCN1RG0FS.

259 "The sources of information overload are not singular in nature. Instead they comprise collections from across all major intelligence agencies. The volume of every form of intelligence increased markedly in the post war era and was not confined to SIGINT. Virtually every form of Technical Intelligence from SIGINT, MASINT, and IMINT (now GEOINT) to include the emerging fields of CYBINT and SOCINT (Social Media Intelligence) are expanding at near exponential rates." Brantly, "When everything becomes intelligence," 566.

260 USGIF, *The State and Future of GEOINT 2018*, 4.

261 Angela Dewan, Milena Veselinovic, and Carol Jordan, "These are all the countries that are expelling Russian diplomats," CNN, March 28, 2018, https://www.cnn.com/2018/03/26/europe/full-list-of-russian-diplomats-expelled-over-s-intl/index.html.

262 U.S. Southern Command, “Posture Statement of Admiral Kurt W. Tidd,” before the Senate Armed Services Committee, February 2018, https://www.southcom.mil/Portals/7/Documents/Posture%20Statements/SOUTHCOM_2018_Posture_Statement_FINAL.PDF?ver=2018-02-15-090330-243.

263 Danielle Cave et al., *Mapping China’s Tech Giants* (Barton, Australia: Australian Strategic Policy Institute, 2019), International Cyber Policy Centre, Issues Paper, Report No. 15, https://www.aspi.org.au/report/mapping-chinas-tech-giants.

264 Reid Standish, “Why Is Finland Able to Fend Off Putin’s Information War?” *Foreign Policy*, March 1, 2017, https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

265 For additional evidence, see Martin Kragh and Sebastian Åsberg, “Russia’s strategy for influence through public diplomacy and active measures: the Swedish case,” *Journal of Strategic Studies* 40, no. 6 (2017): 773-816, https://www.tandfonline.com/doi/abs/10.1080/01402390.2016.1273830?journalCode=fjss20.

266 Kate Fazzini and Kevin Breuninger, “Justice Department charges Chinese nationals in ‘extensive’ global hacking campaign,” CNBC, December 20, 2018, https://www.cnbc.com/2018/12/20/doj-china-national-security-law-enforcement-action.html; Foreign & Commonwealth Office, National Cyber Security Centre, and The Rt Hon Jeremy Hunt MP, “UK and allies reveal global scale of Chinese cyber campaign,” gov.uk, December 20, 2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign.

267 John Schaus et al., “What Works: Countering Gray Zone Coercion,” CSIS, *CSIS Briefs*, July 16, 2018, https://www.csis.org/analysis/what-works-countering-gray-zone-coercion.

268 Joseph Votel et al., “Unconventional Warfare in the Gray Zone,” *Joint Forces Quarterly* 80 (2016), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf.

269 Kennan’s memorandum addressed the full spectrum of gray zone warfare activities which the United States must be prepared to utilize and defend itself from. The memorandum reads: “Political warfare is the logical application of Clausewitz’s doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation’s command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP), and ‘white’ propaganda to such covert operations as clandestine support of ‘friendly’ foreign elements, ‘black’ psychological warfare and even encouragement of underground resistance in hostile states.” History and Public Policy Program Digital Archive, “George F. Kennan on Organizing Political Warfare,” April 30, 1948, Obtained and contributed to CWIHP by A. Ross Johnson. Cited in his book *Radio Free Europe and Radio Liberty*, Ch1 n4 – NARA release courtesy of Douglas Selvage. Redacted final draft of a memorandum dated May 4, 1948 and published with additional redactions as document 269, FRUS, Emergence of the Intelligence Establishment.

270 Meena Bose, “What Have We Learned About How Presidents Organize for National Security Decision Making, 1947–2017?” in Heidi B. Demarest and Erica D. Borghard, eds., *U.S. National Security Reform: Reassessing the National Security Act of 1947* (New York: Routledge, 2019).

271 For more on “New Look,” see NSC 162/2, the culmination of the Project Solarium exercise in devising a revised Containment posture for the United States. For more on “Flexible Response,” see Maxwell Taylor’s *Uncertain Trumpet*; also see M.F. Millikan and W.W. Rostow, “Foreign Aid: Next Phase,” *Foreign Affairs* 36, no. 3 (April 1958): 418–436.

272 For more on “New Look,” see NSC 162/2, the culmination of the Project Solarium exercise in devising a revised Containment posture for the United States.

273 Under the Eisenhower administration, the USG attempted to centralize its economic, military, and technical assistance programs under the Foreign Operations Administration (FOA). Unlike the CIA, however, the traditional authorities—DoD and State—were able to reestablish control by the late-1950s. See Eisenhower’s Reorganization Plan 7, 1953.

274 Richard A. Best, Jr., *The National Security Council: An Organizational Assessment*, (Washington, DC: Congressional Research Service, 2011), RL30840, 13, https://fas.org/sgp/crs/natsec/RL30840.pdf.

275 For more on the differences between a “symmetric” and “asymmetric” approach and their synthesis, see John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security during the Cold War* (New York: Oxford University Press, 2005), 145, 213, 343.

276 Vladislav Zubok, “Soviet foreign policy from détente to Gorbachev, 1975-1985,” in Melvyn Leffler and Odd Arne Westad, eds., *The Cambridge History of the Cold War: Volume III, Endings* (Cambridge, UK: Cambridge University Press, 2010), 102, 106.

277 U.S. National Security Council, "National Security Decision Directive 2," January 12, 1982, https://fas.org/irp/offdocs/nsdd/nsdd-2.pdf.

278 As Richard Betts explains, "designers [of governing institutions] can only aim for structures and processes that will enable a proper process or decision; they cannot select the individuals who accede to power over time and inhabit the structures." Richard K. Betts, "The Durable National Security Act," in Demarest and Borghard, *U.S. National Security Reform*. 2019

279 The OPC was the product of USG recognition that it required an organization to conduct covert operations. However, its initial oversight authorities were ambiguous, with State, DoD, and the CIA exerting differing, and ultimately insufficient, levels of control over its actions. Stephen J.K. Long, "Strategic Disorder, the Office of Policy Coordination and the Inauguration of U.S. Political Warfare against the Soviet Bloc, 1948–1950," *Intelligence and National Security* 27, no. 4 (2012), 465.

280 Betts, "The Durable National Security Act" in Demarest and Borghard, *U.S. National Security Reform*.

281 The "SOG" was initially named the "Special Activities Division."

282 Central Intelligence Agency, "Note for Assistant to the President for National Security Affairs from William J. Casey, DCI," October 19, 1984.

283 Highlighting the importance of multilateral cooperation is the U.S. participation in the Coordinating Committee on Export Controls to impose export restrictions with the Soviet Union. See Tor Egil Førland, "The History of Economic Warfare: International Law, Effectiveness, Strategies," *Journal of Peace Research* 30, no. 2 (May 1993): 155.

284 David B. Green, "From Friends to Foes: How Israel and Iran Turned Into Arch-Enemies," *Haaretz*, May 8, 2018, https://www.haaretz.com/middle-east-news/iran/MAGAZINE-how-israel-and-iran-went-from-allies-to-enemies-1.6049884.

285 "Home Front Command Throughout the Years," Home Front Command, accessed December 19, 2018, http://www.oref.org.il/1045-en/Pakar.aspx.

286 Yosef Kuperwasser, *Lessons from Israel's Intelligence Reforms* (Washington, DC: Brookings Institution, October 2007), https://www.brookings.edu/research/lessons-from-israels-intelligence-reforms/.

287 Belfer Center for Science and International Affairs, *Deterring Terror: How Israel Confronts the Next Generation of Threats* (Cambridge, MA: Harvard University, August 2016), https://www.belfercenter.org/sites/default/files/legacy/files/IDF%20doctrine%20translation%20-%20web%20final2.pdf.

288 Belfer Center for Science and International Affairs, *Deterring Terror: How Israel Confronts the Next Generation of Threats*.

289 In February 2019, the Committee on the Formulation of National Security Doctrine (Meridor Committee) released a report originating in the aftermath of the 2006 war that recommends the Israeli government formulate a longer-term, integrated strategic doctrine to meet the security priorities for today's security environment. While this itself is not a new national security doctrine, it is worth noting that the national security community in Israel is beginning to look at long-term implications and priorities.

290 It is worth noting that the prime minister of Israel has often also acted as defense minister, as empty government positions are legally filled by the prime minister. The first such case was David Ben Gurion.

291 The PMO has launched programs to recruit and pay university students to defend Israeli policy decisions and reputation and engage in other online and social media information battles.

292 Itamar Rabinovich, *Israel and the Changing Middle East* (Washington, DC: Brookings Institution, January 2015), https://www.brookings.edu/wp-content/uploads/2016/06/Israel-Rabinovich-01292015-1.pdf.

293 Elena Chachko, "Cyber Reform in Israel at an Impasse: A Primer," Lawfare, April 27, 2017, https://www.lawfareblog.com/cyber-reform-israel-impasse-primer.

294 Belfer Center, *Deterring Terror*.

295 Tamir Libel, "Looking for meaning: lessons from Mossad's failed adaptation to the post-Cold War era, 1991–2013," *Journal of Intelligence History* 14, no. 2 (April 2015): p. 83-95, https://www.tandfonline.com/doi/abs/10.1080/16161262.2015.1033238.

296 Noam Sheizaf, "Hasbara: Why Does the World Fail to Understand Us?" +972 Magazine, November 13, 2011, https://972mag.com/hasbara-why-does-the-world-fail-to-understand-us/27551/.

297 Chachko, "Cyber Reform in Israel at an Impasse."

298 Lieutenant Colonel Scott C. Farquhar, *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD* (Fort Leavenworth, KS: Combat Studies Institute Press, 2009), https://apps.dtic.mil/dtic/tr/fulltext/u2/a498599.pdf.

299 Kuperwasser, *Lessons from Israel's Intelligence Reforms*.

300 Libel, "Looking for Meaning."

301 David E. Johnson, "Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza," (Santa Monica, CA: RAND Corporation, 2010), https://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP285.pdf.

302 Meir Elran, "The Israeli Home Front Command," *Military and Strategic Affairs* 8, no. 1 (July 2016), http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/MASA8-1Eng_6.04Elran.pdf.

303 Johnson, "Military Capabilities for Hybrid War."

304 Ibid.

305 "An Eye for an Eye: The Anatomy of Mossad's Dubai Operation," *Spiegel*, January 17, 2011, http://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-s-dubai-operation-a-739908.html.

306 Mark Memmott, "'Prisoner X' Mystery Puts Spotlight On Israel's Spy Agency," NPR, February 14, 2013, https://www.npr.org/sections/thetwo-way/2013/02/14/171997678/prisoner-x-mystery-puts-spotlight-on-israels-spy-agency.

307 Libel, "Looking for Meaning."

308 Ibid.

309 Farquhar, *Back to Basics*.

310 Belfer Center, *Deterring Terror*.

311 Brian Katz, "Axis Rising: Iran's Evolving Regional Strategy and Non-State Partnerships in the Middle East," CSIS, *CSIS Briefs*, October 11, 2018, https://www.csis.org/analysis/axis-rising-irans-evolving-regional-strategy-and-non-state-partnerships-middle-east.

312 Francesco Meneguzzo et al., "The great solar boom: a global perspective into the far reaching impact of an unexpected energy revolution," *Energy Science & Engineering* 3, no. 6 (2015): 499–500, https://onlinelibrary.wiley.com/doi/epdf/10.1002/ese3.98.

313 First Solar, Inc., *Annual Report 2006* (Tempe, Arizona: 2006), 7–8, https://s2.q4cdn.com/646275317/files/doc_financials/annual/2006AnnualReport.pdf.

314 Neil Thompson and Jennifer Ballen, "First Solar," MIT Sloan School of Management, September 13, 2017, 1, https://mitsloan.mit.edu/LearningEdge/CaseDocs/17.181.FirstSolar.Thompson.pdf.

315 First Solar, Inc., *Annual Report 2009* (Tempe, Arizona: 2009), 3, https://s2.q4cdn.com/646275317/files/doc_financials/annual/Request-2009_annual_report.pdf.

316 First Solar, Inc., *Annual Report 2011* (Tempe, Arizona: 2011), 4, https://s2.q4cdn.com/646275317/files/doc_financials/annual/Final_11_Annual_Report.pdf.

317 Ibid., 12.

318 Thompson and Ballen, "First Solar," 7.

319 Ibid.

320 First Solar, Inc., *Annual Report 2011*, 3.

321 Thompson and Ballen, "First Solar." See p. 6 for analysis on relative strengths of utility market and p. 15 Exhibit 3 for module size relative to wattage produced of four leading Solar companies, including First Solar.

322 Eric Reguly, "Austerity pulling plug on Europe's green subsidies," *The Globe and Mail*, January 26, 2011, https://www.theglobeandmail.com/report-on-business/rob-commentary/austerity-pulling-plug-on-europes-green-subsidies/article622210/.

323 First Solar, Inc., Annual Report 2011, 6; Thompson and Ballen, "First Solar," 11–12.

324 Keith Bradhser, "China Benefits as U.S. Solar Industry Withers," *New York Times*, September 1, 2011, https://www.nytimes.com/2011/09/02/business/global/us-solar-company-bankruptcies-a-boon-for-china.html.

325 First Solar, Inc., *Annual Report 2011*, 84.

326 Ibid., 43.

327 Ibid., 44–45.

328 First Solar, Inc., "Corporate Governance Guidelines," November 9, 2017, http://www.firstsolar.com/-/media/First-Solar/Documents/Corporate-Collaterals/Corporate-Governance-Guidelines-2017.ashx

329 First Solar, Inc., *Annual Report 2009*, 5.

330 First Solar, Inc., *Annual Report 2011*, 6.

331 Thompson and Ballen, "First Solar," 8.

332 First Solar, Inc., Annual Report 2011, p. 45; First Solar, Inc., *Annual Report 2012* (Tempe, Arizona: 2012), 46, https://s2.q4cdn.com/646275317/files/doc_financials/annual/Final_Annual_Report_Bkmk.pdf.

333 First Solar, Inc., *Annual Report 2010* (Tempe, Arizona: 2010), 14, https://s2.q4cdn.com/646275317/files/doc_financials/annual/Request-FSLR_2011_annual_report.pdf; First Solar, Inc., *Annual Report 2011*, 13; First Solar, Inc., *Annual Report 2012*, 12.

334 First Solar, Inc., *Annual Report 2006*, 17.

335 First Solar, Inc., *Annual Report 2010*, 8.

336 First Solar, Inc., *Annual Report 2013* (Tempe, Arizona: 2013), 20, https://s2.q4cdn.com/646275317/files/doc_financials/annual/2014_FirstSolar_annual_report.pdf.

337 First Solar, Inc. *Annual Report 2011*, 3, and *see* footnote 321.

338 First Solar, Inc., *Annual Report 2011*, 3.

339 Thompson and Ballen, "First Solar," 11.

340 Ibid., 52.

341 First Solar, Inc., *Annual Report 2006*, 14–16.

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

ISBN 978-1-4422-8127-1

52000

9 781442 281271