Gaining Competitive Advantage in the Gray Zone

Response Options for Coercive Aggression Below the Threshold of Major War

Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/RR2942

Library of Congress Cataloging-in-Publication Data is available for this publication.
ISBN: 978-1-9774-0309-4

Published by the RAND Corporation, Santa Monica, Calif.

Cover: Stringer China/Reuters.

Preface

The United States is entering a period of intensifying strategic competition with several rivals, most notably Russia and China. U.S. officials expect this competition to be played out primarily below the threshold of armed conflict, in what is sometimes termed the *gray zone* between peace and war. This report offers the results of a RAND Corporation study examining how the United States might respond to Russian and Chinese efforts to seek strategic advantage through coercive actions. The study sought to build on extensive work to define and understand the gray zone challenge by focusing especially on what to do about it—laying out a strategic concept for the issue and a menu of response options. This report defines the principles on which a theory of success should rest, outlines a four-part concept for responding to gray zone aggression, and identifies and evaluates 35 types of responses that can be used as options for U.S. policy in dealing with gray zone threats.

This research was sponsored by the Office of the Deputy Assistant Secretary of Defense for Force Development and Strategy in the Office of the Secretary of Defense. It was conducted within the International Security and Defense Policy Center of the RAND National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense Intelligence Community.

For more information on the RAND International Security and Defense Policy Center, see www.rand.org/nsrd/ndri/centers/isdp or contact the director (contact information is provided on the webpage).

Contents

Figures and Tables

Figures

Tables

Summary

The 2017 U.S. National Security Strategy and the publicly released summary of the 2018 National Defense Strategy agree on one fundamental theme: The United States is entering a period of intensifying strategic competition with several rivals, most notably Russia and China. Numerous statements from senior U.S. defense officials make clear that they expect this competition to be played out primarily below the threshold of major war—in the spectrum of competition that has become known as the *gray zone*.

Although such tactics as psychological warfare, subversion of political systems, and covert paramilitary and information operations are not new phenomena in international conflict and competition, our analysis shows that some of the tactics employed by Russia and China are comparatively new in form and effect. Moreover, the methods of gray zone coercion vary significantly between Russia and China and require differentiation of scope of threat posed to the United States, as well as types of potential responses. Both problems represent a strategic threat to U.S. and allied interests, especially as techniques and technologies evolve over time. The United States and its allies, we find, have yet to come to terms with the challenge of the threat, let alone fashion a strategy to neutralize it or roll it back.

In this project, therefore, we aimed to provide a framework for conceptualizing the gray zone challenge and offer new policy options for the United States and its allies to consider in response. Despite the challenges involved, one finding of this research is that the United States can treat the ongoing gray zone competition more as an opportunity than a risk: By seeking to coerce, acquire influence within, or

destabilize key countries and regions, Russia and China are opening the space for a vigorous U.S. campaign to rally allies and partners in both regions in the direction of an effective response. This report uses insights from our extensive field research in affected countries, as well as general research into the literature on the gray zone phenomenon, to sketch out the elements of a strategic response to this challenge.

To inform such a response, we sought to (1) identify a potential strategic concept to govern a U.S. strategy in the gray zone and (2) identify and evaluate a menu of specific response options. It is important to emphasize that the scope of this study is to offer a menu of options that could be of utility to U.S. policymakers in both establishing a general strategy and choosing specific actions in response to gray zone tactics. We do not seek to offer a judgment of the relative efficacy of specific courses of action for discrete gray zone events or an assessment of how the adversary may respond; this should be the objective of follow-on research. The study focused on Russian and Chinese gray zone activities and potential U.S. and partner responses to them; we did not consider the gray zone tactics of other challengers.

Our primary source of information to support this analysis was an extensive program of field research in spring 2018. We traveled to Australia, the Czech Republic, France, Germany, Indonesia, Japan, the Philippines, Poland, Singapore, the United Kingdom, and Vietnam to gather perspectives on the ongoing gray zone challenge. We also interviewed officials and scholars in Washington, D.C., including several from the Republic of Georgia, and we met with current and former national security officials, scholars, and researchers.

In addition, we reviewed the existing literature on gray zone challenges for possible response options, as well as the literature on deterrence for its possible lessons for the gray zone context. We relied on all of these sources of information to construct a potential strategic concept for gray zone competition and to inform our evaluation of specific response options.

The set of response options offered in this report is designed to offer an initial draft of a living document. The menu of options ought to be fleshed out and refined over time based on experience and further consultations. We do not pretend that the options offered here

are comprehensive or optimal even now. And new ideas will emerge as the United States and its allies and partners gain more experience in this realm.

Summary of Themes: Russian and Chinese Gray Zone Campaigns and the Regional Responses

Our review of Russian gray zone campaigns in Europe indicates that they consist primarily of disinformation campaigns meant to undermine political institutions. Other Russian gray zone tactics include the use of economic tools to extract concessions or hold countries at risk of being coerced through an over-reliance on Russian energy; the demonstration of military threats through exercises near the borders of certain states; and, in a few extreme cases, the infiltration of Russian security forces to exert de facto control over disputed territory. These approaches are not new, but many of the tools now available provide expanded opportunities for Russia to affect societies and politics outside its border. The sophistication of Russia's tactics has also increased somewhat over time.

Chinese gray zone tactics have often assumed a more materially threatening form. Russia's more virtual and ephemeral approach has complicated policy responses. The long-term challenge for European states hoping to fashion policies that confront Russia's gray zone activities will be prioritizing timely and proportional whole-of-government counter-responses that deter future tactics without escalating to new thresholds of conflict that may lead to war.

As part of our analysis, we examined Chinese gray zone tactics and the regional response in Asia. In Northeast Asia, Japan believes that it is engaged in an increasingly high-stakes competition with China over efforts to change the status quo of territorial sovereignty and administrative control of the Senkaku Islands and nearby areas—a competition that Japanese leaders believe they are partly managing, at least for the time being, by deterring the China Coast Guard from escalating its activities and successfully expelling Chinese fishing boats that enter the Senkaku Islands' territorial waters without incident. Yet

the trends do not bode well for Japan: China Coast Guard patrols have begun to feature the presence of vessels that are more heavily armed, and the Chinese maritime militia continues to penetrate the Senkaku territorial sea with increasing regularity. Although Japan can continue to play defense against Chinese probing tactics, a change in strategy by China in favor of more, better-armed, and more-provocative penetrations by China Coast Guard and maritime militia vessels could potentially strain Japan's capacity to respond without increasing the potential for armed conflict.

In Southeast Asia, countries in the region have grown increasingly wary of China's gray zone aggression in the South China Sea. These activities include the use of law enforcement and a maritime militia in an unprofessional and escalatory manner to deter or, in some cases, actively deny the use of living and nonliving resources. Officials and scholars in the affected countries highlighted such tactics as bumping, shouldering, and ramming, as well as using water cannons, by the China Coast Guard against other nations' coast guard and fishing vessels. China's unprecedented expansion of artificial islands in the South China Sea and subsequent construction of logistics, maintenance, and storage facilities, along with airstrips, harbors, ports, and armament platforms, are in the process of further tilting the regional military balance in favor of China. Finally, China has supplemented these security-oriented aspects of its gray zone strategies with growing employment of economic coercion and political subversion.

Our research in these countries confirmed that they have identified the challenge from Chinese gray zone activities and seek to deter further attacks when feasible and appropriate. But there are significant limits on the ability of these countries to deal with the challenge on their own. They remain constrained by their military capacity to deter Chinese military and paramilitary activities, for example. Even more fundamentally, the nonaligned foreign policy orientations of many regional actors, and their accompanying desire to strike a tenuous balance of deterrence and engagement with China, are preventing more-forceful displays of deterrence.

Developing a Strategy for the Gray Zone

Much of the literature about the gray zone challenge has focused on identifying and characterizing the problem. Some analysts have proposed U.S. responses but have focused on the idea of deterring gray zone aggression, not offering a framework for responding in all dimensions—namely, military, diplomatic, informational, and economic. Rather than recommending that the United States merely remain on the defensive, we recommend a more comprehensive approach by going on the offensive—and adopting a whole-of-government approach to the problem.

In evaluating response options for gray zone activities, we first sought to develop a general strategic concept that would allow the United States to go beyond case-by-case reactions, knitting together individual actions to achieve more-meaningful results over the long term. In developing a strategic concept, we derived the following principles that should guide the U.S. response to the gray zone challenge:

1. The United States should not merely seek to mitigate losses in the gray zone but also aim to gain strategic advantage.
2. In seeking strategic advantage, the United States should be proactive rather than reactive in its approach to the gray zone challenge.
3. A core element of successful gray zone strategy is the ability to respond quickly to new provocations.
4. The United States should attempt to lead through multilateral processes and institutions even while being prepared for "go-it-alone" responses when U.S. leadership is essential to marshal a response.
5. U.S. responses must be aligned with local partners to the greatest extent possible.
6. Any strategy for responding to gray zone aggression must balance excessive risks of escalation—including military, diplomatic, and economic aspects—with the reality that, to be effective, countering gray zone aggression demands some degree of risk tolerance.

7. Gray zone tactics are a symptom of broader regional ambitions and grievances and cannot be addressed outside that context.
8. Russia and China continue to value their status as legitimate and respected members of the international system.
9. Not all gray zone aggression has equal significance for the security of regional allies and partners or for global norms.

Any meaningful strategic concept to gain strategic advantage must be based on a theory of success—that is, an argument for why specific policies are likely to produce desired outcomes. Some causal link must bind means to ends, explaining why the actions undertaken as part of the strategy will lead to or support those ends. The theory of success that we propose in this analysis is grounded in the principles that we develop from our assessment of Russian and Chinese goals and strategies. Those principles describe a situation in which the following are true:

- Russia and China are using gray zone techniques as a way of expressing dissatisfaction with aspects of the regional power and territorial status quo.
- Both are employing such tactics precisely because they want to express those desires and demands without completely alienating themselves from the international community and undermining their claim to great-power status and privileges.
- All significant regional players see these activities as a threat and have a significant—though, in many cases, constrained—appetite for U.S. leadership.
- The gray zone encompasses a wide spectrum of activities that pose consistent short- or long-term risks, and the various levels of threat must be carefully distinguished.
- Many of those tactics take place in such realms as competing over narratives, gaining political influence, and managing economic relations in which the United States and its allies and partners have, or ought to have, natural advantages.

These aspects of the gray zone context suggest the potential value of a theory of success that builds on the essential post–World War II U.S. grand strategic posture: building, leading, and speaking in the collective name of an informal community of status-quo states committed to international norms and rules. In other words, the concept of a rules-based order remains a highly appealing concept to rally support in Europe and Asia and offers the United States an opportunity to significantly strengthen its hand in the unfolding competition by using reactions to Chinese and Russian aggressiveness as the basis for strengthened regional postures.

Pushing the envelope on responses—that is, manipulating the risk of escalation for coercive leverage—can serve U.S. and allied purposes in some cases but not all. On the one hand, both Russia and China seek to avoid outright military clashes with the United States. The whole point of their gray zone approaches is to remain below the threshold of armed conflict. In some cases, more-escalatory U.S. responses could serve to call the bluff of Russia and China by forcing them to either change course or out-escalate the United States and its allies; our field research indicates that the latter option is unlikely in most instances. On the other hand, a strategic concept based solely around using every gray zone provocation as an invitation to out-escalate Russia and China would be neither prudent nor effective. Any escalatory steps obviously carry certain risks of unintended or accidental conflict. More than that, the United States will not be able to adopt a blanket approach of pushing the envelope in risk.

Thus, the theory of success underlying the proposed strategic concept could be stated as follows:

> The combination of intensified multilateral pressure, the identification of specific red lines, the credible commitment of the U.S. military, economic power, and expanded diplomatic efforts to address Chinese and Russian concerns can shift the risk and cost calculus for certain gray zone actions onto the aggressor, partly by playing to Chinese and Russian desires to preserve their international status and avoid regional balancing.

The theory of success that we propose here aims to marry enhanced multilateral cooperation with U.S. diplomatic and military power to change the balance of costs and risks affecting perceptions in Moscow and Beijing. That basic dynamic would be used to *deter* the most dangerous gray zone adventurism and to *dissuade* many other actions in this sphere over time. To achieve both of those objectives, the United States can take *context-setting initiatives* to shape the strategic environment. And finally, because those efforts will not prevent all gray zone activities, the United States should work with allies and partners to *enhance resilience and build tools for competitive success* against less-aggressive, more-gradual gray zone tactics, which are likely to remain persistent.

A Concept for Gaining Strategic Advantage in the Gray Zone

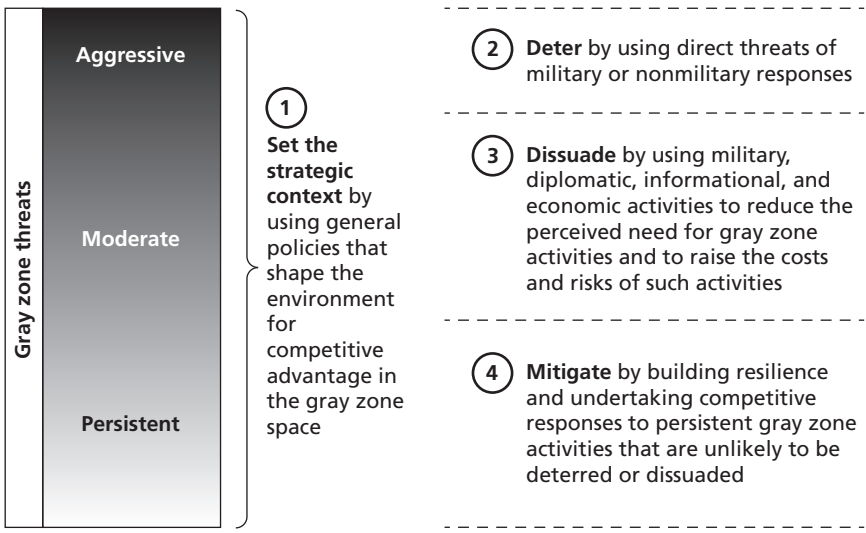
Not all gray zone activities are alike. Responses to more-aggressive gray zone activities will not necessarily mirror those of more-gradual, persistent initiatives. Any strategic concept for the gray zone therefore must distinguish among the various levels and design its responses accordingly. Admittedly, the dividing lines between levels of gray zone tactics will not be precise or well defined in all cases. Rather, they are designed to convey three general conceptual ideas rather than three clearly defined baskets. The three general levels of gray zone activities are (1) *aggressive* actions, at one end of the spectrum, that the United States should seek to deter; (2) *persistent* actions, at the opposite end of the spectrum, that it must live with but can compete against; and (3) *moderate* actions in the middle that the United States should actively seek to discourage over time. As part of this study, we offer a specific framework for distinguishing levels of gray zone actions, and these distinctions then become the basis for the response concept.

Any division of gray zone activities points to one especially critical implication and a theme that our research suggests is essential to any U.S. response strategy. The United States and its allies, partners, and friends *must decide what actions they will resolutely not tolerate* in the

gray zone environment. Because of the difficulty in stopping gradual, sometimes unattributable actions involving secondary interests, identifying the actions that the United States will seek to deter is the one reliable way to draw a boundary around the possible effects of gray zone encroachment. With this conception of a spectrum of gray zone activity levels, we outline a four-part framework for responding to gray zone threats, shown in Figure S.1.

The proposed strategic concept for the gray zone has four major components. It first calls for a whole-of-government approach utilizing geopolitical, military, and economic actions to shape the strategic context. Second, it proposes that the United States should identify a small number of aggressive gray zone tactics to deter with explicit, credible threats of military or nonmilitary responses. Third, it seeks to dissuade a wider range of moderate gray zone activities over time. Finally, it calls for mitigating persistent threats by building a capability for resilience and competitive response to threats that cannot be deterred or dissuaded.

Figure S.1
Overarching Strategic Concept for Responding to Gray Zone Threats



The remaining task for U.S. strategists is then to draw on a rich menu of specific tools, techniques, and capabilities to formulate both ongoing and event-specific responses to gray zone provocations. As part of this study, we laid out a roster of such options. In the process, we did not attempt to build a scripted playbook that specified responses to every plausible Russian or Chinese action. The reality of gray zone competition is too fluid for that, and specific contexts will demand different responses to the same action. Instead, we aimed to assemble a menu from which U.S. officials can choose in such situations, evaluating each potential response option according to three criteria: its potential advantages and benefits, its potential risks and costs, and other considerations derived from our research. In no case do we make a final evaluation of the advisability of any given option in a given situation; that will depend on the specific circumstances when each response takes place.

A multicomponent strategy like the one outlined here will be of limited utility if the U.S. government continues to lack a clear coordinating function with the responsibility for overseeing a renewed effort to gain strategy advantage in the gray zone. An important part of any gray zone response strategy, therefore, is undertaking institutional reform. A major difficulty given the current organization of key U.S. national security departments and agencies is that there is no single ideal home for a gray zone management function. The National Security Council is not an operational body, and it has a small staff devoted to coordinating policy rather than running multicomponent campaigns. The State Department has personnel and funding shortfalls and lacks interagency coordination authorities. It also often lacks an institutional mindset needed for aggressive countermeasures. Finally, placing a gray zone coordinating function solely at the Defense Department risks encouraging a dominant focus on military tools, which would not reflect the character of the challenge.

In considering alternatives for a fresh approach, we assessed two basic options. One can be described as the *thin option* and would use a presidentially directed strategy, perhaps issued in the form of a National Security Presidential Directive or other White House order, as the foundation of the approach. The order would outline the ele-

ments of a gray zone response concept and direct the actions of specific departments and agencies in support. It would then be coordinated by the National Security Council, under a senior director office devoted to the purpose.

Another alternative could be described as the *thick option*. This would assemble a more purpose-built office in the U.S. government, with a significant devoted staff, to run counter–gray zone campaigns. It could be headed by a presidential special representative with the highest subcabinet rank and a direct reporting line to the president. We looked at the National Counterterrorism Center for insights into launching a new, focused organization, although that model is designed to promote information-sharing and strategic operational planning more than the operational control of the strategy. This more elaborate option for institutional change could even include the development of regional implementation offices—the equivalent of military combatant commands—to run the gray zone campaigns in those areas (at a minimum, in Europe and Asia).

Whatever option is chosen, the U.S. government can take several accompanying steps to give the gray zone strategy the necessary profile in national security planning. These steps include the following:

- Make the issue a special focus in state and Defense Department regional offices, ensuring the necessary staff support to track evolving gray zone activities on their own terms.
- Require that responses to gray zone activities be included as a prominent theme in relevant embassy country strategies.
- Require military service initiatives to emphasize gray zone issues in, for example, career development; training and education; and the funding and support for technologies, capabilities, and experimental force design and concepts tailored to the gray zone.

Acknowledgments

We would like to thank Leigh Nolan and her team for their support of the project and intellectual guidance throughout. We also appreciate the reviewers, including Jas Osburg and Nathan Freier, whose feedback greatly improved the quality of the report. This research would not have been possible without the many individuals in Europe, Asia, and the United States who took the time to share with us their insights and made an invaluable contribution to this report. We would also like to thank Célia Belin, Simond De Galbert, Maya Kandel, Claudia Schneider, Constanze Stelzenmueller, Boris Toucas, and Paul Zajac, as well as the countless anonymous experts and government officials who facilitated these discussions.

Abbreviations

ADIZ	Air Defense Identification Zone
AfD	Alternative für Deutschland
ANSSI	French National Cybersecurity Agency
ASEAN	Association of Southeast Asian Nations
CCG	China Coast Guard
CNOOC	China National Offshore Oil Cooperation
ECS	East China Sea
EEZ	exclusive economic zone
EU	European Union
FSB	Federal Security Service
ISR	intelligence, surveillance, and reconnaissance
JASDF	Japan Air Self-Defense Force
JCG	Japan Coast Guard
JGSDF	Japan Ground Self-Defense Force
JSDF	Japan Self-Defense Forces
NATO	North Atlantic Treaty Organization
NGO	nongovernmental organization
PCA	Permanent Court of Arbitration
PLA	People's Liberation Army
PLAN	People's Liberation Army Navy
SCS	South China Sea
UNCLOS	United Nations Convention of the Law of the Sea

CHAPTER ONE

The Gray Zone Challenge

The 2017 U.S. National Security Strategy and the publicly released summary of the 2018 National Defense Strategy agree on one fundamental theme: The United States is entering a period of intensifying strategic competition with several rivals, most notably Russia and China (formally, the People's Republic of China). In the National Security Strategy, the White House argues that "China and Russia challenge American power, influence and interests, attempting to erode American security and prosperity."[1] In the public summary of the National Defense Strategy, the Defense Department argues that "Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security," and it suggests that

> The central challenge to U.S. prosperity and security is the *reemergence of long-term, strategic competition* by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions.[2]

Numerous statements from senior U.S. defense officials make clear that they expect this competition to be played out primarily below

[1] White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017, pp. 1–2.

[2] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018, pp. 1–2.

the threshold of major war. The U.S. Chairman of the Joint Chiefs of Staff, Gen. Joseph Dunford, suggested in 2016 that Russia, China, and Iran employ "economic coercion, political influence, unconventional warfare information ops, [and] cyber ops to advance their interests and they do it in a way that they know we don't have an effective response. They, unlike us, are able to integrate the full range of capabilities their states possess to advance their interests." The traditional U.S. mindset in which "we are either at peace or at war is insufficient to deal with that dynamic," because the emerging situation is primarily "an adversarial competition with a military dimension short of armed conflict."[3]

The National Security Strategy and National Defense Strategy also point to the rising importance of competition undertaken below the threshold of major war. The National Security Strategy notes that "many actors have become skilled at operating below the threshold of military conflict—challenging the United States, our allies, and our partners with hostile actions cloaked in deniability."[4] The National Defense Strategy agrees that "Both revisionist powers and rogue regimes are competing across all dimensions of power. They have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals."[5]

Many other countries have recognized the importance of below-the-threshold aggression. France's 2017 security strategy discusses the issue at some length:

> State and non-state actors now have access to a significantly wider range of tools for achieving their political goals without having to engage their military capabilities in direct confrontations.
>
> The new domains of confrontation (cyberspace and outer space) and the vastly expanded scope for action in the information

[3] Colin Clark, "CJCS Dunford Calls for Strategic Shifts; 'At Peace or at War Is Insufficient,'" *Breaking Defense*, September 21, 2016.

[4] White House, 2017, p. 3.

[5] U.S. Department of Defense, 2018, p. 4.

> field (e.g. Internet, social media, and digital propaganda) enable remote action, unconstrained by boundaries between states' "inside" and "outside" or by the usual distinction between peace, crisis, and war times. These levers are all the more attractive that they are largely unregulated by law, barely subject to control, and that attribution of actions remains a central challenge. Rather than pursuing physical assets, they target objectives directly at the heart of societies (e.g. critical infrastructures and resources), as well as their intangible dimensions (morale and political cohesion). Conventional propaganda tools deployed by way of official media and covert means of action now combine with social media trolls and groups of hackers. . . .
>
> Ambiguous postures and covert aggression are also becoming more common, with certain states making an increasing use of a wide variety of proxies, ranging from manipulated diasporas to militias and other armed groups capable of stalemating conventional forces.[6]

Similar emphasis on the gray zone appears in numerous other recent national security strategies, including those of Australia, Germany, Great Britain, and Indonesia.

There is some debate over just how serious the gray zone is for U.S. interests. Some observers have warned that it provides Russia and China with ways to undermine the health and stability of democracies in potentially dangerous ways while at the same time imposing gradual, and eventually irrecoverable, losses on the U.S. strategic position in key regions. Others are not certain that Russia and China have added to their strategic position through such activities, suggesting that both have generated significant regional reactions.

This study does not proceed from an assumption that either of these views is correct. Although our research highlights the limits of the effectiveness of gray zone strategies, these tactics clearly represent a threat to U.S. and allied interests, especially as techniques and tech-

---

[6] Republic of France, *Defence and National Security Strategic Review 2017—Key Points*, Paris, 2017a, p. 47.

nologies evolve over time.[7] Indeed, the greatest danger may be in the future, when the impulse to achieve aggressive gains short of major war is married to dramatically improved means of doing so—in such disparate areas as information warfare and swarming drone technology. This strategy begins from the claim that it is strongly in the U.S. interest to constrain the growth of gray zone conflict, even if it is not currently posing an imminent, existential threat to U.S. interests.

With this research effort, we aimed to provide a new framework for conceptualizing the gray zone challenge and offer new policy options for the United States and its allies to consider in countering the threat. We started off with an initial conception of the gray zone as the activities by quasi-revisionist states that seek to alter the status quo of the international order through coercive military or political means just below a threshold that would elicit a conventional military response.[8] Our findings revealed a much more comprehensive conception of what a gray zone has evolved to become, including military, informational, diplomatic, and economic means.

Despite the importance of this part of the spectrum of competition, it is generally agreed that the United States is ill prepared and poorly organized to compete in this space.[9] Yet our analysis suggests that the United States can begin to treat the ongoing gray zone competition as an opportunity more than a risk. Early treatments of the phenomenon worried that practitioners like Russia and China would be able to make incremental progress toward their goals without attracting

---

[7] See, for example, Defense Science Board, *Summer Study on Capabilities for Constrained Military Operations*, Washington, D.C.: U.S. Department of Defense, December 2016; International Security Advisory Board, *Report on Gray Zone Conflict*, Washington, D.C.: U.S. Department of State, January 3, 2017; and Nathan P. Freier, *Outplayed: Regaining Strategic Initiative in the Gray Zone*, Carlisle, Pa.: U.S. Army War College, Strategic Studies Institute, June 2016.

[8] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, December 2, 2015.

[9] Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, Santa Monica, Calif.: RAND Corporation, RR-1772-A, 2018.

enough attention—or concern—to spark meaningful responses. That has not turned out to be true: Much evidence, including the results of field research for this study, suggests that nations in Europe and Asia view Russian and Chinese gray zone aggression as a meaningful threat and are anxious for U.S. assistance in mitigating it.[10] By seeking to coerce, acquire influence within, or destabilize regional countries, Russia and China are opening the space for a vigorous U.S. campaign to rally allies and partners in both regions in the direction of an effective response.[11]

This report uses insights from our extensive field research in affected countries, as well as general research into the literature on the gray zone phenomenon, to sketch out the elements of a strategic response to this challenge.

Nature and Methodology of the Study

To inform such a response, we sought to (1) identify a potential strategic concept to govern a U.S. strategy in the gray zone and (2) identify and evaluate a menu of specific response options. Our intention was not to prescribe specific options for specific situations but rather to offer a menu with pro and con evaluations that could be of utility to U.S. policymakers in both establishing a general strategy and choosing responses to specific gray zone actions.

Many studies, including several earlier analyses from the RAND Corporation, have described and discussed the history of the gray zone phenomenon. We did not seek to replicate that work in this study. Although we reviewed this existing literature and we briefly summarize a definition of the gray zone phenomenon later in this chapter, the balance of this study focused on evaluating a response strategy and options.

---

[10] This is generally agreed even among sources that doubt the precision of the term *gray zone*. See, for example, Van Jackson, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflicts Before War," *Naval War College Review*, Vol. 70, No. 3, Summer 2017.

[11] William G. Pierce, Douglas G. Douds, and Michael A. Marra, "Countering Gray Zone Wars: Understanding Coercive Gradualism," *Parameters,* Vol. 45, No. 3, Autumn 2015.

In particular, we focused on Russian and Chinese gray zone activities, as well as potential U.S. and partner responses to them. Other states, most notably Iran and North Korea, are employing similar tactics, but we limited our analysis to the two leading major powers.

Our primary source of information to support this analysis was an extensive program of field research in the spring of 2018. We traveled to Australia, the Czech Republic, France, Germany, Indonesia, Japan, the Philippines, Poland, Singapore, the United Kingdom, and Vietnam to gather perspectives on the ongoing gray zone challenges in those regions. We also interviewed officials and scholars in Washington, D.C., including several from the Republic of Georgia. In addition, we met with current and former national security officials, scholars, and researchers. Our goal was to gather information about (1) the gray zone threat as these countries see it, (2) the response options that they had so far attempted to employ, (3) their experience with the success or failure of those options, and (4) their hopes for how the United States might be able to support their efforts.

In addition, we reviewed the existing literature on gray zone challenges for possible response options, and we examined the literature on deterrence for its possible lessons for the gray zone context. We relied on all of these sources of information to construct a potential strategic concept for gray zone competition and to inform our evaluation of specific response options.

Finally, two half-day tabletop exercises were held at the RAND offices in Arlington, Virginia, at the end of May and beginning of June 2018 to inform potential U.S. and allied responses to gray zone challenges posed by Russia and China. Participants in the exercises were limited to RAND employees with expertise in the subject matter and geographic scope of the issue in question.

The set of response options offered in this report is designed to be an initial draft that ought to be fleshed out and refined over time based on experience and further consultations. New ideas will emerge as the United States and its friends, allies, and partners gain more experience in this realm.

The report unfolds through several components of analysis. After an introduction and discussion of definitions in this chapter, Chap-

ter Two offers a detailed catalog of current gray zone techniques being employed by Russia and China. Chapters Three and Four then reflect the findings of the field research and survey the countries on the receiving end of these campaigns; specifically, we analyze regional surveys of gray zone challenges confronting Europe in Chapter Three and Asia in Chapter Four. In Chapter Five, we draw on the lessons of that research to outline a strategic response concept to guide U.S. strategy in the gray zone. In Chapter Six, we conclude the report by evaluating dozens of specific response options—individual policies, actions, commitments, or tools that the United States and its partners can employ to deal with specific gray zone initiatives. The goal is not to lay out a pre-programmed response for every possible gray zone action; the challenge is too diffuse and evolving for that. Instead, Chapter Six offers a menu of options that the United States can draw from in implementing the concept described in Chapter Five.

Defining the Gray Zone

To lay the groundwork for this analysis, we reassessed existing definitions and conceptions of gray zone aggression.[12] As noted earlier, the purpose of this study was not to assess the phenomenon itself but instead to develop response options. Nonetheless, it was important to reaffirm the essential nature of this challenge to set the foundation for

[12] See the analyses in, for example, Nadia Schadlow, "Peace and War: The Space Between," *War on the Rocks*, August 18, 2014; Mazarr, 2015; David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone,'" *War on the Rocks*, May 18, 2015; Frank Hoffman, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," in Dakota L. Wood, ed., *2016 Index of U.S. Military Strength*, Washington, D.C.: Heritage Foundation, 2015; Antulio J. Echevarria, "How Should We Think About 'Gray-Zone' Wars?" *Infinity Journal*, Vol. 5, No. 1, Fall 2015; U.S. Special Operations Command, *The Gray Zone*, white paper, September 9, 2015; Hal Brands, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016; Nora Bensahel, "Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex," Foreign Policy Research Institute, February 13, 2017; and Michael Green, Kathleen Hicks, Zack Cooper, John Schaus, and Jake Douglas, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Washington, D.C.: Center for Strategic and International Studies, May 9, 2017.

developing a general strategic response concept and evaluating specific response options.

One helpful definition was developed as part of the Department of Defense's joint staff effort to assess the issue in a forum called the Strategic Multilayer Assessment. This project defines the gray zone as

> a conceptual space between peace and war, occurring when actors purposefully use multiple elements of power to achieve political-security objectives with activities that are ambiguous or cloud attribution and exceed the threshold of ordinary competition, yet fall below the level of large-scale direct military conflict, and threaten US and allied interests by challenging, undermining, or violating international customs, norms, or laws.[13]

Based on that and other work, we developed a somewhat revised and compressed definition for the purposes of this study.[14] It holds that

> The gray zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events.

In both cases, and in all leading definitions of the gray zone, there are several characteristics that are most important to the nature of this challenge, as well as typical aspects that tend to be present in most gray zone activities. The first is that gray zone elements *remain below the threshold that would justify a military response*.[15] Gray zone aggressors aim to scale their actions to fall just short, or in some cases well short, of established triggers for military action, by either the United States or

---

[13] Cited in George Popp and Sarah Canna, *The Characterization and Conditions of the Gray Zone*, Boston, Mass.: NSI Inc., Winter 2016, p. 2.

[14] Our definition deals with the actions of state actors and does not consider nonstate actors that may also exhibit gray zone behaviors or tactics, such as terrorist or transnational crime networks or nongovernmental organizations (NGOs).

[15] However, as will be discussed in Chapter Five, there are certain types of gray zone activities that we suggest would cross clear thresholds of military aggression or use of force.

the target of the gray zone coercion. The goal is to avoid major clashes, unambiguous or attributable violations of international law or norms, or outright conflict.[16]

This characteristic can guide the choice of specific actions—such as unattributable cyber harassment or creating a de facto presence in a maritime area—but it can also help shape the character of a gray zone campaign over time. Often, an aggressor will follow a series of more-belligerent actions with a period of calm, designed to ease regional concerns about its activities. Both in their specific actions and in their overall structure, therefore, gray zone campaigns are designed to deny a defender precisely the sort of clarity in violation of rules that is typically important in effectuating a deterrent threat.

The second common characteristic of gray zone activities is that they *unfold gradually over time rather than involving bold, all-encompassing actions to achieve objectives in one step.* By stretching aggressive moves over years or even decades, such "salami tactics" provide less basis for decisive responses—and thus less ability to make unambiguous deterrent threats in advance.[17]

A third characteristic of the gray zone, which applies to some but not all the activities in this sphere, is a *lack of attributability*. Most gray zone campaigns involve actions in which the aggressor aims to disguise its role at least to some degree. Whether using cyberattacks, disinformation campaigns, or proxy forces, these actions allow a gray zone aggressor to deflect responses—and obstruct the potential for successful deterrence—by simply denying that it is responsible.

Some actions in the gray zone are open and attributable. In those cases, they tend to be characterized by a fourth common aspect: *the use*

---

[16] On China's strategy in this regard, see Amy Chang, Ben FitzGerald, and Van Jackson, *Shades of Gray: Technology, Strategic Competition, and Stability in Maritime Asia*, Washington, D.C.: Center for a New American Security, March 2015; and Christopher Yung and Patrick McNulty, *China's Tailored Coercion and Its Rivals' Actions and Responses: What the Numbers Tell Us*, Washington, D.C.: Center for a New American Security, January 2015.

[17] Russian actions in Ukraine have stretched this definitional aspect to its breaking point, essentially crossing the threshold into conventional war. See, for example, András Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, Helsinki: Finnish Institute of International Affairs, Report 43, June 16, 2015.

of extensive legal and political justifications, often grounded in historical claims supported with documentation. Nations undertaking gray zone campaigns make strong efforts to justify their actions under international law. In some cases, as with a handful of specific Chinese legal claims in the South China Sea (SCS), they recruit other countries to their point of view, even if the legal standing of their claims in the international community is tenuous. These tactics complicate the task of generating a local response, as well as enforcing punishments.

Fifth, to avoid decisive responses, gray zone campaigns typically *stop short of threatening the defender's vital or existential interests*. This aspect naturally follows from an approach that remains below thresholds for response, but it deserves special emphasis. By declining to challenge vital interests on the part of the defender—especially a defender practicing extended deterrence, as in the case of the United States today—gray zone aggressors significantly complicate the challenge of effective deterrence and response.

An important quality of gray zone campaigns, therefore, is that they reflect a long series of limited faits accomplis.[18] They represent physical areas or issues with some vacuum of power that Russia or China can fill, daring the United States, its allies, and its partners to respond. This can be true in territorial terms, as when China sends fishing vessels to international waters of the SCS to claim "historical fishing rights," or in normative terms, as when Russia exploits loopholes in the definition of aggression to harass Western democracies through cyberattacks or disinformation. Gray zone aggressors find places where defenders cannot respond quickly or aggressively and stake out positions from which they must be removed, transferring the risk calculus to the defender.

Gray zone activities, in other words, involve an ongoing effort to discover weaknesses in existing U.S. and allied policies and capabilities

---

[18] On the specific aspect of such faits accomplis, see Ahmer Tarar, "A Strategic Logic of the Military Fait Accompli," *International Studies Quarterly,* Vol. 60, No. 4, December 2016; Daniel Altman, "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries," *International Studies Quarterly*, Vol. 61, No. 4, December 1, 2017; and Daniel Altman, *Red Lines and Faits Accomplis in Interstate Coercion and Crisis*, dissertation, Boston, Mass.: Massachusetts Institute of Technology, 2015.

and exploit them for strategic advantage. Any response strategy must come to grips with this essentially opportunistic, gap-seeking character of the gray zone. It points to the need for both continuous dissuasion in areas and issues of high priority and the ability to move quickly once challenges appear. Waiting a week or more to respond to an adversary's actions may allow the gray zone aggressor to achieve an initial advantage that becomes very difficult to dislodge.

A sixth characteristic of gray zone aggression is that, even as it seeks to remain below key thresholds for response, it *uses the risk of escalation as a source of coercive leverage*. Gray zone campaigns are designed to remain below the threshold for large-scale military response—but they also, and somewhat paradoxically, often explicitly hint at the risk of more-violent military actions that provide escalation leverage and complicate deterrent threats. Targets of the gray zone aggression know that if they respond powerfully to a relatively modest gray zone move, the gray zone aggressor can double-down with more-significant capabilities, including military force. China uses such escalatory risks, in part, by deploying maritime militia and coast guard vessels at the point of dispute, with its "gray hull" People's Liberation Army (PLA) Navy (PLAN) assets just over the horizon.[19] Such actions provide a form of intimidation that is central to effective gray zone campaigns.

Seventh, gray zone campaigns are *typically built around nonmilitary tools, as part of the general approach of remaining below key thresholds for response*. They employ diplomatic, informational, cyber, quasi-military forces, militias, and other tools and techniques to avoid the impression of outright military aggression. To respond adequately, defenders must develop parallel tools of statecraft to threaten or carry out deterrent threats.

Eighth and finally, gray zone campaigns *target specific vulnerabilities in the targeted countries*. These can include political polarization; social cleavages, including the existence of ethnic populations sympathetic to the gray zone aggressor; economic stagnation and resulting needs and grievances; and lack of military or paramilitary capabilities.

---

[19] *Gray hull* is a term used for regular navy forces, as opposed to *white hull* (coast guard vessels).

Gray zone aggressors also typically aim to put the defenders in situations where strong responses appear ruled out, or counterproductive, for strategic and domestic political reasons. The aggressors can do this, in part, by establishing economic dependencies that create implicit leverage or by threatening escalation.

Perhaps the cardinal overarching characteristic of the gray zone, therefore, is that it *takes advantage of strategic ambiguity to achieve gradual gains*. In theory, simply removing this ambiguity—declaring a U.S. and allied intent to respond strongly to a full range of activities—can be part of the solution. And indeed, a major theme of the strategic concept defined in this report is to do exactly this: The first step in responding to gray zone aggression is to draw clearer lines where aggression will cross thresholds, thus bounding the problem. But this is likely to be possible with only a small subset of gray zone tactics. The essential insight of gray zone strategies is that an aggressive state can take many actions below the threshold at which a defender will feel able to make such unambiguous promises of response.

The challenge of responding to such gradual aggression is complicated by the fact that allies and partners tend to have different risk appetites and preferences. In Europe, many countries believe that it is important to sustain workable relations with Russia; in Asia, many countries feel caught in between Chinese economic predominance and their concerns about Beijing's coercive moves, so they hesitate to take a clear stand. Even if the United States can recruit one or more regional partners in a more aggressive gray zone response, Moscow and Beijing will try to peel off other countries more worried about a tougher stance.

Finally, in developing a response strategy, we also kept firmly in mind the fact that gray zone campaigns are part of an unfolding global competition, as defined by current U.S. national security strategy documents—and those of the United States' adversaries. The purpose and effect of responses must be viewed in that context. Actions taken in one gray zone context may set expectations for other issues or regions or may contribute to an emerging sense of the trajectory of the overall competition.

CHAPTER TWO

The Character of the Gray Zone Challenge from China and Russia

The United States still enjoys superior conventional military capability against most potential adversaries in most contingencies. As a result of this military overmatch, Russia and China, which are near-peer competitors, have increasingly turned to tactics that undermine U.S. interests but that do so just below a threshold that might prompt a conventional U.S. or allied military response. By relying largely on paramilitary capabilities and political subversion campaigns that undermine sovereign governments, these two competitors confront the United States and its allies with a unique set of security challenges. Although some of the strategies exhibited by these two countries against the U.S. and its allies—such as psychological warfare, disinformation campaigns, and covert paramilitary activities—are not new phenomena in international conflict and competition, we found that tactics employed by Russia and China have grown much more sophisticated, enabled by enhanced technological innovations and platforms.[1]

Russia perceives itself to be in a long-term political, economic, and social competition with the United States and seeks to use primarily nonmilitary tools for both long-term competitive advantage and

[1] On historical examples of such military tactics, see Martin Van Creveld, *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*, New York: Free Press, March 31, 1991; Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century,* St. Paul, Minn.: Zenith Press, February 17, 2006; and Williamson Murray and Peter R. Mansoor, eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, New York: Cambridge University Press, July 9, 2012.

short-term coercive effect.[2] These tools include employing information and cyber warfare, blackmailing and manipulating political leaders or journalists hostile to the aggressor, and funding proxy groups and political organizations hostile to Western institutions. China appears to calculate that, by relying on maritime law enforcement and a maritime militia, in concert with the PLAN, Beijing can systematically coerce regional actors from utilizing their legitimate resources in their exclusive economic zone (EEZ) waters while minimizing the risk of military escalation. By using such tools, China has greatly improved its position and administrative control over much of the disputed territory in the East China Sea (ECS) and SCS and has done so seemingly at minimal material or diplomatic cost.[3]

In this chapter, we seek to provide a broad overview of the types of gray zone challenges posed by these two competitors. In Chapter Three, we highlight the details of these challenges and focus on the results of field research in the different regions.

Russia

In this section, we examine the different types of gray zone actions that the Russian Federation (hereafter, "Russia") has employed in recent years, under the leadership of Vladimir Putin, to influence and coerce foreign states.[4] While the focus here is on Russia's use of gray zone mea-

---

[2] Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1498-A, 2017.

[3] Note that this report focuses primarily on Chinese gray zone tactics in its near abroad, meaning East and Southeast Asia, and does not cover other regions where China may be exerting gray zone behavior to advance its interests. On Chinese improvements to consolidating its territorial claims in Asia, see Ely Ratner, "Course Correction: How to Stop China's Maritime Advance," *Foreign Policy*, July/August 2017.

[4] The choice to focus on Putin stems from a recognition that, under his leadership—whether as president or prime minister—Russia's foreign policy has taken a more aggressive and revisionist turn, illustrated most dramatically by Russia's wars in Georgia in 2008 and Ukraine since 2014. Polyakova and colleagues also note a wider use of gray zone measures since Putin became president again in 2012 (Alina Polyakova, Marlene Laruelle, Stefan

sures in Europe (to include the Caucasus), this use also extends beyond that region. Russia has long employed gray zone measures in Central Asia, for instance, and evidence of more-recent interference in the United States is beginning to emerge. Gray zone measures are not a recent phenomenon, either. They were employed long before Putin came to power and date back to the Soviet era and even the tsarist regime.[5]

Russian gray zone measures generally fall into three categories:

1. influencing a specific outcome, such as an election or a dispute between Russia and the targeted state
2. shaping the environment, which consists of creating conditions in a country for a national policy more favorable to Russia's interests[6]
3. punishing a state for taking actions that Russia perceives as offensive or contrary to its national interests; the idea is that such punishment should not only convey Russia's displeasure but also, and more importantly, convince the targeted country's leaders that such behaviors are not to be repeated.

Modern Russian gray zone actions bear a distinct resemblance to those used during the Cold War by the Soviet Union. For instance, military intimidation, covert operations, and the stirring of political

---

Meister, and Neil Barnett, *The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom*, 3rd ed., Washington, D.C.: Atlantic Council, November 2016, p. 3).

[5] For instance, Russia suspended its gas supplies to Estonia in 1993 in retaliation for the passing of a new law perceived by Russia as detrimental to Estonia's Russian minority (Celestine Bohlen, "Russia Cuts Gas Supply to Estonia in Protest," *New York Times*, June 26, 1993). See also Mark Galeotti, "Russia's Hybrid War as a Byproduct of a Hybrid State," *War on the Rocks*, December 6, 2016. On Soviet "active measures" against the United States and the North Atlantic Treaty Organization (NATO) during the Cold War, see Ashley Deeks, Sabrina McCubbin, and Cody M. Poplin, "Addressing Russian Influence: What Can We Learn from U.S. Cold War Counter-Propaganda Efforts?" Lawfare, October 25, 2017.

[6] To some extent, shaping the environment is similar to influencing outcomes but with a longer time horizon. Funding a far-right political party, for instance, would be shaping the environment, while launching an information campaign aimed at discrediting a specific political party on the eve of an election would be influencing a specific outcome.

dissent are but a few of the gray zone categories that have remained very similar over time.[7] New means of influence and targets have appeared in recent years, however. Most prominently, the cyber domain has become a tool that can facilitate, or amplify the effect of, other measures. For instance, Russia may seek to influence a targeted country's political process, as witnessed with the hacking of personal documents from the political campaign of French presidential candidate Emmanuel Macron and the subsequent public release in the days preceding the May 2017 French election.[8] Affecting a country's cyber platforms can also be an objective in itself, such as when gray zone actors use denial-of-service attacks to incapacitate a state or degrade its cyber capabilities. In the information domain, social media represents a new platform that creates opportunities for targeting large numbers of individuals and attempting to influence their perceptions and political decisions.

The modality of Russian gray zone measures is also multifaceted. When used to punish, gray zone actions do not necessarily correlate with the actions that prompted them. For instance, cyberattacks were used to coerce Estonia's leaders into changing their decision on the relocation of a statue in 2007, and economic sanctions were imposed against Turkey after a Russian military plane was shot down by Turkish armed forces in September 2015. Regardless of the specific purpose they serve, gray zone measures can be used in a variety of patterns and over an undetermined period.

In the remainder of this section, we lay out a typology of gray zone measures, broken down along military measures, information operations, cyberattacks, legal and diplomatic measures, economic coercion, and political influence. We also examine what makes countries in the region more or less vulnerable to gray zone measures, and we provide

---

[7] Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections*, Vol. 15, No. 1, Winter 2016.

[8] Rick Noack, "Cyberattack on French Presidential Front-Runner Bears Russian 'Fingerprints,' Research Group Says," *Washington Post*, April 25, 2017a.

some observations regarding the past effectiveness of these measures in helping Russia achieve its foreign policy and security aims.[9]

Types of Russian Gray Zone Measures in Europe

Military Measures

Although gray zone measures, by definition, stop short of war, they may still involve military personnel, equipment, or posturing, either in Russia or abroad. Generally speaking, Russia's military measures fall into two broad categories: war by proxy and military intimidation.

War by proxy refers to the provision of personnel, equipment, or other enablers to proxy forces militarily active in the targeted country. This would include, for instance, Russia's transfer of military equipment to separatists in Abkhazia and South Ossetia before the 2008 war in Georgia.[10] War by proxy also includes sending military personnel to fight without identifying insignia (the "little green men" seen in Ukraine).

Military intimidation is the use of military assets to convey the threat of a potential military attack or a risk of military escalation. This tactic can be carried out in several ways, including massing troops at a border, as Russia did in April 2014 to threaten Ukraine of a full-scale invasion while pushing for the annexation of Crimea;[11] conducting large-scale exercises to ostensibly prepare for a contingency in a targeted country, such as Russia's July 2008 exercise near the border with Georgia;[12] violating a targeted country's airspace, often with transponders turned off to prevent contact with the air authorities of the targeted country; and establishing a military presence in a contested area, as Russia has done, for instance, in Transnistria in spite of

---

[9] This paper offers an overview of past and current use of gray zone measures by Russia in Europe. The categories listed here do not purport to be exhaustive, and examples aim to provide only illustrations of these different measures.

[10] Luke Harding, "WikiLeaks Cables Claim Russia Armed Georgian Separatists," *The Guardian*, December 1, 2016.

[11] Kofman et al., 2017, p. 24.

[12] Angela Stent, *The Limits of Partnership: U.S.-Russian Relations in the Twenty-First Century*, Princeton, N.J.: Princeton University Press, 2014, pp. 169–170.

repeated calls from Moldovan authorities to terminate this presence and in spite of Russia's own commitment at the 1999 Istanbul Summit of the Organization for Security and Co-operation in Europe to withdraw by 2002.[13]

Information Operations

Information operations consist of "the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent."[14] While not new, this practice has evolved to incorporate new technologies and new platforms. It has also changed in fundamental ways to resemble now what some analysts call a "firehose of falsehood," characterized by a high number of dissemination channels and the propagation of known falsehoods in a rapid and continuous manner.[15]

Information operations serve various purposes, including the following:

- *Diffusing and amplifying messages that echo Russia's official policy or views.* Russia promotes its message using different platforms, characterized by the widespread diffusion of Moscow-controlled news outlets, such as RT and Sputnik, often broadcasting in the local language. These practices can manipulate online polls.[16]
- *Attacking alternative messages.* Russia has used information operations to attack, or undermine, various individuals or institutions perceived as negatively affecting Russian interests—for instance, by propagating news articles of a clear anti–European Union (EU) or anti-NATO nature.

---

[13] Organization for Security and Co-operation in Europe, *Istanbul Document 1999*, Istanbul, January 2000, p. 50; and International Crisis Group, "Moldova's Uncertain Future," *Europe Report*, No. 175, August 17, 2006, p. 11.

[14] RAND Corporation, "Information Operations," webpage, undated.

[15] Chris Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016, p. 1.

[16] Daniel Victor, "Why You Shouldn't Trust 'Polls' Conducted Online," *New York Times*, September 28, 2016.

- *Shaping public opinion to destabilize targeted states, influence local political outcomes, or both.* Russia seeks to shape the discussion on social media by placing political ads on various platforms and promoting selected news stories, often through fake accounts. In an October 2017 hearing before a U.S. Senate judiciary subcommittee, lawyers for Twitter revealed that 1.4 million tweets had originated from Russian bots during the 2016 presidential election.[17] These efforts have included, in particular, the promotion of controversial stories that stoke political and social divisions in targeted countries.[18]

Cyberattacks

This category refers to the use of cyber intrusions as a tool to disrupt the operations of the targeted state—for instance, through denial of service or attacks against critical infrastructure. In December 2015, more than 200,000 Ukrainians found themselves without power following a coordinated cyberattack against several energy providers.[19] Defacement of websites is another type of attack that prohibits users from viewing or operating certain websites or forces users to view propaganda. Cyber campaigns target different types of actors, as happened in Estonia in 2007 when several banks, newspapers, and government agencies found themselves simultaneously under attack.[20] Attribution of the attackers' origin is often obscured. There is still no evidence, for instance, that the Russian government played a role in the 2007 attacks

---

[17] Hamza Shaban, Craig Timberg, and Elizabeth Dwoskin, "Facebook, Google and Twitter Testified on Capitol Hill. Here's What They Said," *Washington Post*, October 31, 2017.

[18] Cortney Weinbaum, "Covert Influence Is the New Money Laundering," *TechCrunch*, November 5, 2017; and Donie O'Sullivan and Dylan Byers, "Exclusive: Fake Black Activist Accounts Linked to Russian Government," CNN, September 28, 2017.

[19] Another successful cyberattack against the Ukrainian power grid took place in December 2016 (see, for instance, Pavel Polityuk, Oleg Vukmanovic, and Stephen Jewkes, "Ukraine's Power Outage Was a Cyber Attack: Ukrenergo," Reuters, January 18, 2017.

[20] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

against Estonia, although forensics strongly suggest that the Russian government was culpable.[21]

Legal and Diplomatic Measures

Russia has pursued a *passportization* policy since the early 1990s by granting Russian passports to ethnic Russians, Russian speakers, and other minorities residing in other states, even if dual citizenship is prohibited in the state where these individuals reside.[22] Although, in most cases, individuals accepting these passports do so voluntarily—for instance, to get benefits that would not be available to non-Russians, such as social security or pensions—some citizens can be coerced, as when ethnic Georgians in Abkhazia and South Ossetia were given a choice between taking the Russian citizenship or being expelled from their homes following the 2008 conflict with Russia.[23]

Passportization has been a particularly prevalent tool in the post–Soviet Union era. After the fall of the Soviet Union, the Russian government sought to provide citizenship to ethnic Russians who found themselves outside of Russia's boundaries and who did not want to adopt the citizenship of their new country of residence. Russian-speaking minorities in Estonia and Latvia, for instance, largely found themselves in that situation.[24] Russia has used this practice in contested areas, such as South Ossetia, Abkhazia, and Transnistria, as well. More than one-third of the population of Transnistria holds a Russian pass-

---

[21] Martin C. Libicki, "It Takes More Than Offensive Capability to Have an Effective Cyber-deterrence Posture," testimony before the House Committee on Armed Services, Washington, D.C., March 1, 2017. It is notable that Russia's preferred response to Western reports of Russian government involvement in most disinformation campaigns is to deny and make counter-accusations against Western governments. See Luke Harding, "'Deny, Distract and Blame': How Russia Fights Propaganda War," *The Guardian*, May 3, 2018.

[22] Agnia Grigas, *Beyond Crimea: The New Russian Empire*, New Haven, Conn.: Yale University Press, 2016, p. 41.

[23] Max Planck Institute, *Independent International Fact-Finding Mission on the Conflict in Georgia: Report*, Vol. I, Heidelberg, Germany, September 2009, p. 29; and Damien McElroy, "South Ossetian Police Tells Georgians to Take a Russian Passport, or Leave Their Homes," *The Telegraph*, August 30, 2008.

[24] Grigas, 2016, p. 41.

port.[25] This practice not only undermines the sovereignty of the state in which these new Russian citizens live but also creates a risk that Russia will justify a potential military intervention on the grounds that it needs to protect its citizens. Russia's passportization policy was particularly active in Crimea prior to 2014.[26]

Economic Coercion

Economic coercion, in the broadest sense, refers to the disruption or threat of disruption of relations between Russia and the targeted country through unilateral economic actions. Russia's actions may affect trade, labor, investment flows, transportation, or energy. More specifically, in the past, Russia has initiated the following economic actions against regional states:

- *Imposing restrictions on trade and investment by sanctioning or banning specific imports to Russia*. In some cases, the measures are punitive, as when Russia banned the import of several Turkish agricultural products a few days after Turkish authorities downed a Russian military plane.[27] In other cases, Russia has issued hidden sanctions—for instance, when it banned wine from Georgia (2006) and Moldova (2006 and 2013) under the pretext that the products did not pass quality or hygiene tests.[28] In both cases, the measures coincided with disputes between Russia and these countries regarding their pro-EU orientation.
- *Imposing physical or legal barriers on the circulation of persons, such as limiting or prohibiting the use of foreign labor and increasing visa requirements for workers or tourists in Russia*. These measures can

[25] Karina Lungu, "Transnistria: From Entropy to Exodus," European Council on Foreign Relations, September 1, 2016.

[26] Grigas, 2016, p. 43.

[27] Jack Stubbs and Alexander Winning, "Russia Approves Detailed Sanctions Against Turkey over Downed Plane," Reuters, December 1, 2015.

[28] Kieran Cooke, "Georgia's Wine Frozen Out by Russia," BBC, November 30, 2006; T. J. Chisinau, "Why Has Russia Banned Moldovan Wine?" *The Economist*, November 25, 2013; and C. J. Chivers, "A Russian 'Wine Blockade' Against Georgia and Moldova," *New York Times*, April 6, 2006b.

be particularly painful for countries, such as Moldova, that rely heavily on remittances sent by their nationals employed in Russia back to their home country.[29]

- *Disrupting communication, including transportation lines, phone lines, cell phone services, and postal services*. During its 2006 "spy row"[30] with Georgia, for instance, Russia cut postal and transport lines between the two countries.[31]
- *Disrupting energy markets by manipulating energy prices (including by reconsidering preferential tariffs) and disrupting energy supplies*. Notably, Russia cut gas supplies to Ukraine in 2006, 2008–2009, and 2014 over price disputes.[32] Figure 2.1 lays out Russian energy supplies to Europe.

Political Influence

Political influence measures aim to provide Russia with some degree of control over the political process and outcomes of foreign states. They may target individuals, organizations, or communities, sometimes resorting to violence. Some key Russian activities in this domain include the following:

- *Manipulating population groups*. Russia has a track record of stoking tensions between population groups in an attempt to divide and destabilize, and these activities can target either minority groups (for instance, Russian-speaking minorities in Estonia and Latvia; Serbs in Kosovo and Bosnia) or majority groups (for instance, by promoting anti-immigrant speech and movements in Western European societies).[33]

---

[29] Eugene Rumer, "Moldova Between Russia and the West: A Delicate Balance," Carnegie Endowment for International Peace, May 23, 2017.

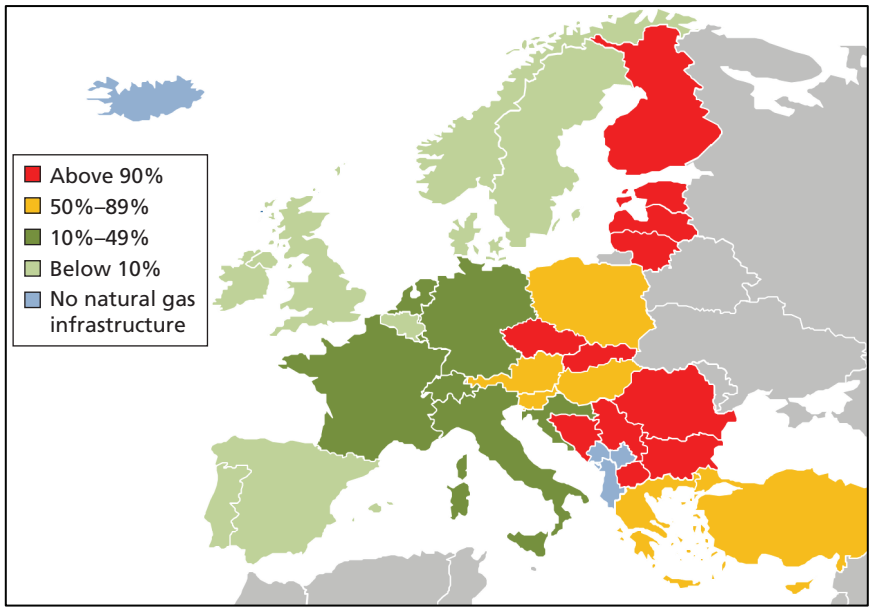
[30] The *spy row* refers to a dispute between Russia and Georgia related to Georgia's arrest of four suspected Russian spies in Tbilisi in September 2006.

[31] Cooke, 2006.

[32] Paul Kirby, "Russia's Gas Fight with Ukraine," BBC News, October 31, 2014.

[33] An example of the latter is the fake story, widely reported in Germany, of the rape of a 13-year old Russian-German girl by Arab migrants (the "Lisa case"), and this case illustrates how disinformation, largely relayed by Russian media, is used to amplify divisions within

Figure 2.1
Russian Supplies as a Percentage of Total Gas Imports in Europe



SOURCE: F. Stephen Larrabee, Stephanie Pezard, Andrew Radin, Nathan Chandler, Keith Crane, and Thomas S. Szayna, *Russia and the West After the Ukrainian Crisis: European Vulnerabilities to Russian Pressures*, Santa Monica, Calif.: RAND Corporation, RR-1305-A, 2017, p. 35.

- *Supporting or funding individuals and political parties*. For example, the French National Front party received an $11.7 million loan from a Russian bank in September 2014.[34] Although this is one of a very few cases in which a direct financial link is documented, Russia has more generally supported anti-EU parties,

Western societies over polarizing political and societal issues. See Adam Taylor, "An Alleged Rape Sparked Tensions Between Russia and Germany. Now Police Say It Was Fabricated," *Washington Post*, January 29, 2016; and Stefan Meister, "The 'Lisa Case': Germany as a Target of Russian Disinformation," *NATO Review Magazine*, undated.

[34] Laura Motet, "Visites, Financements: Le Front National et la Russie, une Idylle Qui Dure," *Le Monde*, November 18, 2016; and Suzanne Daley and Maïa de la Baume, "French Far Right Gets Helping Hand with Russian Loan," *New York Times*, December 1, 2014.

mostly on the far right but also on the far left.[35] Russia has also exploited the weak institutions and high corruption levels present in some countries to gain leverage over politicians and business leaders and to influence the political debate.[36]

- *Inciting political action through violent or nonviolent street action*. Russia has initiated several covert campaigns to foment anti-government sentiments against states whose ruling party Russia perceives as anti-Russian. For such events, attribution of direct Russian influence is difficult to ascertain. However, demonstrations like those that took place in Tallinn, Estonia, to protest the removal of the statue of a Soviet soldier in April and May 2007 were generally assumed to have been supported by Moscow. A more direct link was established in the case of Russian paramilitary training with the neo-Nazi National Front movement in Hungary.[37]
- *Using covert direct action, including assassinating political opponents to Putin abroad*. For instance, Alexander V. Litvinenko was assassinated in London in 2006, and Denis M. Voronenkov, a former member of the Russian Parliament, was assassinated in Ukraine in March 2017.[38] The October 2016 attempted coup in Montenegro, reportedly to assassinate Montenegrin Prime Minister Milo Djukanovic and replace him with a pro-Russian figure before the country could join NATO, is another example. Serbia allegedly

[35] See Larrabee et al., 2017, pp. 54–60.

[36] Polyakova et al., 2016, p. 4.

[37] Andrew Byrne, "Shootout Raises Fear over Russian Ties to Hungary's Far Right," *Financial Times*, November 27, 2016.

[38] According to journalist Andrew E. Kramer,

> Used extensively in the Soviet era, political murders are again playing a prominent role in the in the Kremlin's foreign policy, the most brutal instrument in an expanding repertoire of intimidation tactics intended to silence or otherwise intimidate critics at home and abroad (Andrew E. Kramer, "More of Kremlin's Opponents Are Ending Up Dead," *New York Times*, August 20, 2006).

deported two Russian nationals suspected of involvement in the attempted coup, while the Kremlin denied any responsibility.[39]

To be successful, gray zone measures must be well tailored to the countries they target. They require knowledge of the society, political debate, information landscape, and economic and financial forces at play within a given country. Russia takes advantage of these vulnerabilities along four main lines:

- *Energy dependence.* Several countries in northern, central, and southeastern Europe rely on Russia for a large share of their gas consumption (see Figure 2.1). The countries that rely on gas for a large part of their energy consumption are vulnerable to abrupt changes in prices for gas from Russia. Russia also uses the debt accumulated by some countries (for instance, Moldova[40]) as a source of leverage to extract various benefits, such as an expanded Russian role in those countries' key national industries.
- *Strength of institutions.* Measures or indicators of institutional strength include accountability, the rule of law, corruption levels, and the presence of strong cyber infrastructure and defenses. Weak institutions are much easier to infiltrate, and a corrupt bureaucracy offers countless points of entry for Russian influence.
- *Societal division.* Russia's efforts at stoking tensions between population groups are most effective in countries whose national unity is tenuous, such as Bosnia and Herzegovina. Yet countries that are largely homogenous, such as Kosovo, can still experience Russian efforts to stir discord among the minority populations that live there (such as the Serbs in Kosovo).[41]
- *Economic dependency.* The difficulty of finding alternative export markets on short notice and the cost of switching import sources

[39] Editorial Board, "Beware: The Russian Bear Is Getting Bolder," *Washington Post*, December 1, 2016; and Julian Borger, Andrew MacDowall, and Shaun Walker, "Serbia Deports Russians Suspected of Plotting Montenegro Coup," *The Guardian*, November 11, 2016.

[40] Rumer, 2017.

[41] See Marta Szpala, "Russia in Serbia—Soft Power and Hard Interests," Warsaw: Center for Eastern Studies, Commentary No. 150, October 27, 2014.

create vulnerabilities for countries that have extensive trade relations with Russia. Countries with large numbers of migrant workers in Russia are also vulnerable to changes in Russia's visa regulations.

To be sure, when a country has extensive financial, trade, and energy relations with Russia, there is a cost for Russia to disrupt or even sever these relations. This can act as a deterrent if Russia is in a position of economic or financial fragility. There are also long-term costs for Russia. Threatening a disruption of gas supplies, for instance, might motivate the targeted country to seek a diversification of its energy resources—even at a higher cost for that country—in order to reduce its vulnerability. Russia, then, would lose not just immediate revenue but also long-term revenue as one of its clients shifts to other suppliers. The same rationale applies to nonenergy products. When Russia banned imports of Moldovan wine, for example, depriving Moldova of its biggest market for a product critical to its economy, Moldova turned to a U.S. program to modernize its wine industry and target Western markets instead,[42] reducing its reliance on the Russian market.

Conclusion

Russia's gray zone measures have shown varying degrees of effectiveness but, taken in totality, present a unique challenge to countries vulnerable to Russian influence in the region. Russia's use of proxy groups, information operations, cyberattacks, economic coercion, and military intimidation have succeeded in sowing discord and division within many countries in Eastern and Western Europe while escaping some of the negative consequences of participating in an open conflict or political, economic, or military retaliation against Russian territory. Information operations—particularly the spreading of fake news and forgeries—present the two benefits of being often cheap and having a low threshold for success. Commenting on the factual inaccuracies and spelling mistakes found in forged documents that appeared in Sweden in 2015–2016, scholars note that poor quality was also a common fea-

[42] Mark Baker, "Drinking Games," *Foreign Policy*, July 29, 2015.

ture of Soviet forgeries during the Cold War era, yet it did not prevent large audiences from treating them as genuine and from disseminating them further.[43] The effect of disinformation campaigns can also be remarkably long-lasting, as the original source (even when it is known to be Russia) progressively fades and the erroneous information becomes general knowledge on a given topic.[44] By sowing doubt about the legitimacy of democratic institutions, Russia's efforts have achieved some level of success in undermining the democratic and liberal values within nations in the region.

China

Over the past decade, maritime actors have begun employing Chinese gray zone actions in East and Southeast Asia. In this section, we provide an overview of the types and drivers of these gray zone measures in the region, broken down along seven categories: military intimidation, paramilitary activities, co-opting of state-affiliated businesses, manipulation of borders, information operations, lawfare and diplomacy, and economic coercion. We then conclude with observations on the stakes of the gray zone challenge from China for the United States, its allies, and its partners.

While China employs a broad array of gray zone actions against countries in East and Southeast Asia, China's unique brand of gray zone measures involves the use of civilian tools (e.g., fishing vessels), paramilitary tools (e.g., a *maritime militia*, or a group of civilian fishermen who receive military training and coordinate their actions under state and military guidance), and government vessels (e.g., coast guards) to assert

---

[43] Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies*, Vol. 40, No. 6, 2017, p. 807.

[44] One oft-cited example of a particularly resilient forgery is the antisemitic "Protocols of the Elders of Zion." Originally published in 1903, it was exposed as a forgery by the *London Times* in 1921. Yet, it is still widely in circulation today and is presented as historical fact in the school textbooks of several countries. See U.S. Holocaust Memorial Museum, "Protocols of the Elders of Zion," Holocaust Encyclopedia, undated.

administrative control over disputed island features and the maritime zones that those features create. China's employment of nonmilitary capabilities in its maritime territorial disputes with Japan in the ECS and with several countries, including Vietnam and the Philippines, in the SCS have increased over the past few years.[45] For example, China has employed maritime law enforcement vessels to assert its claims to the disputed Senkaku Islands, which are administered by Japan but claimed by China and Taiwan (formally, the Republic of China). Beijing has also consolidated administrative control within its "Nine-Dash Line" in the SCS using maritime law enforcement assets and, more recently, a maritime militia to harass and coerce rival claimants in Southeast Asia.[46] Chinese fishermen and maritime militiamen have become increasingly brazen in challenging attempts by coast guard forces in East and Southeast Asia to assert jurisdiction in their territorial waters or EEZs—is some cases, leading to deaths at sea.[47]

The areas where China has focused its maritime gray actions in the SCS are outlined in Figure 2.2. These include the Senkaku Islands, which are claimed by China, Taiwan, and Japan; the Pratas Islands, claimed by China and Taiwan; the Paracel Islands, claimed by China, Taiwan, and Vietnam; the Macclesfield Bank, claimed by China, Taiwan, and the Philippines; the Scarborough Shoal, claimed by China, Taiwan, and the Philippines; and the Spratly Islands, claimed by China, Taiwan, the Philippines, Vietnam, Malaysia, and Brunei.

---

[45] Lyle J. Morris, "Blunt Defenders of Sovereignty: The Rise of Coast Guards in East and Southeast Asia," *Naval War College Review*, Vol. 70, No. 2, Spring 2017c.

[46] For detailed background on these forces, see Conor M. Kennedy and Andrew S. Erickson, *China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA*, Newport, R.I.: U.S. Naval War College, China Maritime Studies Institute, China Maritime Report No. 1, March 2017; Andrew S. Erickson and Conor M. Kennedy, "Trailblazers in Warfighting: The Maritime Militia of Danzhou," Center for International Maritime Security, February 1, 2016; Andrew S. Erickson and Conor M. Kennedy, "Irregular Forces at Sea: Not 'Merely Fishermen'—Shedding Light on China's Maritime Militia," Center for International Maritime Security, November 2, 2015; and Christopher P. Cavas, "China's 'Little Blue Men' Take Navy's Place in Disputes," *Defense News*, November 2, 2015.

[47] Paula Hancocks, "S. Korea: Chinese Fisherman Kill Coast Guard Member," CNN, December 12, 2011; and Malcom Moore, "Mackerel War Between China and South Korea Sees Fisherman Shot Dead," *The Telegraph*, October 10, 2014.

Figure 2.2
Areas of Gray Zone Competition Between China and Regional States

SOURCE: Lori Fisler Damrosch and Bernard H. Oxman, "Agora: The South China Sea," *American Journal of International Law*, Vol. 107, No. 1, January 2013, p. 96. Used with permission.
NOTE: CLCS = Commission on the Limits of the Continental Shelf; nm = nautical mile.

China appears to calculate that relying on maritime law enforcement vessels, a maritime militia, and other nonmilitary capabilities, while keeping PLAN surface ships largely in the background, will enable it to achieve its sovereignty goals over these maritime features while minimizing the risk of further escalation. It has arguably been successful in this strategy.[48] China has greatly improved its position and administrative control over much of the disputed territory in the ECS and SCS and has done so at minimal material or diplomatic cost. China has also been successful at "civilianizing" the optics of the threat; that is, China's use of civilian and other nonmilitary assets ensures that if one of its rivals responds with navy ships, that country will appear to be the party engaging in escalatory behavior rather than China. Moreover, the country employing naval assets risks creating an opportunity for China to respond in kind, thus escalating the conflict to a level at which China enjoys conventional naval superiority.[49]

The following section provides a typology of Chinese gray zone actions in the ECS and SCS; we then conclude with observations for the region.

Types of Chinese Gray Zone Measures in East and Southeast Asia

While Chinese gray zone challenges inhabit many forms, the seven categories described in this section represent the most common in East and Southeast Asia.

Military Intimidation

Military intimation involves the use of military assets to convey the threat of a potential military attack or a risk of military escalation. Examples of gray zone tactics in this category include the following:

- *Troops massed at contested borders.* On October 16, 2012, seven PLAN warships returning from exercises in the Western Pacific

[48] Tobias Burgers and Scott N. Romaniuk, "Hybrid Warriors: China's Unmanned, Guerilla-Style Warfare in Asia's Littorals," *The Diplomat*, February 16, 2017.

[49] Lyle J. Morris, "The Era of Coast Guards in the Asia Pacific Is upon Us," Asia Maritime Transparency Initiative, Center for Strategic and International Studies, March 8, 2017b; and Lyle J. Morris, "Indonesia-China Tensions in the Natuna Sea: Evidence of Naval Efficacy over Coast Guards?" *The Diplomat*, July 5, 2016.

passed through the contiguous zone near Yonaguni Island, which is near Japan. This constituted the first time that Chinese naval vessels had transited through the contiguous zone near the main islands in the Nansei (or Ryukyu) chain.[50] This event occurred a month after Japan nationalized the Senkakus. Another example of such an action involved reports that Chinese troops massed along the border with Vietnam during the Haiyang Shiyou 981 incident in 2014.[51]

- *Large-scale exercises.* The PLAN has progressively expanded its incursions into Japanese airspace, particularly in the ECS and around the Senkaku Islands.[52] In response to these exercises, the Japan Air Self-Defense Force in 2016 flew the highest number of scrambles on record since 1958.[53] The PLAN flights seek to challenge Japanese administrative control of the Senkakus while bolstering China's position in the ECS. Since 2014, China has also begun to fly H-6 bombers near Taiwan, through the Miyako and Tsushima Straits of Japan and into the Western Pacific and the SCS.[54] These flights serve strategic signaling purposes and are part of China's efforts to normalize its military presence in those regions and near disputed waters and territory.
- *Threats of force*. The Chinese government has threatened military retaliation toward countries with which it is engaged in ter-

---

[50] "Chinese Warships Criticized for Crossing Waters Near Japan Island," Associated Press, October 17, 2012.

[51] Joshua Philipp, "Chinese Military Said to Be Massing Near the Vietnam Border (+Photos)," *Epoch Times*, May 18, 2014. The Haiyang Shiyou 981 is a Chinese oil-drilling platform, and the incident refers to tensions between China and Vietnam when the platform was moved into disputed waters in the SCS. See Chapter Four for more details.

[52] Japan Ministry of Defense, "China's Activities Surrounding Japan's Airspace," webpage, undated-a.

[53] Japan Ministry of Defense, "Statistics on Scrambles Through Fiscal Year 2016," press release, April 13, 2017.

[54] See Nathan Beauchamp-Mustafaga, Derek Grossman, and Logan Ma, "Chinese Bomber Flights Around Taiwan: For What Purpose?" *War on the Rocks*, September 13, 2017; and Nathan Beauchamp-Mustafaga, Cristina L. Garafola, Astrid Stuth Cevallos, and Arthur Chan, "China Signals Resolve with Bomber Flights over the South China Sea," *War on the Rocks*, August 2, 2016.

ritorial disputes. In mid-June 2017, for example, Talisman Vietnam, a subsidiary of Spanish energy company Repsol, received permission from the Vietnamese government to drill for gas at the southeast corner of Hanoi's EEZ in the SCS. A few weeks later, the Chinese Foreign Ministry reportedly warned the Vietnamese ambassador in Beijing to halt drilling or else China would take military action against Vietnamese-occupied islands in the Spratly Island chain in the SCS.

- *Provocative actions against U.S. military assets operating in China's EEZ*. Such gray zone tactics involve Chinese civilian, government, or military assets shadowing or intercepting U.S. military assets operating in China's EEZ, sometimes in a dangerous or unprofessional manner. Examples include the following:
  - On April 1, 2001, a PLAN fighter jet crashed into a U.S. Navy EP-3 reconnaissance aircraft 70 miles off of Hainan Island in the SCS when the PLAN jet was conducting dangerous close-in maneuvers to warn the U.S. Navy plane to leave the area. The crash killed the Chinese pilot and forced the U.S. plane to make an emergency landing at Lingshui Air Base on Hainan.[55]
  - On December 5, 2013, the USS *Cowpens*, a guided missile cruiser, nearly collided with a PLAN vessel in international waters in the SCS.[56] The collision reportedly occurred while the *Cowpens* conducted surveillance of the PLAN aircraft carrier *Liaoning,* which was conducting sea trials at the time.
  - On August 19, 2014, a PLA J-11 fighter conducted a dangerous intercept of a U.S. Navy Poseidon P-8 patrol aircraft 135 miles east of Hainan Island.[57] The fighter apparently came within 20 ft of the Poseidon and performed a barrel-roll at close range, in addition to displaying its underbelly with weapons exposed.

---

[55] Paul Eckert, "Dismantled U.S. Spy Plane Flown Out of China," ABC News, July 3, 2001.

[56] David Alexander and Pete Sweeney, "U.S., Chinese Warships Narrowly Avoid Collision in the South China Sea," Reuters, December 13, 2013.

[57] Craig Whitlock, "Pentagon: China Tried to Block U.S. Military Jet in Dangerous Mid-Air Intercept," *Washington Post*, August 22, 2014.

- On May 17, 2016, two PLA J-11 fighters engaged in what the Pentagon called an "unsafe" intercept of a U.S. EP-3 aircraft over waters off Hainan, with one fighter flying within 50 ft.[58]
- In December 2016, a Chinese naval vessel seized an underwater naval drone that was being used by the USNS *Bowditch* to test water conditions in the SCS.[59]
- In May 2018, Chinese naval vessels reportedly maneuvered in an "unprofessional manner" (per the U.S. Navy) when responding to a freedom of navigation operation by the USS *Higgins*, an *Arleigh Burke*–class guided-missile destroyer, and the USS *Antietam*, a *Ticonderoga*-class guided-missile cruiser, near the Paracel Islands, claimed by China, Taiwan, and Vietnam.[60]

Paramilitary Activities

China employs a broad array of maritime paramilitary assets whose platform or operators blur the distinction between civilian and military. Examples include the following:

- *Maritime law enforcement.* China uses maritime law enforcement assets to assert administrative control over disputed waters in the ECS and SCS by adopting tactics that break conventional norms of good seamanship, such as ramming and shouldering, as well as using water cannons, to repel foreign civilian or coast guard vessels from disputed waters. The use of coast guards nominally under civilian control as instruments to conduct peacetime patrols of disputed maritime territory has blurred the line between the platforms and missions traditionally associated with law enforcement and those associated with national defense.[61]

---

[58] Idrees Ali and Megha Rajagopalan, "China Demands End to U.S. Surveillance After Aircraft Intercept," Reuters, May 19, 2016.

[59] Missy Ryan and Dan Lamothe, "Pentagon: Chinese Naval Ship Seized an Unmanned U.S. Underwater Vehicle in South China Sea," *Washington Post*, December 17, 2016.

[60] "U.S. Navy: Chinese Warships Maneuvered in 'Unprofessional' Manner," CBS News, May 30, 2018.

[61] Morris, 2017c.

- *Maritime militia.* China also uses civilian vessels nominally manned by civilian personnel, but these operators are, in reality, naval reservists trained in naval operations. In addition, their vessels may or may not have been equipped with devices to facilitate communication with China Coast Guard (CCG) and PLAN assets during contingencies.[62] Major General Zhang Zhaozhong coined the use of a maritime militia working in tandem with government and military assets as China's *cabbage strategy*—surrounding a contested area in operational layers composed of maritime militia, maritime law enforcement, and navy warships, with the warships positioned the farthest away from direct engagements to avoid escalation while still maintaining a presence.[63]

Co-Opting of State-Affiliated Businesses

The Chinese government has turned to the use of state or state-affiliated bodies and state-owned enterprises, such as state-owned energy and engineering companies, as strategic tools to advance Chinese interests in disputed areas. Some examples of these types of actions include the following:

- *China National Offshore Oil Corporation (CNOOC).* CNOOC is an active player in advancing Chinese territorial claims in the SCS. In June 2012, for example, it offered an international tender of nine oil and gas blocks in the SCS to foreign customers, although no one placed bids because the areas fell within the EEZ and continental shelf of Vietnam. Prior to the deployment of the Haiyang Shiyou 981 platform, CNOOC Chairman Wang Yilin declared that "large deep-water drilling rigs are our mobile national territory and strategic weapon for promoting the development of the country's offshore oil industry."[64]

---

[62] Andrew S. Erickson, "Understanding China's Third Sea Force: The Maritime Militia," Fairbank Center Blog, Harvard University, September 8, 2017.

[63] Harry Kazianis, "China's Expanding Cabbage Strategy," *The Diplomat*, October 29, 2013.

[64] Charlie Zhu, "China Tests Troubled Waters with $1 Billion Rig for South China Sea," Reuters, June 20, 2012.

- *China Communications Construction Company.* Satellite imagery analyzed by IHS Jane's showed that Tianjin Dredging Company, a subsidiary of CCCC Dredging, operated most of the barges involved in the dredging of Mischief Reef, Subi Reef, and Fiery Cross Reef.[65] At least 23 Chinese state-owned enterprises have participated in land reclamation and construction projects in the SCS.[66]

Manipulation of Borders

Similar to Russia's use of the passportization tactic used in Eastern Europe, China has undertaken covert and overt actions to alter the status quo or delineation of territorial or maritime disputes. Such tactics include building artificial islands and dual-use facilities on those islands to alter the status quo in the SCS.[67] China appears to claim expansionist maritime entitlements from these artificial islands, contrary to international law.[68] In addition, to support its Nine-Dash-Line claim, China has issued new passports featuring the line in its pages, thereby compelling foreign governments to issue a "stamp of approval" during customs inspections.[69]

Information Operations

Although not as robust as Russia's tactics, China's gray zone activities including using cyber, media, and propaganda mechanisms against regional states to justify China's claims to sovereignty or to uphold the moral authority of its actions. In the international sphere, such actions include discrediting or responding to other countries' sovereignty claims over islands and maritime space in the ECS and SCS, as

---

[65] Laura Zhou, "Chinese Island-Building Firm Wins Contract with South China Sea Rival Claimant, the Philippines," *South China Morning Post*, October 27, 2017.

[66] Greg Levesque, "China's Evolving Economic Statecraft," *The Diplomat*, April 12, 2017.

[67] Thomas Shugart, "China's Artificial Islands in the South China Sea Are Bigger (and a Bigger Deal) Than You Think," *War on the Rocks*, September 21, 2016.

[68] Tara Devenport, "Island-Building in the South China Sea: Legality and Limits," *Asian Journal of International Law*, Vol. 8, No. 1, January 2018.

[69] Ben Blanchard and Manuel Mogato, "China Decries Attempts to 'Read Too Much into' Passport Map Row," Reuters, November 28, 2012.

well as coordinating campaigns to get nonaligned countries to support China's position on disputed territory.[70] Domestically, this involves bolstering China's claims to disputed maritime features and maritime space in the ECS and SCS through public education, textbooks, and media, as well as discrediting international tribunal judgments and United Nations Convention on the Law of the Sea (UNCLOS) principles in the Chinese media.[71] China has also employed cyber techniques to disrupt the communications of other states. For example, a Philippine naval installation was reportedly compromised when it lost "all communications signals" prior to a clandestine mission in March 2014 to supply Philippine troops stationed on Second Thomas Shoal in the SCS.[72] China has also launched cyber intrusions against Japan and the Philippines during the Scarborough Shoal standoff and after the 2016 Permanent Court of Arbitration (PCA) ruling, as well as against Vietnam during the Haiyang Shiyou 981 standoff in 2014.[73]

In recent years, the Chinese Communist Party has stepped up efforts to influence foreign governments through overt and covert means. Overt means include increasing the number of party-controlled media outlets and cultural institutions operating abroad, such as Confucius Institutes in foreign universities. Covert means include supporting United Front–backed political influence campaigns abroad and supporting Chinese citizens and students to study at key Western academic institutions and corporations to absorb knowledge of key technologies and trade secrets.[74]

---

[70] See, for example, Wang Wen and Chen Xiaochen, "Who Supports China in the South China Sea and Why," *The Diplomat*, July 27, 2016.

[71] Alessandro Uras, "The South China Sea and the Building of a National Maritime Culture," *Asian Survey*, Vol. 57, No. 6, December 2017; and Matt Schrader, "China's Media on the South China Sea Ruling," *The China Story*, September 20, 2016.

[72] Nikko Dizon, "AFP Uses Couriers to Foil China Spies," *Philippine Inquirer*, April 29, 2014.

[73] Anni Piiparinen, "The Chinese Cyber Threat in the South China Sea," *The Diplomat*, September 18, 2015.

[74] Peter Mattis, "Russian and Chinese Political Interference Activities and Influence Operations," in Richard J. Ellings and Robert Sutter, eds., *Axis of Authoritarians: Implications of China-Russia Cooperation*, Seattle, Wash.: National Bureau of Asian Research, October 2018.

Legal and Diplomatic Measures

China has increasingly turned to legal narratives, scholarship, and diplomatic overtures to legitimize its stance on territorial disputes and undermine claims by other states. In many cases, China has sought to carve out exceptions within the existing rules-based order to advance or protect its interests. Examples of such gray zone tactics include the following:

- Abandoning China's Nine-Dash Line in favor of its claim to islands and maritime zones around four archipelagos in the SCS, called the Four Shas,[75] or claiming that China's jurisdiction is the SCS is based on historic rights or traditional fishing grounds that predate the UNCLOS.[76]
- Using legal arguments in its position paper on a dispute with the Philippines to reiterate why China chose to ignore the case and why the arbitral tribunal ruling on the matter has no jurisdiction over the case.[77]
- Declaring an Air Defense Identification Zone (ADIZ) in the ECS, out of line with established practice and norms of other ADIZ rules and regulations.[78]
- Regulating fisheries to strengthen administrative control over disputed areas under the pretext of protection of marine life. For example, in December 2013, China's Hainan Provincial People's Congress passed a law requiring foreign fishing vessels to obtain

---

[75] Julian Ku and Chris Mirasola, "The South China Sea and China's 'Four Sha' Claim: New Legal Theory, Same Bad Argument," Lawfare, September 25, 2017.

[76] Florian Dupuy and Pierre-Marie Dupuy, "A Legal Analysis of China's Historic Rights Claim in the South China Sea," *American Journal of International Law*, Vol. 107, No. 1, January 2013.

[77] Ministry of Foreign Affairs of the People's Republic of China, *Position Paper of the Government of the People's Republic of China on the Matter of Jurisdiction in the South China Sea Arbitration Initiated by the Republic of the Philippines*, Beijing, December 7, 2014.

[78] Edmund J. Burke and Astrid Stuth Cevallos, *In Line or Out of Order? China's Approach to ADIZ in Theory and Practice*, Santa Monica, Calif.: RAND Corporation, RR-2055-AF, 2017.

Chinese permission before operating in a zone covering two-thirds of the SCS.[79]

- Funding research on alternative approaches to international law, such as incentivizing Chinese international law academics to focus their research on certain areas of national interest, including, most prominently, the law of the sea and international economic laws that favor China's position on certain issues.[80] This strategy includes establishing an international maritime judicial center to provide legal backing for China's territorial claims.[81]

Economic Coercion

China uses trade, aid, investments, and threats of sanctions to influence state behavior in contested regions. In most cases, China applies economic coercion against states taking actions related to Chinese territorial claims in Asia, but it also does so against actions related to other Chinese core interests, such as Tibet, Xinjiang, or other human rights issues. Examples of these economic tactics include the following:

- Imposing travel bans and showing tacit support for boycotting South Korea's Lotte Group to compel South Korea to abandon the deployment of U.S. ballistic missile defense system.[82]
- Banning imports of rare earth metals to Japan in light of a Chinese fishing captain's detention in 2010.[83]

---

[79] Craig Murray and Kimberly Hsu, *China's New Fishing Regulations Seek to Justify and Consolidate Control in the South China Sea*, Washington, D.C.: U.S.-China Economic and Security Review Commission, January 27, 2014; and Chen Qingqing and Huang Ge, "China Begins Summer Fishing Moratorium," *Global Times*, May 1, 2017.

[80] Anthea Roberts, "China's Strategic Use of Research Funding on International Law," Lawfare, November 8, 2017.

[81] Ben Blanchard, "Amid Sea Disputes, China to Set Up Maritime 'Judicial Center,'" Reuters, March 12, 2016.

[82] Ethan Meick and Nargiza Salidjanova, *China's Response to U.S. Korean Missile Defense System Deployment and Its Implications*, Washington, D.C.: U.S.-China Economic and Security Review Commission, July 26, 2017.

[83] Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *New York Times*, September 22, 2010.

- Banning fruit imports from the Philippines during the 2012 Scarborough Shoal standoff.[84]
- Suspending salmon imports from Norway in the aftermath of Chinese dissident Liu Xiaobo winning the Nobel Peace Prize.[85]
- Imposing fees on Mongolian commodity exports to China after a visit by the Dalai Lama in 2016.[86]
- Suspending hydrological data-sharing with India to exert pressure during the Doklam standoff in 2017.[87]
- Imposing barriers on the circulation of persons, such as limiting or prohibiting the use of foreign labor and increasing visa requirements for workers or tourists, with the purpose of affecting remittances in the targeted country or affecting the revenues of its tourist industry. For example, China banned tourist groups from traveling to South Korea during the aforementioned dispute over the U.S. ballistic missile defense system.[88] Chinese authorities also issued a travel advisory that adversely affected the tourist industry of the Philippines in 2014.[89]

Conclusion

By exploiting the seams between civilian and military jurisdiction and responses, China's gray zone actions confront countries in what it considers its sphere of influence with a series of policy and strategy challenges. The first challenge is developing approaches that will better

---

[84] Andrew Higgins, "In Philippines, Banana Growers Feel Effect of South China Sea Dispute," *Washington Post*, June 10, 2012.

[85] Terje Solsvik, "Norway Signs Deal to Help Resume Salmon Exports to China," Reuters, May 23, 2017.

[86] "China Slaps New Fees on Mongolian Commodity Exporters Amid Dalai Lama Row," Reuters, November 30, 2016.

[87] Joel Wuthnow, "Did China Use Water as a Weapon During Doklam Standoff?" *War on the Rocks*, October 4, 2017.

[88] Kim Kyung-rok, "THAAD Deployment Causes South Korea's Biggest Ever Services Deficit with China," *The Hankyoreh*, August 6, 2017.

[89] "China Travel Warning Hits PH Tourism Industry," *Philippine Inquirer*, September 23, 2014.

enable these states to deter Chinese nonmilitary but coercive actions. Another challenge is deciding how to respond when such actions are ineffective in deterring China from using its nonmilitary maritime capabilities for coercive purposes. These challenges are compounded by the fact that many countries in the region, such as Japan, perceive gray zone aggression as a domestic law enforcement matter and therefore seek to employ maritime law enforcement actors, such as coast guards, as the primary agents to meet the challenge, while navies play a supporting role.[90]

This survey of Chinese gray zone tactics in the ECS and SCS carries several implications for two key questions being addressed by this study: (1) What are the level and character of the strategic challenge posed by such tactics, and (2) what responses are feasible and appropriate? One obvious lesson is that the vast majority of these challenges cannot be addressed by the United States alone, especially through military means. The United States is not a claimant to any of the disputed maritime features in the ECS and SCS and therefore does not have a direct stake in the resolution of the underlying issue of sovereignty.

Another lesson is that China's ambitions are aimed squarely at two U.S. treaty allies—Japan and the Philippines—as well as a larger set of partners (such as Taiwan and Vietnam) with which the United States has close economic, political, and security ties. If Chinese gray zone tactics were ever to evolve or escalate into unambiguous military aggression involving casualties, the United States would be compelled to respond in some form.

Absent overt military aggression, Chinese attempts to claim almost the entirety of the SCS (including the denial of the legitimate use of the high seas by civilian and military assets and the prevention of the legitimate exploitation of the resources within the EEZs of coastal states under the UNCLOS) presents arguably the most direct and formidable challenge to U.S. interests in the region. How and to what extent the United States is willing to challenge Chinese attempts

[90] Lyle J. Morris, "The New 'Normal' in the East China Sea," *The Diplomat*, March 2017a; and Satoshi Ogawa, "Lessons Learned from Senkaku War Games," *Japan Times*, May 7, 2017.

to restrict these freedoms will cut to the heart of the challenge for U.S. planners contemplating potential policies to combat gray zone measures in the region. Chapters Five and Six will offer a menu of policy options for U.S. leaders to contemplate as they assess how to respond to future Chinese gray zone tactics in the region.

CHAPTER THREE

Findings from Field Research on Gray Zone Challenges in Europe

In this chapter, we seek to build on Chapter Two's broad characterization of the types of gray zone challenges emanating from Russia. Specifically, we offer the key findings from field research that we conducted in France, Germany, the Czech Republic, and Poland, as well as interviews with officials from the Republic of Georgia in Washington, D.C., between late 2017 and early 2018.[1] We first examined specific gray zone threats faced by each of the countries and then surveyed the responses that those countries have begun to put into place, both individually and collectively.

After analyzing the field research and interviews, we argue that Russian gray zone campaigns in Europe consist primarily of disinformation campaigns meant to undermine political institutions. Other Russian gray zone tactics include the use of economic tools to extract concessions or hold countries at risk of being coerced through an overreliance on Russian energy; the demonstration of military threats through exercises near the borders of certain states; and, in a few very extreme cases, the infiltration of Russian security forces to exert de facto control over disputed territory. These approaches are not new, but many of the tools now available provide expanded opportunities for Russia to affect societies and politics outside its border. The sophistication of Russia's tactics has also increased somewhat over time.

[1] We did not conduct field research in Ukraine, whose gray zone vulnerabilities have been covered widely in other analyses. See, for example, Kofman et al., 2017; and Larrabee et al., 2017.

As we will note in Chapter Four, Chinese gray zone tactics have often assumed a more materially threatening form. Russia's more virtual and ephemeral approach has complicated policy responses. The long-term challenge for European states hoping to fashion policies that confront Russia's gray zone activities will be to prioritize timely and proportional whole-of-government counter-responses that deter future tactics without escalating to new thresholds of conflict that may lead to war.

France

France has been the target of cyber and information operation actions from Russia, most prominently during the 2017 election cycle when then–presidential candidate Emmanuel Macron's campaign was hacked by individuals strongly suspected of having ties to the Russian government.[2] Although Macron maintains the "dialogue and firmness" policy of his predecessor and seeks to maintain positive diplomatic relations with Russian president Vladimir Putin, France is more attuned to the threat of Russian gray zone measures than it has been in the past.[3] Although France sees gray zone threats as emanating primarily from Russia, French leaders also see China and criminal groups, for instance, as potential perpetrators of cyberattacks. In combating disinformation challenges, France benefits from its experience countering jihadist propaganda, which was believed to be responsible for inciting several terrorist attacks in France since January 2015 and

[2] French Ministry of Foreign Affairs official, interview with the authors, Paris, February 14, 2018.

[3] Laurent Fabius, "La Politique Étrangère de la France: Quelle Autonomie pour Quelle Ambition?" speech before the French Senate, October 15, 2015. Putin's visit to Versailles in May 2017 was the starting point of the Trianon Dialogue, which aimed to promote dialogue between the French and Russian civil societies (French Ministry of Foreign Affairs official, interview with the authors, Paris, February 14, 2018).

which threatens French forces currently deployed in the Sahel region of Africa and elsewhere.[4]

Types of Gray Zone Threats Faced by France

Attacks During the 2017 Election Cycle

Gray zone threats against France became clearly visible during the presidential and parliamentary election campaigns of late 2016 and early 2017.[5] Then-candidate Macron was targeted by a disinformation campaign and cyberattack. The disinformation campaign consisted of supposed revelations about Macron's sexual orientation and hidden offshore banking accounts. The first rumor appears to have started from a Sputnik article that quickly spread to social and traditional media.[6] The second rumor—that Macron had bank accounts in the Bahamas—started from documents, later established as fraudulent, that were posted on an anonymous bulletin board called "4chan forum" through a source in Latvia and spread through websites and social media users associated with the dissemination of false information.[7]

In February 2017, the Secretary General of Macron's political party, En Marche, accused Russia of trying to destabilize Macron's campaign.[8] In April, the Trend Micro research group further added to the suspicion of Russian involvement, noting that "new cyberattacks on the campaign offices of the front-runner in France's presidential race carried digital 'fingerprints' similar to the suspected Russian hacking of the Democratic National Committee and others in the 2016 U.S.

---

4 Boris Toucas, "Peut-on 'Hacker' Unde Démocratie? Election Présidentielle Américaine et Cyberpuissance Russe," French Ministry of Foreign Affairs, Center for Analysis, Forecasting, and Strategy, January 4, 2017, p. 43.

5 One interviewee noted that cyberattacks targeted the Macron campaign starting as early as fall 2016 (French Ministry of Foreign Affairs official, interview with the authors, Paris, January 16, 2018).

6 Patrick Beuth, Marc Brost, Peter Dausend, Steffen Dobbert, and Götz Hamann, "War Without Blood," *Zeit Online*, February 26, 2017.

7 "How We Debunked Rumours That Macron Has an Offshore Account," *France 24*, May 5, 2017.

8 Martin Untersinger, "Cyberattaques: La France Menace de 'Mesures de Rétorsion' Tout Etat Qui Interférerait dans l'Élection," *Le Monde*, February 15, 2017.

election."[9] Yet the French National Cybersecurity Agency (ANSSI) did not confirm Russia's role—which Russia denied—noting that this could have been the work of another actor trying to masquerade as emanating from Moscow.[10]

The highest-profile attack, known as the "Macron leaks," took place on May 5, 2017. A large number of email files from the Macron campaign were hacked and posted on an anonymous sharing site. The event took place shortly before the official blackout period that begins a week before the presidential vote, during which candidates are not allowed to speak publicly and the media is not allowed to report on them.[11] The leaks spread quickly through social media, but mainstream media mostly refrained from commenting on them.[12]

Financing of a Far-Right Political Party

The French National Front (which changed its name in June 2018 to National Rally) is the only extreme-right political party in Western Europe with acknowledged financial ties to Russia, having received an $11.7 million loan from a Russian bank in September 2014.[13] Some other such associations with Russia—for instance, with the Alternative für Deutschland (AfD) party in Germany—are suspected but not clearly established.

Influence in Business and Intellectual Circles

Several political, business, and intellectual circles in France share pro-Russian views. It is important to note that these views are far from marginal; rather, they are the legacy of a Gaullist tradition of maintaining France's strategic independence between East and West by balanc-

---

9 Noack, 2017a.

10 Noack, 2017a.

11 See, for instance, Megha Mohan, "Macron Leaks: The Anatomy of a Hack," BBC News, May 9, 2017.

12 Dana Priest, "Lessons from Europe's Fight Against Russian Disinformation," *New Yorker*, July 24, 2017.

13 Motet, 2016; Daley and de la Baume, 2014; and Polyakova et al., 2016, p. 7.

ing the influence of the United States and the Soviet Union or Russia.[14] It is particularly telling, in this regard, that out of the four political parties that obtained the most votes during the first round of the presidential election in May 2017, three (National Front, the extreme-left La France Insoumise, and the mainstream right-wing party Les Républicains) openly shared pro-Russian views.[15] Some business leaders with interests in Russia also argue for a more lenient sanctions policy toward Russia.[16] As an illustration of the relations between French business circles and Russia, Russia named its first icebreaking liquefied natural gas tanker after Christophe de Margerie, former chief executive of French oil corporation Total, who died in a plane crash in Moscow in 2014 and was close to Putin.[17] There are also several pro-Russian organizations and research institutions in France, such as the Institute of Democracy and Cooperation, led by a Russian lawyer who has served in the Public Chamber of the Russian Federation.[18] The Russian Orthodox Church has only a small following in France but recently increased its profile with the construction of a new church and cultural center near the Eiffel Tower in Paris.[19] Russia seeks to leverage these interest groups who hold pro-Russia views to its advantage, particularly during times of heighted bilateral tension with France.

Specific Threats Against the Military

The French military sees two key areas in which gray zone threats need to be countered. The first resides in the cyber domain; gray zone tactics

---

[14] Polyakova et al., 2016, p. 7.

[15] Laura Daniels, "How Russia Hacked the French Election," *Politico*, April 23, 2017. For more details on the pro-Russian views of French political parties and political leaders, see, for instance, Nicolas Hénin, *La France Russe: Enquête sur les Réseaux de Poutine*, Paris: Fayard, 2016, pp. 91–130.

[16] Polyakova et al., 2016, pp. 8–9.

[17] Benjamin Quénelle, "Le 'Margerie,' Homage Posthume à un 'Ami,'" *Les Echos*, March 31, 2017.

[18] Polyakova et al., 2016, p. 9. For more details on this institute, see, for instance, Cécile Vaissié, *Les Réseaux du Kremlin en France*, Paris: Les Petits Matins, 2016, pp. 115–118.

[19] "A New Orthodox Church Next to the Eiffel Tower Boosts Russian Soft Power," *The Economist*, December 5, 2016.

could target military networks to steal information, disrupt operations, or compromise the integrity of critical infrastructure. France's 2017 Strategic Review of Defence and National Security notes,

> the capacity to take action in cyberspace and in the informational domain is becoming increasingly accessible. As a result, our societies, populations, government services and businesses are more directly exposed to interference or malicious actions that may have major consequences.[20]

The document further adds that particularly serious cyberattacks might be defined as "armed aggression" and justify the use of force in self-defense.[21] A second key concern is the security of French forces deployed in outside missions, particularly in the Baltic states (Estonia, Latvia, and Lithuania) but also in the Sahel. French forces are seen as potentially vulnerable to the same type of threats as German soldiers—for example, the dissemination of fake news to stir up popular and local resentment to the deployment of French forces, as well as the theft of personal or confidential information from French soldiers.[22]

How Has France Responded to Gray Zone Threats from Russia?

Tactical Response During the 2017 Election Cycle

The Macron campaign developed a multipronged strategy to counter both the disinformation and the cyber threats against its candidate. Among other actions, Macron campaign officials inserted random elements into their communications, effectively creating informational noise that rendered stolen material more difficult to exploit by Russian hackers.[23] Campaign officials monitored social media, and candidate Macron spoke publicly about false information in an attempt to under-

---

[20] Republic of France, 2017b.

[21] Republic of France, *Revue Stratégique de Défense et de Sécurité 2017*, Paris, 2017a, p. 35, para. 90 (authors' translation).

[22] French Ministry of Defense official, interview with the authors, Paris, February 16, 2018.

[23] French Ministry of Foreign Affairs official, interview with the authors, Paris, February 14, 2018.

cut any potential negative blowback from Russia's actions.[24] During the Macron leaks, the Macron campaign managed to deflect the public's attention by focusing on mechanisms through which the information was disseminated, including prominent alt-right channels in the United States, rather than on the information itself.[25]

The French government was also active in responding to what it saw as clear attempts to sow discord during the 2017 elections. The Ministry of Foreign Affairs removed electronic voting for parliamentary elections for French citizens living abroad, for example, after a thorough review by the French government made it clear that the system had vulnerabilities that could compromise the entire ballot.[26] ANSSI offered cybersecurity awareness seminars for political parties, all of which accepted the training, with the exception of the National Front party. French authorities also sent political parties a list of preapproved companies that could provide cyber expertise.[27]

Public Diplomacy

Following Germany's response to cyber hacks by Russia,[28] which will be discussed later in this chapter, the French government leveraged

---

[24] French diplomat, interview with the authors, Washington, D.C., January 16, 2018. For a more detailed account on the methods used by the Macron campaign, see Adam Nossiter, David E. Sanger, and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *New York Times*, May 9, 2017.

[25] French Ministry of Foreign Affairs official, interview with the authors, Paris, February 14, 2018.

[26] French Ministry of Foreign Affairs officials, interview with the authors, Paris, February 13, 2018; and French Ministry of Foreign Affairs officials, interview with the authors, Paris, February 14, 2018. See also Damien Leloup, "Législatives: Les Français de l'Étranger Privés de Vote Électronique pour des Raisons de Sécurité," *Le Monde*, March 6, 2017. This article notes that, because of similar concerns, the Netherlands had made a similar decision to prohibit electronic votes for its parliamentary elections in March 2017.

[27] Mehdi Chebil, "France Takes Steps to Prevent an Election Hack Attack," *France 24*, January 16, 2017; and Daniels, 2017.

[28] Germany's handling of its own gray zone threats during its 2017 election is seen in France as a positive example, particularly the decision to comment publicly on the risks of Russian meddling in the upcoming elections. The way the hack of the Democratic National Committee was handled in the United States was seen as counterproductive (French diplomat,

public diplomacy in response to Russian actions.[29] In February 2017, Prime Minister Jean-Marc Ayrault raised the issue of Russian cyber operations before the French National Assembly in response to a question from a member of Parliament; Ayrault named Russia twice and suggested that retaliatory measures were possible.[30] A similar message was sent through formal bilateral channels with Putin and Russian Foreign Minister Sergey Lavrov, as well as to the Russian ambassador in Paris.[31] Finally, shortly after his election as president in May 2017, Macron described Russian media outlets RT and Sputnik as "organs of influence and propaganda" in front of Putin during his official visit to France.[32]

New Strategies, Structures, and Legislation

Since the issue of Russian information operations in France gained prominence, the French government put into place strategies designed to address cyber and informational threats. These efforts have been particularly enhanced since Macron—himself a target of both types of attacks—won the presidency. Recent initiatives include the publication of a *Strategic Review of Cyber Defense* in February 2018, which focuses on cyber threats but also includes some elements on disinformation campaigns.[33] The review formalizes interagency coordination that

---

interview with the authors, Washington, D.C., January 16, 2018; and French Ministry of Foreign Affairs officials, interview with the authors, Paris, February 14, 2018).

[29] French Ministry of Foreign Affairs officials, interview with the authors, Paris, February 14, 2018.

[30] Jean-Marc Ayrault, "Questions au Gouvernement," Paris: Assemblée Nationale, February 15, 2017.

[31] French diplomat, interview with the authors, Washington, D.C., January 16, 2018; French Ministry of Foreign Affairs officials, interview with the authors, Paris, February 14, 2018; and U.S. Senate Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Washington, D.C.: U.S. Government Printing Office, January 10, 2018, p. 125.

[32] James McAuley, "French President Macron Blasts Russian State-Owned Media as 'Propaganda,'" *Washington Post*, May 29, 2017; and Audrey Kucinskas, "Fustigés par Macron, RT et Sputnik, des Medias 'Stratégiques' pour la Russie," *Express*, June 9, 2017.

[33] Republic of France, *Revue Stratégique de Cyberdéfense*, Paris: General Secretariat of Defense and National Security, February 12, 2018.

existed informally previously.[34] It also recommends creating a Coordination Center for Cyber Crises aimed at providing relevant agencies with a coordinated understanding of current attacks.[35] Another flagship initiative, led directly by President Macron, is a legislative proposal on controlling the dissemination of so-called fake news during electoral periods.[36] Macron is also intent on reforming the French broadcasting authority (Conseil Supérieur de l'Audiovisuel) to tighten the standards and the vetting and fact-checking processes of broadcasting.[37]

Use of Existing Responses

France is devoting more resources to counter global cyber threats.[38] Initiatives include reinforcing government information technology systems; doubling the budget of ANSSI between 2010 and 2014;[39] enhancing research and development efforts, such as "crypto-quantique";[40] expanding the purview of the digital ambassador position (initially limited to the issue of internet governance[41]); and moving the Junior Ministry for Digital Affairs, previously subordinate to the Ministry of Economy, to the Prime Minister's office.[42] ANSSI also offers recommendations for "operators of vital importance," including private entities and political parties. One noteworthy element of the French

---

[34] French think-tank researcher, interview with the authors, February 15, 2018.

[35] French Ministry of Foreign Affairs officials, interview with the authors, February 14, 2018. See Republic of France, 2018, p. 137.

[36] See, for instance, "Voeux à la Presse: Macron Annonce une Loi Contre les 'Fake News,'" Radio France Internationale, January 4, 2018; and "Macron Annonce un Projet de Loi pour le Contrôle des 'Fausses Informations,'" *France 24*, January 3, 2018.

[37] French think-tank researcher, interview with the authors, February 15, 2018.

[38] Marine Pennetier, "Under Threat, France Grooms Army Hackers for Cyber Warfare," Reuters, April 5, 2017.

[39] U.S. Senate Committee on Foreign Relations, 2018, p. 125.

[40] French Ministry of Foreign Affairs officials, interview with the authors, Paris, February 13, 2018.

[41] French Ministry of Foreign Affairs official, interview with the authors, Paris, February 16, 2018.

[42] French think-tank researcher, interview with the authors, Paris, February 15, 2018.

response is its very clear separation between system protection (under ANSSI) and intelligence and offensive issues (managed by civilian and military intelligence services). This distinction makes it easier for ANSSI officials to speak publicly about cybersecurity threats and attacks and facilitates coordination with the private sector and international partners.[43]

Self-Discipline and Private Initiative

When the Macron leaks surfaced, the French electoral commission instructed the French news media not to report on the leaks, because of the blackout law. The media complied—although it is unclear whether they did so for ethical reasons or because such reporting might have been illegal.[44] The media has also developed various fact-checking initiatives, such as Decodex, offered by the *Le Monde* newspaper, and CheckNews, offered by the *Libération* newspaper. Social media companies were active as well: Facebook suspended 30,000 accounts for promoting propaganda before the French elections.[45] Facebook and others have developed their own initiatives to combat fake news and have funded some of the fact-checking initiatives of French newspapers.[46] One interviewee noted that the experience of counter-jihadist propaganda in France had provided lessons that public affairs efforts, such as the Stop Jihadism campaign, were not effective and that reaching out to local communities proved more effective.[47] This suggests that public efforts should be supplemented with a greater focus on civil society.

Military Measures

The French military has taken a variety of measures to mitigate gray zone threats, including the December 2016 creation in a cyber opera-

---

[43] French Ministry of Foreign Affairs official, interview with the authors, Paris, February 14, 2018; and Chebil, 2017.

[44] French Ministry of Foreign Affairs official, interview with the authors, Paris, February 14, 2018; and Priest, 2017.

[45] Eric Auchard and Joseph Menn, "Facebook Cracks Down on 30,000 Fake Accounts in France," Reuters, April 13, 2017.

[46] French think-tank researcher, interview with the authors, Paris, February 15, 2018.

[47] French Ministry of Defense official, interview with the authors, Paris, February 14, 2018.

tional command tasked with defending the Ministry of Defense and other critical infrastructure networks against attack.[48] This command was projected to receive 1 billion euros in funding by 2019 and include a staff of up to 3,200 military officers, along with a reserve force of 4,400.[49] Another initiative of interest includes the French Ministry of Defense's funding of the Russian Cyberspace Observatory to study and monitor how Russia uses the digital domain to diffuse influence.[50]

To protect French forces, the Ministry of Defense's response includes educating soldiers who are set to deploy abroad to increase their awareness of potential threats. This is coupled with a careful communication strategy toward local populations, as well as the monitoring of social media for potential fake news that might affect the safety or reputation of the French armed forces. These measures were assessed after the Estonia deployment and retaken before the deployment of French troops to Lithuania. However, they are not specific to the Baltic theater; measures of prevention and protection are also taken in other theaters (e.g., the Sahel).[51]

Germany

Similar to the methods used in France, Russia's gray zone methods in Germany appear aimed at undermining German democracy, including by calling into question the legitimacy and competence of its elected leaders.[52] Russia has affinities with political parties, such

---

[48] French Ministry of Defense official, interview with the authors, Paris, February 16, 2018; and French Ministry of Defense officials, interview with the authors, Washington, D.C., January 19, 2018.

[49] Pennetier, 2017.

[50] French researcher on cyber issues, interview with the authors, Paris, February 15, 2018. See Chaire Castex de Cyberstratégie, "Observatoire de l'Infosphère Russophone," webpage, undated.

[51] French Ministry of Defense official, interview with the authors, Paris, February 16, 2018.

[52] Constanze Stelzenmüller, "The Impact of Russian Interference on Germany's 2017 Elections," testimony before the U.S. Senate Select Committee on Intelligence, June 28, 2017.

as the extreme-right AfD and extreme-left Die Linke, and with the anti-migrant movement Pegida.[53] Many suspect that there are some financial links between Russia and some of these parties (particularly AfD), but no links have been proven. The influence that Russia wields within mainstream German political parties, such as the Social Democratic Party and the Christian Social Union in Bavaria, is thought to be more limited.[54]

Officials and researchers that we interviewed in Germany highlighted the fact that Germany is or could become the target of gray zone tactics by other countries besides Russia. China's growing economic influence, including through the acquisition of German companies or through economic espionage, was mentioned, and German research institutions have started to focus more attention on the topic.[55] Interviewees also mentioned Turkey's efforts to influence the Turkish minority in Germany, some of which appear to have been aimed at intimidating Turkish opposition politicians at home through their diaspora followers in Germany.[56]

The German government openly recognizes that Russia employs or could employ gray zone activities to undermine its political system, undermine the legitimacy of its elected officials, and accentuate existing divisions in German society. Civilian authorities see disinformation as their most pressing concern, along with cyber threats. German government responses to these threats have been inspired, in part, by the U.S. response to the Democratic National Committee hack and by the French response to the Macron leaks. The German armed forces (the Bundeswehr) see cybersecurity as a primary concern. Disinformation also remains a threat, as illustrated by the false accusations of

---

[53] For more details on this issue, see Melanie Amann and Pavel Lokshin, "German Populists Forge Ties with Russia," *Spiegel Online*, April 27, 2016.

[54] German think-tank researcher, interview with the authors, Berlin, February 13, 2018; and Stelzenmüller, 2017.

[55] German armed forces official, interview with the authors, Berlin, February 12, 2018.

[56] German think-tank researcher, interview with the authors, Berlin, February 13, 2018; and German armed forces official, interview with the authors, Berlin, February 12, 2018.

rape against German troops in Lithuania that appeared in the media in 2017.[57]

Types of Gray Zone Threats Faced by Germany

Disinformation Campaigns

The most prominent example of Russian disinformation in Germany is the "Lisa case," in which reports alleged that a 13-year-old Russian-speaking girl had been raped in Berlin by asylum seekers.[58] The Lisa story prompted protests from the Russo-German community, and a public statement from Russian Foreign Minister Lavrov publicly cast doubt on the ability of the German police to investigate the case.[59] This story, however, backfired to some extent. Russia's interference was much criticized in Germany after the episode, particularly after the story was clearly established to be a fabrication, and a survey of Russo-Germans conducted by German domestic intelligence services illustrated that the community felt "betrayed" and was less likely to undertake similar protests in the future.[60] More broadly, several pro-Russian media outlets that are active in Germany, including RT Deutsch, Sputnik, and News Front, have shown a bias for issues that are controversial or divisive in Germany.

Two communities in Germany appear most at risk of Russian influence: the Russian-speaking minority in Germany, estimated at around 2.5 million people,[61] and citizens from former East Germany, who tend to hold more-positive views of Russia than the rest of the German population does.[62] A key issue for Germany is the relationship between Russian influence and extreme-right (particularly AfD) influ-

---

[57] German armed forces official, interview with the authors, Berlin, February 12, 2018; and German researcher, phone interview with the authors, March 1, 2018.

[58] German researcher, phone interview with the authors, March 1, 2018.

[59] Damien McGuiness, "Russia Steps into Berlin 'Rape' Storm Claiming German Cover-Up," BBC News, January 27, 2016.

[60] German armed forces official, interview with the authors, Berlin, February 12, 2018.

[61] Stelzenmüller, 2017.

[62] German diplomat, interview with the authors, Washington, D.C., December 12, 2017.

ence.[63] The Russo-German community is traditionally a conservative group, making its members sympathetic to themes promoted by AfD and right-wing parties more generally.[64] Those with business interests represent a third community that is potentially sympathetic to Russian views. Former Chancellor Gerhard Schroder, for example, is on the board of several energy companies controlled by the Russian government and several business groups that hold a pro-Russia orientation.[65]

Cyberattacks

Germany has experienced a series of cyberattacks, starting with a distributed denial-of-service attack against the German government's websites on January 7, 2015, as Ukrainian Prime Minister Arseni Yatsenuk was approaching Berlin for his upcoming meeting with German Chancellor Angela Merkel. The attack was attributed to the CyberBerkut hacker group and ceased shortly after Yatsenuk departed Berlin.[66] The German Parliament (the Bundestag) was the target of a cyberattack in May 2015 that resulted in the theft of 16 gigabytes of data from the computers of 14 members.[67] According to German domestic intelligence, the perpetrator of the attack was the Fancy Bear group, which is believed to be responsible for the hack against the Democratic National Committee in the United States.[68] Finally, in November 2016, Deutsche Telekom was the target of a cyberattack that disrupted services but failed to achieve the large-scale denial-of-

---

63 German researcher on cyber issues, phone interview with the authors, February 21, 2018.

64 German think-tank researcher, interview with the authors, Berlin, February 13, 2018; and German think-tank researcher, interview with the authors, Berlin, February 13, 2018.

65 See, for instance, Rick Noack, "He Used to Rule Germany. Now, He Oversees Russian Energy Companies and Lashes Out at the U.S." *Washington Post*, August 12, 2017b; and Stelzenmüller, 2017.

66 Beuth et al., 2017.

67 Beuth et al., 2017.

68 Beuth et al., 2017; Stelzenmüller, 2017.

service that it was meant to provoke.[69] Additional cyberattacks have targeted political officials and parties of Germany.[70]

Specific Threats Against the Military

The German military's main concerns are cyber threats against its information technology networks and various forms of pressure exerted against its forces currently deployed in Lithuania. The 2016 *White Paper on German Security Policy and the Future of the Bundeswehr*, for example, highlights "challenges from the cyber and information domains" as "challenges for Germany's security policy."[71] In Lithuania, German forces have faced cyberattacks, espionage, overflights of installations by drones, actions by agent provocateurs, harassment, and the dissemination of false information stating that German soldiers had raped a Lithuanian girl (reminiscent of the aforementioned "Lisa case").[72]

How Has Germany Responded to Gray Zone Threats from Russia?

Strategic Communication and Diplomacy

On the civilian side, a key aspect of the German response has been a growing willingness to name Russia as a threat in public forums—partly in reaction to the Barack Obama administration's more muted response to the U.S. Democratic National Committee leak, a response that Germans generally considered ineffective.[73] The directors of Germany's internal and external intelligence services (the Office for the Protection of the Constitution and the Federal Intelligence Service) took the unusual step of speaking publicly about the risks of cyberattacks and electoral interference from Russia. Russia was also clearly

---

[69] "Russia Hackers: German Spy Chief Kahl Warns of Election Disruption," BBC News, November 29, 2016; and Beuth et al., 2017.

[70] Andrea Shalal, "Germany Challenges Russia over Alleged Cyberattacks," Reuters, May 4, 2017.

[71] German Federal Government, *White Paper on German Security Policy and the Future of the Bundeswehr*, Berlin, July 2016. This document notes, "On the whole, the cyber and information domain has become an area of international and strategic importance that has practically no limits. Its significance will continue to grow" (pp. 36–37).

[72] German armed forces official, interview with the authors, Berlin, February 12, 2018.

[73] German diplomat, interview with the authors, Washington, D.C., January 16, 2018.

named as being responsible for the cyberattack on the Bundestag.[74] As one analyst noted, "Public acknowledgement of Russian interference by senior officials is deliberate and aims to both raise the bar for the Kremlin and sensitize the German public."[75]

Such strategic communications were complemented by private warnings from German officials to Russia. For instance, Chancellor Merkel directly warned Putin during their meeting at Sochi in May 2017 that Germany would take "decisive measures" if Russia tried to interfere in the upcoming German elections.[76]

New Legislation and Structures

Germany's flagship initiative to counter disinformation is a law passed by the Bundestag in October 2017 that obliges large social media platforms to remove within 24 hours posts that are considered "illegal" under Germany's criminal code.[77] Companies are also required to report publicly every sixth months on compliance with the law.[78] Although it is too early to gauge whether this law will have a positive effect, it is worth noting that the new legislation forces social media platforms to remove swiftly only the content that is being flagged by users. It is not a fact-checking law and, therefore, might have limited effects on disinformation campaigns while raising issues related to freedom of speech.

Cybersecurity

Over the past few years, Germany has increased the resources devoted to cybersecurity and resilience. Initiatives include the publication in 2016

---

[74] "Russia 'Was Behind German Parliament Hack,'" BBC News, May 13, 2016. See also Shalal, 2017; Esther King, "Russian Hackers Targeting Germany: Intelligence Chief," *Politico*, November 29, 2016; and "Russia Hackers: German Spy Chief Kahl Warns of Election Disruption," 2016.

[75] Stelzenmüller, 2017.

[76] Lynn Berry and David Rising, "Putin, Merkel Spar in Russia over Election Meddling," Associated Press, May 2, 2017.

[77] Linda Kinstler, "Can Germany Fix Facebook? A New Law Seeks to Protect 'Human Dignity' on the Internet," *The Atlantic*, November 2, 2017.

[78] Melissa Eddy and Mark Scott, "Delete Hate Speech or Pay Up, Germany Tells Social Media Companies," *New York Times*, June 30, 2017.

of a cybersecurity strategy that creates "rapid reaction cyber teams" across the government;[79] the creation of a Cyber Defense Center;[80] the reinforcement of governmental information technology networks;[81] and a massive expansion of the Federal Office for Information Security, which provides advice and recommendations for cybersecurity.[82]

Several German responses in this domain take place at the EU and NATO levels. EU initiatives include the 2016 *EU Joint Framework on Countering Hybrid Threats: A European Union Response*, the creation in the same year of the Hybrid Fusion Cell to enable intelligence agencies to share information on cyber threats, the adoption of an EU directive to impose minimal standards of cyber protection for critical infrastructure,[83] and a 2017 joint EU communication on "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU."[84] NATO has also developed seven standards of resilience,[85] and it is leading an effort to enhance cyber threat awareness.[86]

Education

Another line of effort focuses on education. In Germany, the government has engaged the Russo-German community by providing the Federal Center for Political Education website in Russian. The center offers conferences on Russo-German experiences and sponsors town

---

[79] U.S. Senate Committee on Foreign Relations, 2018, p. 131.

[80] Stelzenmüller, 2017.

[81] Stelzenmüller, 2017.

[82] German Ministry of Foreign Affairs officials, interview with the authors, Berlin, February 13, 2018.

[83] German Ministry of Foreign Affairs officials, interview with the authors, Berlin, February 12, 2018.

[84] For a summary of recent EU initiatives, see European Commission, "Security and Defence: Significant Progress to Enhance Europe's Resilience Against Hybrid Threats—More Work Ahead," press release, Brussels, July 19, 2017.

[85] German Ministry of Foreign Affairs officials, interview with the authors, Berlin, February 12, 2018. See also Lorenz Meyer-Minnemann, *Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience*, Washington, D.C.: Johns Hopkins School of Advanced International Studies, Center for Transatlantic Relations, undated.

[86] German researcher on cyber issues, phone interview with the authors, February 21, 2018.

hall meetings for Russo-Germans.[87] Externally, Germany has been providing support to the Baltic states for media education since 2014.[88]

Private Initiatives

Some German initiatives have been initiated by private actors. For example, in the run-up to the September 2017 election, social media companies worked with German authorities to improve fact-checking, provide cybersecurity training to candidates, and purge their platforms of fake accounts.[89] New investigative media organizations, such as CORRECTIV of Germany, have started tracking instances of disinformation campaigns as well.[90]

Improved Coordination at the National Level

One challenge that Germany has faced in warning citizens about and responding to gray zone tactics is the structure of the federal government.[91] Germany has more than a dozen intelligence agencies at the federal level, many of which lack a holistic picture of national security threats.[92] Additionally, network security is not standardized across the federal and local levels, and local authorities have their own response system for cyber incidents. To address these issues, the national Cyber-Security Council convenes federal, local, and other key security leaders and researchers several times a year to exchange information.[93] In addition, the Federal Foreign Office has established a department for strategic communication to address the problem of disinformation,

---

87 German think-tank analyst, interview with the authors, Berlin, February 9, 2018.

88 German think-tank researcher, interview with the authors, Berlin, February 13, 2018.

89 U.S. Senate Committee on Foreign Relations, 2018, p. 131.

90 German analyst, interview with the authors, February 9, 2018. CORRECTIV is a profit news organization in Germany whose purposes are to investigate injustice and abuses of power and to promote media literacy and educational programs. See CORRECTIV, homepage, undated.

91 German analyst, interview with the authors, Berlin, February 9, 2018.

92 German armed forces official, interview with the authors, Berlin, February 12, 2018.

93 German Ministry of Foreign Affairs officials, interview with the authors, Berlin, February 12, 2018.

including developing knowledge to assist other EU member states in the Baltics, the Balkans, and elsewhere through bilateral channels.[94]

Military Responses

The German military has adopted specific responses to gray zone threats. A Cyber Command, staffed with about 13,500 military and civilian personnel, was launched in 2017 as the sixth branch of the German armed forces. One of its missions is to defend military networks against cyber threats.[95] Other initiatives include building a more integrated response for deployed German battalions against threats of espionage, psychological pressure, or theft of personal data; recruiting top information technology experts from the civilian world; creating a Cyber Innovation Hub initiative to fund civilian cyber start-ups; funding a master's degree on cyber defense at the University of Munich; and modernizing and professionalizing the Ministry of Defence's department of public affairs.[96] The German military also takes part in exercises with a hybrid component involving nontraditional security challenges. Examples include NATO's annual Crisis Management Exercise, which focuses on interoperability and the joint definition of common warnings and indicators for when a crisis response should be triggered; the EU's 2017 Parallel and Coordinated Exercise, which represented the EU's first attempt at a crisis response exercise directly applied to cyber and hybrid threats; and a 2017 exercise for EU defense ministers in Tallinn focusing on "cybrid" (cyber hybrid) issues.[97] The Ministry of Defence is also leading Germany's participation in the European Centre of Excellence for Countering Hybrid Threats, a think tank based in Helsinki, Finland.[98]

---

[94] German researcher, phone interview with the authors, March 1, 2018.

[95] U.S. Senate Committee on Foreign Relations, 2018, p. 131.

[96] German armed forces official, interview with the authors, Berlin, February 12, 2018.

[97] German armed forces official, interview with the authors, Berlin, February 12, 2018; and European Union External Action, "EU Launches Exercise to Test Crisis Management Mechanisms in Response to Cyber and Hybrid Threats," press release, Brussels, September 28, 2017.

[98] German armed forces official, interview with the authors, Berlin, February 12, 2018.

Overall, because the data stolen from the Bundestag did not resurface on anonymous web forums or on social media and because there were no known incidents during the September 2017 federal election, Germans have perceived this as evidence that their responses to gray zone threats were effective. It is unclear, however, how much of this outcome was due to Germany's preventive measures. Other potential explanations include that Russia did not perceive the Bundestag data to be valuable, that influencing a multi-party election is generally difficult, and that Russia was concerned that interference might backfire and increase popular support for Chancellor Merkel. By the time of our interviews in Germany, discussions of gray zone threats had somewhat receded from the public debate, particularly as Germany focused on forming a governing coalition.[99] However, the revelation in March 2018 of a December 2017 hack against governmental networks that targeted the Foreign Office, which Russia is suspected of implementing, suggests that Germany's efforts at addressing gray zone tactics still fall short of what is needed to eliminate or significantly curtail the threat.[100]

Czech Republic

The Czech Security Information Service has identified a range of goals of Russia's influence campaign in the Czech Republic. These include the following broad tactics:

- disrupting the coherence and readiness of NATO and the EU in the Czech Republic
- isolating and damaging the reputation of Ukraine within the Czech media
- using disinformation campaigns from Czech sources for a Russian audience

[99] German think-tank researcher, interview with the authors, Berlin, February 13, 2018.

[100] German researcher, phone interview with the authors, March 1, 2018.

- directly targeting Czech institutions and society with information operations, including weakening independent Czech media and exacerbating Czech intersocietal and interpolitical tensions.[101]

Interviews conducted for this study corroborate these tactics and the characterizations of threats. As one interviewee noted, Russia seeks to gain influence and sow discord in the EU, to ensure that the Czech Republic remains in a "zone of influence," and to demonstrate to the Russian population that there is support for the current Russian regime in the West.[102]

Types of Gray Zone Threats Faced by the Czech Republic

Political Influence

Interviewees indicated that Russia's influence penetrates the highest political levels in the Czech government. The leading example cited by interviewees was the fact that current President Miloš Zeman, of the Party of Civic Rights, maintains strong connections with Russia and is known to hold pro-Russian views. Within the Czech Republic, Zeman plays a pivotal role in amplifying Russian disinformation by promoting Kremlin positions in public statements.[103] For example, Zeman stated that Crimea is Russian territory, denied the presence of organized Russian troops in Ukraine, and demanded that Western countries lift sanctions against Russia.[104] Within Russia, Zeman is portrayed as a "strong anti-American leader who is a close friend of Vladimir Putin"—a position that helps the Kremlin regime justify its foreign policy position and paints a picture that Russia is not interna-

---

[101] Jakub Janda, "Czech Intelligence Alarmed by Russian 'Threat,'" *EUobserver,* September 2, 2016.

[102] Anonymous, interview with the authors, Prague, February, 2018.

[103] Jakub Janda and Veronika Vichova, "The Kremlin's Hostile Influence in the Czech Republic: The State of Play," Warsaw Institute, August 10, 2017.

[104] Jakub Janda, "How Czech President Miloš Zeman Became Putin's Man," *Observer*, January 26, 2018. Zeman told the Parliamentary Assembly of the Council of Europe that sanctions against Russia were "destructive and ineffective" and called the annexation of Crimea a "done deal" (Keno Verseck, "Is the Czech Republic Moving Closer to China and Russia?" *Deutsche Welle,* January 31, 2018).

tionally isolated.[105] Zeman has also threatened to hold a referendum on a Czech departure from the EU, popularly known as Czexit.[106]

Potential sources of Russian influence on President Zeman include the following:

- *Russian business leverage over senior advisers*. Zeman's key advisers include Martin Nejedlý and Zdeněk Zbytek, two entrepreneurs with established ties to Russian businesses who advocate for Russian business interests in the Czech Republic.[107] Nejedlý, the Czech representative of Russia's Lukoil petroleum and natural gas company, openly backed Zeman's Party of Civic Rights.[108]
- *Ideological and social cultivation*. President Zeman is a frequent attendee of the Rhodes forums in Cyprus, an anti-Western conference organized by Putin affiliate Vladimir Yakunin.[109]
- *Participation in Russian disinformation activity during presidential campaigns.* Zeman's 2018 presidential campaign included a large-scale unattributed social media campaign against opponent

---

[105] European Values, *Policy Shift Overview: How the Czech Republic Became One of the European Leaders in Countering Russian Disinformation,* Prague, October 5, 2017.

[106] Mark Chandler, "Czech Election Result: EU Panics as Populist Zeman Wins—and He Welcomes EU Referendum," *Express,* January 27, 2018.

[107] Ivana Smoleňová, Barbora Chrzová, Iveta Várenyiová, Dušan Fischer, Dániel Bartha, András Deák, András Rácz, and Andrzej Turkowski, *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries,* Prague: Prague Security Studies Institute, November 2017.

[108] Owen Matthews, "The Kremlin's Campaign to Make Friends," *Newsweek,* February 16, 2015. The article also states that "Russian editions of Zeman's books were published by a Lukoil-backed publishing house."

[109] Anonymous, interview with the authors, Prague, February, 2018. According to a 2016 news article,

> Yakunin's career has taken him from the Soviet Army through the Soviet Union's diplomatic mission to the United Nations, through Russia's Transport Ministry to finally become the president of Russia's state railway operator, a position he held till 2015. In 1996, he also became one of the co-founders, along with Putin, of the Ozero dacha housing cooperative—a circle of businessmen considered to be the Russian president's "inner circle," all of whose members have held powerful government or business positions in Russia since. (Ben Knight, "Putin Associate Opens Russia-Friendly Think Tank in Berlin," *Deutsche Welle,* July 1, 2016)

Jiří Drahoš accusing him of collaborating with the secret police during Communist rule.[110]

Czech Prime Minister Andrej Babiš of the ANO party (based on the former Action for Dissatisfied Citizens movement) has also occasionally advocated a warmer relationship with Moscow. He has, on several occasions, been critical of the EU and once called for a ban on Muslim immigrants, for example.[111] Although some journalists have claimed that Babiš maintains ties with Putin, Babiš has publicly denied these claims.[112] He has been under investigation for corruption charges related to alleged EU farm subsidy fraud, although he says that the charges are politically motivated.[113] Interviewees further claimed that Russia has maintained support for extreme political parties—specifically, Communists and right-wing movements—but the channels through which Russia purportedly provides support are unclear.[114] The Communist Party and the Social Democratic Party are both openly pro-Russian and previously have called for referendums on the EU and NATO.[115]

Disinformation Campaigns

Russia uses various recurring narratives in the Czech Republic, combined with political influence, in an effort to weaken national unity

---

[110] Marc Santora, "Czech Republic Re-Elects Milos Zeman, Populist Leader and Foe of Migrants," *New York Times,* January 27, 2018.

[111] Karen Friar, "5 Things to Know About the Billionaire 'Czech Donald Trump' Who Just Won a General Election," *MarketWatch,* October 23, 2017.

[112] For claims made by Anne Applebaum, see Anne Applebaum, "Russia's New Kind of Friends," *Washington Post,* October 16, 2015. For Babiš's rebuttal, see Andrej Babiš, letter to the editor, *Washington Post,* October 23, 2015.

[113] Friar, 2017; "Czech PM Andrej Babis Stripped of Immunity Amid Fraud Charges," BBC News, January 19, 2018; and Lily Bayer, "Czech Police Recommend Charges Against Prime Minister in Fraud Case," *Politico*, April 17, 2019.

[114] Anonymous, interview with the authors, Prague, February 2018.

[115] However, news sources indicated in 2018 that the Czech president and prime minister stressed that leaving the EU or NATO was not under discussion. See Chris Johnstone, "Czech PM and President Reassert EU and NATO Membership Commitment," Radio Praha, February 9, 2018.

and decisionmaking in the country, as well as to leverage Czech membership in the EU and NATO to undermine those institutions. Disinformation campaigns exploit existing biases and emotions in Czech society, including the following:

- *migration*, by promoting the narrative that migration is undermining the identity of the EU
- *Euroscepticism*, by promoting the idea that the Czech Republic would be better off outside of the EU and NATO[116]
- *"evil Germany" messages*, promoting the idea that the EU is dominated by German policies hostile to Czech interests[117]
- *traditional Czech skepticism about the government*, by fanning populist narratives about the ineffectiveness of the Czech government.

Czech interviewees estimated that between 40 and 50 "disinformation platforms" were operating in the Czech Republic.[118] These include websites, such as Sputnik and Aeronet; printed publications, such as *Vedomi*;[119] accounts on social media platforms, such as Facebook and YouTube; and cable television shows.[120] European monitors have identified at least 30 Czech language websites disseminating pro-Putin language and conspiracy theories on global political developments.[121] Conspiracy theories include a story that the Czech

---

[116] Anonymous, interview with the authors, Prague, February 2018.

[117] This tactic plays on a historic sentiment of "evil Germany." This message may be tied into the messages that focus on Euroscepticism.

[118] Anonymous, interview with the authors, Prague, February 2018. The interviewee cited several examples, noting that disinformation outlets are sometimes started as websites and later may also develop a printed version. For example, the *Vedomi* magazine was founded by AC24, a conspiracy theory website. *Parlamentní Listy* is another example; it was created in 2008 as a platform for all political parties, but it tends to post extreme positions.

[119] Ivana Smoleňová, *The Pro-Russian Disinformation Campaign in the Czech Republic and Slovakia,* Prague: Prague Security Studies Institute, June 2015.

[120] Anonymous, interview with the authors, Prague, February 2018.

[121] Anna Nemtsova, "The Next NATO Ally Russia Is Trying to Disrupt," *Daily Beast,* January 12, 2017.

government was covering up the existence of a "nuclear cloud" from France that was hovering over the Czech Republic,[122] as well as false claims of plans to affiliate the Czech Armed Forces brigade with the German Panzer division.[123] Information and rumors from these platforms is sometimes reproduced by mainstream media sources. Additionally, pro-Russian NGOs, such as the Institute of Slavic Strategic Studies, propagate disinformation in the Czech Republic. These organizations participate in pan-Slavic congresses, which serve as networking opportunities and further integration within the pro-Kremlin, informal club of NGOs.[124]

According to Kremlin Watch, a local Czech organization, 25 percent of the country's population of 10.5 million read disinformation sources.[125] Interviewees offered varying assessments of the effects of disinformation. One interviewee noted that Czechs are generally able to recognize disinformation campaigns.[126] Another noted that disinformation efforts have become more successful because of social problems, including lack of trust in the government and lack of satisfaction with

---

[122] Anonymous, interview with the authors, Prague, February, 2018; and EU vs Disinformation, "Europe Threatened by Nuclear Cloud," *Disinformation Review*, March 16, 2017. This message was relevant for the Czech Republic in light of the Chernobyl disaster (in Ukraine) and the crisis in Fukushima, Japan.

[123] Anonymous, interview with the authors, Prague, February 2018. According to our interviewee, this false information was used by the Communist Party in the Parliament and by "concerned citizens." It built on the sensitivity of the "German question" and the negative feelings toward Germans commanding Czech soldiers, stipulating that Czechs would no longer be able to be the decisionmakers. This disinformation was a surprise to the Czech Ministry of Defence because the Czech Armed Forces have existing close cooperation with the German Armed Forces via exercises with the Panzer division, which gives the Czech Army the opportunity to train at the division level. While cooperation exists, there are no legal or command and control implications for the Czech brigade, and the cooperation is included in the 2017 defense strategy (see Czech Ministry of Defence, *Defense Strategy of the Czech Republic*, Prague, 2017).

[124] Smoleňová et al., 2017.

[125] Philip Heijmans, "Europe's New Cold War: Fake News," *U.S. News and World Report,* January 18, 2017.

[126] Anonymous, interview with the authors, Prague, February 2018.

current values.[127] Interviewees also cited concern about the strength of independent media outlets, which are often attacked by politicians, the president, and various disinformation activities. For example, President Zeman, who has advocated nationalizing public television in the country, has drawn large street protests for his attacks on the Czech media.[128]

Energy Coercion

Although the Czech Republic uses coal for 35 percent of its overall energy supply and nuclear energy for 17 percent of the supply, nearly all of the country's natural gas and half of its crude oil originate from Russia, leaving the Czech Republic potentially vulnerable to Russian oil or natural gas embargos.[129] There were suspicions that Russia employed gray zone tactics in the energy sector following a decision by the Czech Republic to support a U.S. missile defense system in Europe in 2008.[130] Soon after the Czech announcement, the Russian oil pipeline firm Transneft cut Czech oil shipments by half and warned of further cuts. Although Moscow provided verbal assurances that the move was not political, citing technical problems with oil extraction, a Czech government spokesperson conveyed skepticism when he brought up the fact that neighboring countries faced no cuts.[131]

Cyberattacks

The Czech Republic has experienced significant cyberattacks in recent years on both government and civilian institutions. One interviewee identified cyberspace as a likely area of conflict between Russia and

---

[127] Anonymous, interview with the authors, Prague, February 2018.

[128] Český Rozhlas, "Czech President Attacks Public Television Broadcaster, Calls for Debate over Its Future," *Hello Czech Republic*, May 13, 2016; and "Czech Television Rejects Zeman's Attacks on Media," *Prague Daily Monitor,* March 9, 2018.

[129] According to the Organisation for Economic Co-operation and Development, about 30 percent of Czech natural gas is purchased via European spot markets and thus could come from alternative sources (Organisation for Economic Co-operation and Development, "Fossil Fuel Support Country Note: Czech Republic," Paris, April 2019).

[130] Andrew E. Kramer, "Czechs See Oil Flow Fall and Suspect Russian Ire on Missile System," *New York Times*, July 12, 2008.

[131] "Czechs Not Buying Russian Energy Claims," United Press International, July 15, 2008.

the Czech Republic, mentioning Estonia as an example of a European country that is enhancing cybersecurity and resilience through targeted policy decisions and programs.

The Czech Security Information Service reported "very active" cyberattacks against Czech government institutions in 2016.[132] One case involved the APT28 (also known as Fancy Bear) campaign in which computers outside of the country hacked the private email accounts of the Czech military. The report warned that "the misappropriated data and information may be used for various purposes, including political or industrial ends, discrediting specific persons or countries, and disinformation and blackmail."[133] Hackers also infiltrated emails of senior Czech diplomats in 2017. Foreign Minister Lubomír Zaorálek's email account was breached in a "sophisticated" operation suspected of being conducted by Russia.[134] In 2013, the Czech Republic experienced distributed denial-of-service attacks targeting bank websites, media outlets, mobile phone operators, the stock exchange, and even the Czech National Bank. Some victims traced internet protocol addresses to Russia, but others were traced elsewhere and no responsibility was ever assigned for the attacks.[135] Finally, an October 2017 cyberattack targeting the general parliamentary election shut down election websites of the Czech Statistical Office.[136]

How Has the Czech Republic Responded to Gray Zone Threats from Russia?

In the current Czech political environment, one major challenge in responding to Russian gray zone activity, according to one interviewee,

---

[132] Krystof Chamonikolas, "Czech Republic Says Russian Hackers Were 'Very Active' There in 2016," *Bloomberg,* October 24, 2017.

[133] Chamonikolas, 2017.

[134] Robert Tait, "Czech Cyber-Attack: Russia Suspected of Hacking Diplomats' Emails," *The Guardian,* January 31, 2017.

[135] B.C., "Cyber-Attack in the Czech Republic: Thieves in the Night," *The Economist,* March 13, 2013.

[136] "Cyber Security Office to Assist in Presidential Election," *Prague Monitor,* January 5, 2018.

is that any response will be limited if senior government leaders choose to ignore or deny the threat.[137] Except for some former defense officials, the Czech government has issued no strong statements to condemn Russian interference, for example.[138] Similarly, public responses from senior Ministry of Foreign Affairs personnel regarding the Nord Stream pipeline issue have been lukewarm.[139] However, the Czech government has undertaken several bureaucratic initiatives that appear to at least partially address gray zone threats from Russia, and we discuss these next.

National Security Audit

The Czech Ministry of the Interior led a national security audit in 2016, during which it evaluated the strengths and weaknesses of Czech defense and security policies, including those for resilience against foreign interference and influence.[140] The audit report highlighted the ongoing counterintelligence work of the Czech national security agency—which publishes an annual report analyzing Russian influence—and collected the analysis of 120 security and intelligence experts identifying vulnerabilities.[141] Two of the chapters were particularly relevant to gray zone threats: "Influence of Foreign Powers," drafted by the Interior Ministry, and "Hybrid Threats," drafted by the Defence Ministry. [142]

---

[137] Anonymous, interview with the authors, Prague, February 2018.

[138] For example, the former Chief of General Staff General Petr Pavel has been vocal.

[139] Anonymous, interview with the authors, Prague, February 2018. The Nord Stream pipeline was seen as a move by Russia to bypass traditional transit countries, such as Ukraine, Slovakia, the Czech Republic, Belarus, and Poland, which some Eastern European countries believed could expose transit countries to Russian influence by threatening gas supplies without affecting supplies to Western Europe. A Nord Stream 2 pipeline, which will follow essentially the same route, is under construction.

[140] Janda and Víchová, 2017.

[141] European Values, 2017.

[142] European Values, 2017.

Centre Against Terrorism and Hybrid Threats

In 2017, the Czech Interior Ministry established the Centre Against Terrorism and Hybrid Threats, which offers government departments analysis on internal security threats and helps combat disinformation through social media. Press reports and our interviews indicate that similar teams are planned at other ministries. Reviews of the center have been mixed. The decision to create it was initially controversial: Some claimed that "it would be similar to an Orwellian 'Ministry of Truth.'"[143] In the run-up to the 2017 parliamentary elections, the center received some criticism for issuing only a few corrective tweets amid a significant disinformation campaign.[144] One interviewee suggested that the Czech Republic still needed "good fact-checking."[145] However, another interviewee noted that the center was able to correct false information about a purported crime by a migrant within 24 hours. Overall, interviewees felt that the center represented an important development to help coordinate activities within the Czech government.[146]

Nongovernmental Initiatives

Nongovernmental entities, such as universities and NGOs, have taken some steps to build societal resilience to disinformation. Examples of nongovernmental activities include the following:

- People in Need *(Člověk v Tísni)* is a nonprofit organization that organizes workshops and provides educational courses at grammar and secondary schools to help teach about Communism and its impact.[147]

---

[143] Anonymous, interview with the authors, Prague, February 2018; and Jan Lopatka, "Czech 'Hybrid Threats' Center Under Fire from Country's Own President," Reuters, January 4, 2017.

[144] Rick Noack, "Czech Elections Show How Difficult It Is to Fix the Fake News Problem," *Washington Post,* October 20, 2017c.

[145] Anonymous, interview with the authors, Prague, February 2018.

[146] Anonymous, interview with the authors, Prague, February 2018.

[147] People in Need, Czech Republic, homepage, undated.

- Masaryk University students have established a program called Choose Your Info, which seeks to identify disinformation campaigns.[148]
- TOL Education, a Prague-based journalism trainer and publisher, provides courses on information verification.[149]

Although these initiatives were generally well received, more work is needed to address the challenge. Additional needs may include a long-term media literacy program, systematic training for public officials, and more international research and case comparison to educate the public about disinformation activities.[150]

Energy Supply Diversification

Czech government efforts at energy diversification have been mixed. A transnational oil pipeline from Germany, built by the Czech government in the 1990s, provides access to oil supplied from the Middle East and the North Sea.[151] However, the Czech government maintains long-term contracts with Gazprom for most of the country's natural gas through 2035.[152] The Czech Republic had planned a natural gas interconnector pipeline from Poland (Stork II), but the project was postponed.[153]

Cybersecurity

The primary government-level response to cyber threats has been the establishment of the National Cyber and Information Security Agency.[154] In August 2017, the institution detached from the National Security Authority after the Czech government tasked that agency with

---

[148] Anonymous, interview with the authors, Prague, February 2018.

[149] TOL Education, "Become an Expert Fact Checker and Hoax Buster!" course description, 2018.

[150] Anonymous, interview with the authors, Prague, February 2018.

[151] Kramer, 2008.

[152] Organisation for Economic Co-operation and Development, 2019.

[153] "There Are Plans and No Cheap Gas: How Poland Is Trying to Become a Gas Hub," *EurAsia Daily,* November 22, 2017.

[154] National Cyber and Information Security Agency, homepage, undated.

cybersecurity. The office operated in "emergency mode" during the January 12–13, 2018, presidential election, and had up to 25 cyber technicians ready to defend against cyberattacks.[155] The National Cyber and Information Security Agency includes a computer emergency response team; has established crypto standards; and coordinates with the Ministry of the Interior, the Ministry of Transport, and major private telecommunication companies (e.g., Telefónica).

The Czech government has engaged in a range of other cybersecurity initiatives, including a taskforce formed by the Foreign Ministry following the 2017 hack,[156] new courses on cybersecurity at the Czech University of Defence as of spring 2018,[157] and a push by the Czech Army to recruit personnel with cyber skills.[158] Beginning in 2016, the Czech military initiated cyber education programs at about 15 schools to raise awareness about national security; the programs provide training support to teachers and send mobile teams from the Army to speak to students.

Poland

Although gray zone activities were acknowledged as important in our discussions with Polish interlocutors, Poland's predominant concern continues to be the conventional threat posed by Russia in light of the permanent deployment of Iskander rockets in Kaliningrad, recent increases in Russian military capabilities in the region, military exercises at the Baltic states' borders, and ongoing Russian military activity in Ukraine.[159] Some interviewees expressed a concern that Russia's threshold for military action has lowered in recent years, while others argued that Russia was unlikely to cross the NATO Article V threshold

---

155 "Cyber Security Office to Assist in Presidential Election," 2018.

156 Tait, 2017.

157 "Cyber Security to Be Newly Taught at Czech Army's University," *Prague Daily Monitor,* March 5, 2018.

158 Anonymous, interview with the authors, Prague, February 2018.

159 Anonymous, interview with the authors, Poland, 2018.

prompting collective self-defense, instead relying on more-ambiguous tactics in an effort to confuse decisionmakers about the character of Russia's actions.[160] Conversations with Polish experts and officials invariably turned to the need to strengthen conventional deterrence in Poland and the wider Baltic region, as well as to ensure energy and economic independence.

This section addresses four categories of gray zone tactics used by Russia to gain influence or sow discord: military intimidation, cyberattacks, energy and infrastructure coercion, and disinformation campaigns.

Types of Gray Zone Threats Faced by Poland

Military Intimidation

Poland's threat perception aligns more closely with that of the Baltic states than with Poland's fellow "Visegrad Four" countries (the Czech Republic, Hungary, and Slovakia).[161] Poland's 2016 Strategic Defence Review notes that the security challenges from Russia had been adequately addressed in the past, prompting a clear assessment of traditional and hybrid threats and Poland's ability to defend its own territory.[162] Polish officials from across the political spectrum are predominantly focused on military threats, and those whom we interviewed appeared to be acutely aware that Poland lies on what could be the front line of a conflict with Russia. Russian military activities and verbal threats from Russian leaders have contributed to this perception. These activities include the following:

- Statements by Putin in 2016 that Poland and Romania would be in Russia's "crosshairs" due to their decision to host U.S. missile defense elements.[163]

---

[160] Anonymous, interview with the authors, Poland, 2018.

[161] For more on the Visegrad Four, see Visegrad Group, "About the Visegrad Group," webpage, undated.

[162] Ministry of National Defence of Poland, *The Concept of Defence of the Republic of Poland*, Warsaw, May 2017.

[163] Denis Dyomkin, "Putin Says Romania, Poland May Now Be in Russia's Cross-Hairs," Reuters, May 27, 2016.

- Reported movement of additional Iskander ballistic missile systems to Kaliningrad in response to U.S. forces in Poland.[164]
- Large-scale Russian military drills near Poland's borders. In 2017, Russia's Zapad exercise included 100,000 troops and involved firing nuclear-capable ballistic missiles and the participation of electronic warfare units.[165] The drills, which simulated a conflict with NATO, appear orchestrated to demonstrate Russia's ability to rapidly mass large numbers of troops with Poland as a possible target.[166]

Cyberattacks

Poland has experienced a series of cyberattacks against both military and civilian targets in recent years. In these attacks, the perpetrators sought to access data, potentially immobilize critical infrastructure, and conduct phishing attacks.[167] The attacks highlighted Polish cyber vulnerabilities, as well as the potential for serious crisis if these vulnerabilities are not managed properly.[168] Recent examples of cyberattacks in Poland include the following:

- In October 2017, the Ministry of National Defence reported that hackers had attempted to install malware on its information technology systems in order to access data. Polish leaders also believed that the attack could represent an attempt to access and

---

[164] Samuel Osborne, "Russia Deploys Nuclear-Capable Missiles to Border with Poland and Lithuania," *The Observer,* February 7, 2018.

[165] Anna Maria Dyner, "The Importance of the Zapad 2017 Exercises," Polish Institute of International Affairs, Bulletin No. 86 (1026), September 21, 2017.

[166] Robin Emmott, "Russia's Zapad War Games Unnerve the West," Reuters, September 13, 2017.

[167] CERT Polska, *Security Landscape of the Polish Internet,* Warsaw, Poland, 2016.

[168] Joanna Świątkowska, Izabela Albrycht, and Dominik Skokowski, *National Cyber Security Organisation: Poland*, Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence, 2017.

potentially immobilize critical infrastructure, which could lead to "paralysis in the functioning of the state."[169]

- The Polish Stock Exchange and the Warsaw airport were reportedly targeted in 2014 and 2015, respectively, disrupting operations and, in the case of the Warsaw airport, grounding planes and stranding passengers.[170] Interviewees also cited broader cyberattacks on Polish businesses and individuals, although it has proven difficult to attribute these attacks to anyone.[171]
- As Warsaw hosted the NATO summit in 2016, a cyberattack targeted the Polish banking system, and a web-based disinformation campaign suggested that Polish Ministry of National Defence employees were involved in a secret U.S. spy program.[172]
- In January 2017, the websites of two municipalities hosting U.S. troops were attacked with pro-Russian and anti-NATO content, including an attempt to smear the image of Poland's allies.[173]

Energy and Infrastructure Coercion

Energy dependence—specifically, dependence on raw materials for oil and gas production in domestic refineries—is viewed as a key vulnerability in Poland.[174] For example, as of 2016, 83.7 percent of crude oil imports, 74.3 percent of natural gas imports, 60.6 percent of coal

---

[169] "Poland Targeted by Spate of Cyberattacks: Defence Minister," Radio Poland, October 18, 2017.

[170] Anonymous, interview with the authors, Poland, 2018; Cory Bennett, "Hackers Breach the Warsaw Stock Exchange," *The Hill,* October 24, 2017; and Wiktor Szary and Eric Auchard, "Polish Airline, Hit by Cyber Attack, Says All Carriers Are at Risk," Reuters, June 22, 2015.

[171] Anonymous, interview with the authors, Poland, 2018.

[172] CERT Polska, 2016.

[173] Pawel Sobczak and Lidia Kelly, "Attacks on U.S.-Linked Polish Sites Back Higher Cyber Spending: Minister," Reuters, March 15, 2017.

[174] Igor Protasowicki, Slawomir Czepielewski, Krzysztof Ksiezopolski, and Witold Jurasz, *Bezpieczenstwo Energetyczne RP,* Warsaw, Poland: Narodowe Centrum Studiów Strategicznych, 2016.

imports, and 37.3 percent of oil product imports came from Russia.[175] This leaves Poland vulnerable to coercive acts by Russia to disrupt Poland's energy supply under the guise of innocuous "technical malfunctions of supply networks."[176] Poland views Russian development of the Nord Stream 2 pipeline with concern, as it is a potential source of future leverage against Western governments.[177] As noted earlier, opponents of the Nord Stream 2 pipeline are worried that Russia could use it to threaten the gas supply of traditional transit countries, including Poland and Ukraine, as well as increase Russia's economic influence on Western European countries.[178] Although Russia has not exploited this dependence using gray zone means, this is an ever-present concern in the Polish national security establishment.[179]

Finally, interviewees cited one potential example of infrastructure sabotage in which the Łazienkowski Bridge in Warsaw burned under undetermined circumstances, making it unusable for more than a year. Warsaw has a shortage of bridges, and the interviewee believed that the incident could have been a way of testing infrastructure resilience in Poland.[180]

Disinformation Campaigns

Polish analysts note that Russian media plays a relatively minor role in Poland, despite efforts to expand its presence, and that internet-based sources propagating anti-Western or pro-Russian disinformation have a limited but expanding audience.[181] Unlike in the Czech Republic,

---

[175] International Energy Agency, *Energy Policies of IEA Countries: Poland 2016 Review*, Paris, January 25, 2017.

[176] Anonymous, interview with the authors, Poland, 2018.

[177] Anonymous, interview with the authors, Poland, 2018; and "Polish President Andrzej Duda Calls for Stop to Nord Stream 2 Gas Pipeline," *Deutsche Welle*, October 23, 2018.

[178] Anonymous, interview with the authors, Poland, 2018; and Konrad Szymanski, "Russia's Gas Pipeline Threatens European Unity," *Financial Times*, October 21, 2016.

[179] Anonymous, interview with the authors, Poland, 2018.

[180] Anonymous, interview with the authors, Poland, 2018. For more about the Łazienkowski Bridge, see "Warsaw's Łazienkowski Bridge up in Flames," Radio Poland, February 14, 2015.

[181] Smoleňová et al., 2017.

Poland has no major political party or prominent think tank that advocates closer relations with Russia. However, Poland's democratic backsliding leaves it more vulnerable to gray zone tactics, given a weakened independent media, lower trust in government, and the rise of radical political movements.[182] Nonetheless, interviewees cited disinformation efforts by Russia to portray U.S. soldiers in a negative light, but they also noted that, because of the high levels of support for the U.S. military presence and a general understanding of the reasons for that presence, these disinformation activities had not been successful.[183]

How Has Poland Responded to Gray Zone Threats from Russia?

Military Enhancements

Poland's 2016 Strategic Defence Review sought to address threats from Russia, emphasizing territorial defense and the modernization of the military's intelligence aircraft, missile defense systems, and electronic warfare capabilities.[184] The document was noteworthy because it recognized the structural and equipment-related challenges in the Polish armed forces. To address concerns about the conventional threat posed by Russia, the Polish Ministry of National Defence has taken several measures to enhance Poland's military capabilities, including the following:

- A new part-time military force to combat potential hybrid attacks on Polish territory. The force is composed of 17 brigades, called the Territorial Defence Force, and will include 53,000 volunteer and professional members by the time it is fully stood up.[185] The force's missions include protecting key infrastructure, countering

---

[182] Peter Jančárik, Adam Reichardt, Roman Shutov, and Ivana Smoleňová, eds., *Countering Pro-Russian Disinformation: Current Challenges and the Way Forward,* seminar summary, Prague: Prague Security Studies Institute, May 31, 2016.

[183] Anonymous, interview with the authors, Poland, 2018.

[184] Aaron Mehta, "In Russia's Zapad Drill, Poland Sees Confirmation of Its Defense Strategy," *Defense News,* December 6, 2017.

[185] "Poland Plans Paramilitary Force of 35,000 to Counter Russia," BBC News, June 3, 2016.

disinformation and sabotage, and helping stabilize situations of crisis and martial law.[186]
- New arms deals, including for rocket artillery and Patriot batteries from the United States in 2017 and 2018.[187]

Poland has prioritized its role as host of 3,000 U.S. troops, which serve as part of Poland's Enhanced Forward Presence battalion within NATO. The battalion in Poland is recognized as a positive step for bolstering deterrence in the region. Most Poles reportedly feel safer with the U.S. and NATO presence in Poland.[188] The fact that Exercise Anaconda 2018 was held in Poland in summer 2018 is also viewed as a positive sign that Poland is contributing to NATO deterrence in Eastern Europe. Polish National Defence Minister Antoni Macierewicz, said that "due to the complex geopolitical situation on the eastern flank of NATO, this exercise should be a deterrent and demonstrate [the] alliance's might."[189]

Cybersecurity

Poland's responses to increasing cybersecurity encompass both the military and civilian domains. In October 2017, the Polish government announced that it would spend about 1 billion zlotys (or about U.S. $250 million) a year on cybersecurity, which is several times the amount previously spent.[190] Management and responsibility for cybersecurity is shared between the Ministry of Digital Affairs and the Ministry of National Defence. Dedicated agencies and teams are in place to respond to cyber incidents; these parties include the Government Computer Security Incident Response Team (established in 2008),

---

[186] Charlie Gao, "This Is How Poland Plans to Fight Russia in a War," *National Interest*, March 8, 2018.

[187] Lidia Kelly, "Poland Signs $4.75 Billion Deal for U.S. Patriot Missile System Facing Russia," Reuters, March 28, 2018.

[188] Anonymous, interview with the authors, Poland, 2018.

[189] Jan Radziunas, "Anaconda 2018 Exercise in Poland Is a Preparation for War," *Modern Diplomacy,* December 13, 2017.

[190] Sobczak and Kelly, 2017.

which performs emergency responses, and the Polish Military Computer Incident Response Team.

In the military domain, the Polish armed forces are establishing new defensive and offensive cyber roles and organizations, including, in 2012, a special position called the plenipotentiary of the Minister of National Defence responsible for the security of cyberspace and, in 2013, the National Cryptology Centre, which coordinated the ministry's cyber protection efforts.[191] Furthermore, the Armed Forces Technical Modernization Program for 2017–2022 specifically prioritizes the need to develop cyber-related capabilities.[192] Finally, interviewees noted that Poland's armed forces had initiated a process in 2015 to develop capabilities to counter information warfare.[193]

Georgia

In contrast to the other case studies in Western and Eastern Europe, Georgia stands out as a distinct target of Russian gray zone actions. Since the 2008 conflict with Russia, Russia has consolidated control over Abkhazia and South Ossetia and employed tactics that have challenged Georgia's ability to administer this territory. For the gray zone activities described in this section, we focus predominantly on the perceived risk of a creeping Russian annexation of these occupied regions, but we also consider Russian information operations, cyberattacks, and energy coercion against Georgia.

[191] Dziennik Urzedowy Ministra Obrony Narodowej, "W sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni," Decyzja Nr 38/MON, 2012.

[192] Świątkowska, 2017.

[193] Anonymous, interview with the authors, Poland, 2018.

Types of Gray Zone Threats Faced by Georgia

Territorial Expansion

In the decade since the August 2008 conflict,[194] Russia has taken measures to solidify control over Abkhazia and South Ossetia.[195] In 2017, around 4,000 Russian troops occupied the 7th Military Base in South Ossetia and another 4,000 occupied the 4th Military Base in Abkhazia.[196] Russia also maintains military equipment at both bases, including S-300 air defense systems in Abkhazia that contribute to Russian counterintervention capabilities over the Black Sea.[197] Over the years, Russian and South Ossetian security forces have slowly moved the South Ossetian boundary line—which they claim as an international border—deeper into Georgia's previously undisputed territory.[198] Some have speculated that this could be an effort to align the South Ossetian boundary with the former Soviet administrative borders.[199]

---

[194] Prior to August 2008, Russia maintained what it called peacekeeping forces in the separatist regions of Abkhazia and South Ossetia after brokering a 1992 ceasefire agreement between South Ossetia and Georgia. For additional history and details on the 2008 conflict, see Jim Nichol, *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests,* Washington, D.C.: Congressional Research Service, RL34618, March 3, 2009.

[195] In 2016, the *New York Times* reported that

> the nominally independent country [South Ossetia] is already Russian territory in all but name. It has its own small security force, but its self-declared frontiers are mainly guarded by Russia's border service, an arm of the Federal Security Service, the post-Soviet version of the K.G.B. It houses three Russian military bases with several thousand troops and, with no economy beyond a few farms, depends almost entirely on Russian aid for its survival. (Andrew Higgens, "In Russia's 'Frozen Zone,' a Creeping Border with Georgia" *New York Times,* October 23, 2016)

[196] Giorgi Menabde, "Russian Military Absorbs 'Army of South Ossetia,'" *Eurasia Daily Monitor*, Vol. 14, No. 38, March 21, 2017; and David Batashvili, "Russia Troop Deployments Menace Georgia," *Civil Daily News Online*, April 4, 2017.

[197] Dmitry Solovyov, "Russia Deploys Missiles to Protect Georgia Rebels," Reuters, August 11, 2010.

[198] Higgins, 2016.

[199] Higgins, 2016.

One interviewee emphasized that Russia could well have solidified the boundaries of the occupied regions soon after the 2008 invasion, but it is choosing instead to move slowly and discretely in order to destabilize and test the resolve of the Georgian government—and without prompting a major military response.[200] The interviewee noted that this strategy has been a key source of social and political discord in Georgia: Every time a village is divided or someone is abducted at the border, such actions prompt protests and internal division in Georgian policymaking circles.[201]

To solidify control over disputed territories in Georgia, Russia also seeks to create joint military agreements, such as its ratified agreement with the de facto leaders in Georgia's breakaway region of South Ossetia in 2018.[202] The move, which was condemned as invalid in a statement by the U.S. State Department, sought to tighten Russian military control under the guise of a formal bilateral defense pact with separatists in South Ossetia.[203] President Putin echoed past agreements, such as unifying Abkhazian and Russian forces under Russian leadership in November 2016.[204]

In addition to military agreements, Russian authorities continue to incentivize residents in these territories to apply for passports

---

[200] Senior Georgian official, interview with the authors, March 21, 2018.

[201] Senior Georgian official, interview with the authors, March 21, 2018.

[202] "U.S. Condemns Russian Military Deal with Georgian Breakaway Region," Radio Free Europe/Radio Liberty, January 26, 2018.

[203] According to one Georgian military analyst, who was interviewed by the *Eurasia Daily Monitor,*

> Moscow wants to ensure that armed formations formally independent of Russian generals are not created in either South Ossetia or Abkhazia. . . . Russia considers the local armed groups to have already "done their job" by having provoked the conflict of 2008 by attacking Georgian villages and Georgian peacekeepers; it no longer makes any sense [for Moscow] to maintain these local armed forces' formal "independence" from the Russian army. (Menabde, 2017)

[204] "Georgia, U.S. Criticize New Russian-Abkhaz Military Force," Radio Free Europe/Radio Liberty, November 23, 2016.

for South Ossetia and Abkhazia, which requires the individuals to renounce their Georgian citizenship.[205]

Finally, Russian Federal Security Service (FSB) officers regularly carry out arbitrary detentions for so-called illegal border crossings along the occupation lines with the Abkhazia and Tskhinvali regions, and detention periods can last up to several months.[206] In a case described by one interviewee, a retired Georgian soldier who had served in Iraq was travelling across the Abkhazian boundary line for business and was detained, tortured, and killed.[207] The case became a rallying cry for criticism of the current government's handling of the creeping annexation challenge.

Information Operations

All interviewees cited the prevalence of Russian information operations throughout Georgian society but appeared to agree that such efforts have achieved only limited success. Channels for Russian disinformation efforts in Georgia include social media, NGO groups that travel throughout the Georgian countryside, and media outlets that openly propagate pro-Russian material. Disinformation campaigns are tailored by region. For example, in southern regions, there are false claims

---

[205] According to the Ministry of Foreign Affairs of Georgia,

> in June 2015, the Tskhinvali occupation regime began accepting applications for so called "South Ossetian passports," which required individuals [to] renounce their Georgian citizenship. . . . As for the Abkhazian region, during the reporting period a process of so called "passportisation" was underway in the occupied Abkhazia. The above process implies procession of 300 thousand new documents—250 thousand so called "passports" and 50 thousand so called "residence permits." All 300,000 documents were processed in the Russian Federation. (Ministry of Foreign Affairs of Georgia, *First Quarterly Report (January–March 2017) of the Ministry of Foreign Affairs of Georgia on the Human Rights Situation in the Occupied Regions of Georgia*, Tbilisi, Georgia, 2016, pp. 5–6)

[206] Per the Ministry of Foreign Affairs of Georgia,

> On 4th and 5th January 2016, a resident of the village of Bershueti, Gori district and a resident of Tbilisi were detained by the Russian FSB officers for so called "illegal border crossing". On 4th January 2016, two residents of the village of Bershueti, Gori district were detained by eight Russian FSB officers when they were entering the local church for religious ritual. (Ministry of Foreign Affairs of Georgia, 2016, pp. 7–8)

[207] Senior Georgian official, interview with the authors, March 21, 2018.

propagated on social media that if Georgia were to join NATO, Turkey would establish a military base on Georgian soil. In more socially conservative areas in Georgia, information operations emphasize the EU's more-liberal positions on gay marriage.[208]

Cyberattacks

Interviewees noted Russia's use of cyber capabilities before and during the 2008 conflict. Unattributed cyberattacks against Georgia began weeks before the August 2008 conflict, including distributed denial-of-service attacks that shut down Georgian servers.[209] Russia's use of cyber capabilities during the conflict acted as a force enabler; for example, denial-of-service attacks disabled government communications and disrupted Georgian banks, transportation companies, and private telecommunication providers.[210]

Energy Coercion

Energy coercion was cited as a key form of Russian pressure in the aftermath of the Rose Revolution, or the peaceful change of power in Georgia in November 2003. Georgia's gas prices rose by nearly 500 percent between 2004 and 2006, in contrast to other post-Soviet states closer to Russia.[211] One interviewee highlighted a winter 2006 pipeline explosion—which Russia was believed to have caused—that made Georgia entirely reliant on Russian gas.[212] As noted in the next section, the Georgian government moved quickly to diversify its energy supply and reduce its vulnerability in this area.

---

[208] Senior Georgian official, phone interview with the authors, February 27, 2018.

[209] John Markoff, "Before the Gunfire, Cyber Attacks," *New York Times*, August 12, 2008.

[210] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare*, Arlington, Va.: CNA, Occasional Paper Series, DOP-2016-U-014231-1Rev, March 2017.

[211] Randall E. Newnham, "Oil, Carrots, and Sticks: Russia's Energy Resources as a Foreign Policy Tool," *Journal of Eurasian Studies*, Vol. 2, No. 2, July 2011; and Andrew Osborn, "Moscow Accused of Using Gas Prices to Bully Georgia," *The Independent*, November 3, 2006.

[212] "Blasts Cut Georgia Gas, Electricity Supplies," CNN, January 22, 2006.

How Has Georgia Responded to Gray Zone Threats from Russia?

Peaceful Appeals to Occupied Regions

Since the 2008 conflict with Russia, the Georgian government has focused on nonmilitary measures to persuade Abkhazians and South Ossetians that their future lies as citizens of Georgia, not Russia. One current senior Georgian official described the approach as a "focus on populations, not territory."[213] The official noted that reconciliation between the populations would be necessary even in the absence of Russian interference. In order to achieve reconciliation, the Georgian government is offering the populations of Abkhazia and South Ossetia visa-free travel to Europe and universal health care, including to former separatist fighters, if they are willing to acquire or maintain Georgian passports. The policy, labeled the Georgia Peace Initiative, has been supported by the U.S. State Department, for example.[214]

Another senior Georgian official underscored that successive Georgian government administrations have expressed public commitment to peaceful resolution of the disputes with Abkhazia and South Ossetia. Negotiations between Georgia and Russia over former nonaggression pacts deteriorated in April 2018.[215] Although unilateral Georgian pledges have arguably been ineffective in combating Russian gray zone activity, given the persistence of such activities on the border of the occupied regions, the pledge has proven important in maintaining

---

[213] Senior Georgian official, phone conversation with the authors, February 28, 2018.

[214] Heather Nauert, "United States Welcomes Georgia Peace Initiative," Washington, D.C.: U.S. Department of State, Office of the Spokesperson, April 4, 2018

[215] Accounts of the April 2018 breakdown in negotiations vary, but one enduring challenge has centered on Russian insistence on the "signing of formal nonaggression pacts between Georgia and the two breakaway polities. Tbilisi has dismissed that demand, arguing that it is Russia, rather than Abkhazia or South Ossetia, that poses a threat to regional peace and stability" ("Has Russia Called Georgia's Bluff over Stated Desire to Improve Relations?" Radio Free Europe/Radio Liberty, March 16, 2018).

support from the United States and Europe, which Georgia views as critical to its long-term security objectives.[216]

Finally, the Georgian government seeks to maintain Western attention on the ongoing Russian gray zone activities in and around Abkhazia and South Ossetia. Specific steps have included

- a parliamentary resolution identifying Russians and local citizens involved in recent detentions and killings in the occupied regions[217]
- ongoing work on a hearing with the U.S. Helsinki Commission[218]
- quarterly reports about the ongoing dispute posted on the Ministry of Foreign Affairs website.[219]

Cybersecurity

Georgia has been proactive in responding to the cyber threat posed by Russia. In the wake of the 2008 crisis, Georgia sought advice from Estonian cyber defense advisers and moved some of its operations to private servers in the United States to offset cyber intrusions from Russia.[220] In 2010, the Georgian government launched the Data Exchange

---

[216] In March 2018, a U.S. representative explicitly praised Georgia's approach to the occupied territories, stating that,

> For almost 10 years, Russia has sought to create an alternate reality. While Georgia seeks opportunities for engagement with people living in Abkhazia and South Ossetia, Russia maintains relations with two fictitious countries as a ruse to control and occupy regions of a neighboring sovereign state. We will continue to use the Permanent Council and other fora to hold Russia accountable for its violation of international law, and to expose Russia's attempts to distort the truth and rewrite history. The United States urges Russia to withdraw its forces to pre-war positions per the 2008 ceasefire agreement and reverse its purported recognition of the Georgian regions of Abkhazia and South Ossetia as independent States. (Michele Siders, "Response to Georgian Deputy Foreign Minister David Dondua," Vienna: U.S. Mission to the Organization for Security and Cooperation in Europe, April 12, 2018, p. 2)

[217] Senior Georgian official, interview with the authors, March 21, 2018.

[218] Senior Georgian official, interview with the authors, March 21, 2018.

[219] Ministry of Foreign Affairs of Georgia, homepage, undated.

[220] On August 8, 2008, while in Georgia, the owner of TSHost apparently contacted Georgian government officials and offered assistance in reconstituting Georgia's internet capabili-

Agency with a computer emergency response team. According to a 2011 briefing, the agency successfully identified and mitigated a range of cyberattacks during its first year of operation, including a bot attack on military computers, bot activity from a major Georgian internet host, an attack on a Georgian government ministry, and local denial-of-service attacks.[221]

Energy Supply Diversification

The previous and current Georgian governments have also taken aggressive steps to reduce Georgian dependence on Russian gas. In 2006, Georgia started purchasing gas from Azerbaijan and acting as a key transport hub from Azerbaijan to European buyers, which helps these countries diversify away from Russia.[222] By January 2018, Georgian authorities announced that almost all of Georgia's gas demand would be met by Azerbaijan, thereby ceasing all gas imports from Russia.[223]

Efforts to Combat Information Warfare

Following the 2008 conflict with Russia, the Georgian government under President Mikheil Saakashvili banned Russian propaganda organs, which included cutting cable access to Russian media channels. The government has reversed that policy in recent years, leading to criticisms that the "door has been reopened" to Russian information operations.[224] One interviewee, in his previous government position, citied recent government efforts to counter Russian misinformation campaigns, including a program of direct engagement with leaders of

---

ties. A day later, the Georgian government transferred critical cyber capabilities to TSHost servers in the United States, including the websites of Georgia's president and the Ministry of Defense. See Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Vol. 38, No. 4, Winter 2009.

[221] Irakli Lomidze, "Cyber Attacks Against Georgia," briefing slides, Tbilisi, Georgia: Ministry of Justice of Georgia, Data Exchange Agency, 2011.

[222] C. J. Chivers, "Georgia Reopens Old Gas Line to Ease Post-Blast Shortage," *New York Times*, January 24, 2006a.

[223] Thea Morrison, "Georgia Not to Purchase Gas from Russia in 2018," *Georgia Today,* January 9, 2018.

[224] Former senior Georgian official, interview with the authors, March 24, 2018.

Georgian Orthodox churches across the country—typically a major outlet of Russian disinformation. The relationship sought to open new channels of communication between the Orthodox Church and the Georgian government to clear up misunderstandings and increase mutual trust.[225]

Overall Findings: Field Research in Europe

Russian gray zone activities against the countries examined in this report in Western and Eastern Europe consist primarily of disinformation campaigns meant to undermine political institutions. Such activities are manifested in

- the hacking of political campaigns, which is designed to damage the reputation of candidates in democratic elections in favor of candidates who are regarded in Moscow as holding pro-Russian views
- the creation of bots on social media or the use of media channels to propagate false information meant to sow discord or confusion
- the dissemination of rumors or false information meant to undermine the cohesiveness of NATO or the EU
- the use of cyber weapons to steal information from governmental institutions or influence the efficient flow of communications within government organs.

Other Russian gray zone tactics include the use of economic tools to extract concessions or hold countries at risk of being coerced through an overreliance on Russian energy; the demonstration of military threats through exercises near the borders of certain states; and, in the case of Georgia, the infiltration of Russian security forces to exert de facto control over disputed territory within the border of another state.

The overall strategy of states seeking to undermine or influence other states through political subversion is not altogether new or

[225] Senior Georgian official, interview with the authors, March 21, 2018.

unprecedented. What is new, however, are the tactics and tools at Russia's disposal. Democratic institutions, even ones regarded as stable and well protected, such as those in France and the United States, are no less vulnerable to Russian interference than less-stable institutions. The sophistication of tactics and the obfuscation of Russian state involvement have only increased over time, giving Russia a freer hand to devise variations of tactics used in the past and giving it an advantage over countries attempting to prevent such attacks from occurring.

Compared with the gray zone tactics in Asia emanating from China (discussed in the next chapter), which take on a more materially threatening form, the ephemeral manner in which gray zone tactics from Russia are prosecuted—at least at the moment—makes the policy response arguably more challenging. The long-term challenge for European states hoping to fashion policies that confront Russia's gray zone activities will be to prioritize timely and proportional whole-of-government counter-responses that deter future tactics without escalating to new thresholds of conflict that may lead to war.

CHAPTER FOUR

Findings from Field Research on Gray Zone Challenges in Asia

This chapter offers the key findings from field research that we conducted in Japan, Vietnam, the Philippines, Indonesia, Singapore, and Australia in 2017 and 2018. In each case, we examine the gray zone threat or challenge faced by the regional actor and the responses the nation is undertaking to deal with it. These responses include political, economic, and military measures designed to counteract Chinese efforts to impose outcomes and gain predominant influence.

As we describe in more detail later, we identified several primary lessons from this research. In Northeast Asia, Japan believes that it is engaged in an increasingly high-stakes competition with China over efforts to change the status quo of territorial sovereignty and administrative control of the Senkaku Islands and nearby areas—a competition that Japanese leaders believe they are partly managing, at least for the time being, by deterring CCG from escalating its activities and successfully expelling Chinese fishing boats that enter the Senkaku Islands' territorial waters without incident. Yet the trends do not bode well for Japan: CCG patrols have begun to feature the presence of vessels that are more heavily armed, and the Chinese maritime militia continues to penetrate the Senkaku territorial sea with increasing regularity. Although Japan can continue to play defense against Chinese probing tactics, a change in strategy by China in favor of more, better-armed, and more-provocative penetrations by CCG and maritime militia vessels could potentially strain Japan's capacity to respond without increasing the potential for armed conflict.

In Southeast Asia, countries in the region have grown increasingly wary of Chinese gray zone aggression in the SCS. These activities include the use of law enforcement and a maritime militia in an unprofessional and escalatory manner to deter or, in some cases, actively deny the use of living and nonliving resources in the SCS. Officials and scholars in the affected countries highlighted such tactics as bumping, shouldering, and ramming, as well as using water cannons, by CCG against other nations' coast guard and fishing vessels. China's unprecedented expansion of artificial islands in the SCS and subsequent construction of logistics, maintenance, and storage facilities, along with airstrips, harbors, ports, and armament platforms, are in the process of further tilting the regional military balance in favor of China. Finally, China has supplemented these security-oriented aspects of its gray zone strategies with growing employment of economic coercion and political subversion.

Our research in these countries confirmed that they have identified the challenge from Chinese gray zone activities and seek to deter further attacks when feasible and appropriate. But there are significant limits on their ability to deal with the challenge on their own. They remain constrained by their military capacity to deter Chinese military and paramilitary activities, for example. Even more fundamentally, the nonaligned foreign policy orientations of many regional actors and their accompanying desire to strike a tenuous balance of deterrence and engagement with China are preventing more-forceful displays of confrontation.

Japan

Territorial disputes with Japan in the ECS have been a significant focus of China's gray zone efforts. China poses gray zone challenges in the maritime and air domains in Japan's southwest island chain, particularly near the Senkaku Islands (called *Diaoyu* in Chinese), which are administered by Japan but also claimed by China and Taiwan. Since the Japanese government nationalized three features in the Senkakus in September 2012, China has adopted enhanced military,

paramilitary, diplomatic, and political campaigns to alter the status quo of the islands in Beijing's favor and inject doubt over administrative control over the waters surrounding these islands. Through the use of coast guard and maritime militia assets, China has undertaken near-constant deployments since 2012 to challenge Japanese administrative control and test Japan's will to respond. These moves represent a challenge to Japanese maritime forces to respond to every incursion that takes place.

Most Japanese officials believe that China will not try to seize the islands by force for the foreseeable future. This is rooted in an understanding that China fears the high political and military costs that such an action would induce. Japan thus far has been able to successfully counter Chinese attempts to alter the status quo by monitoring, shadowing, and warning off Chinese intrusions into the territorial seas of the Senkakus. The keys to maintaining the status quo are (1) a capable coast guard fleet and strong Japan Self-Defense Forces (JSDF) that can provide continuous Japanese presence around the islands and (2) a strong U.S.-Japan alliance.

Types of Gray Zone Threats Faced by Japan

Paramilitary Activities

Although the Senkaku Islands have been a friction point between Beijing and Tokyo since China asserted territorial sovereignty over the islands in 1971, the issue did not become an operational challenge until 2010. On September 7, 2010, a Chinese fishing trawler deliberately rammed two Japan Coast Guard (JCG) ships. In response, JCG arrested the captain and detained him under Japanese law. China retaliated economically and diplomatically.[1] More alarming, Chinese state-owned ships made multiple intrusions into the contiguous zone around the Senkaku Islands over subsequent months.[2] In September 2012, relations further deteriorated after Tokyo purchased three of the

[1] Green et al., 2017, pp. 66–94.

[2] Japan Ministry of Foreign Affairs, "Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response," webpage, April 5, 2018.

islands from their private Japanese owner.[3] The action triggered a surge of Chinese activity in the water and airspace around the islands. Ever since, CCG ships have become a regular presence in Japan's contiguous zone and territorial waters (Figure 4.1). Initially, this presence conformed to a 3-3-2 pattern: three times a month, three ships enter territorial waters for roughly two hours.[4] In autumn 2016, however, China increased the number of ships entering the territorial waters from three to four, resulting in a 3-4-2 pattern. The ships have also gotten bigger, and now one ship always carries weapons.[5]

Although these ships generally refrain from the gray zone activities seen in the SCS, such as ramming or using water cannons to repel JCG or Japanese fishing vessels, their presence in Japan's contiguous zone and territorial waters is meant to demonstrate China's sovereign control over the Senkaku Islands. This is because the ships' stated operational intent is to conduct law enforcement missions.[6] This supports Beijing's intention to assert a new operational normal in the gray zone.[7]

China's gray zone challenge is not limited to the employment of CCG assets. Chinese fishermen also challenge Japan's administrative control. It is believed that many of these fishermen are part of the maritime militia, but they are dressed in civilian clothing to disguise their affiliation. Additionally, there is a belief that many of these fishing vessels are equipped with communication devices that enable them to talk to CCG and PLAN units operating in the area. The most prominent example occurred over four days in August 2016. Between 200 and 300 Chinese fishing vessels swarmed the waters around the Senkakus.

---

3 The purchase included Uotsuri, Kita-kojima, and Minami-kojima. The United States still leases the other two islands—Kuba and Taisho. The three remaining islets or rocks remain in the ownership of the central government.

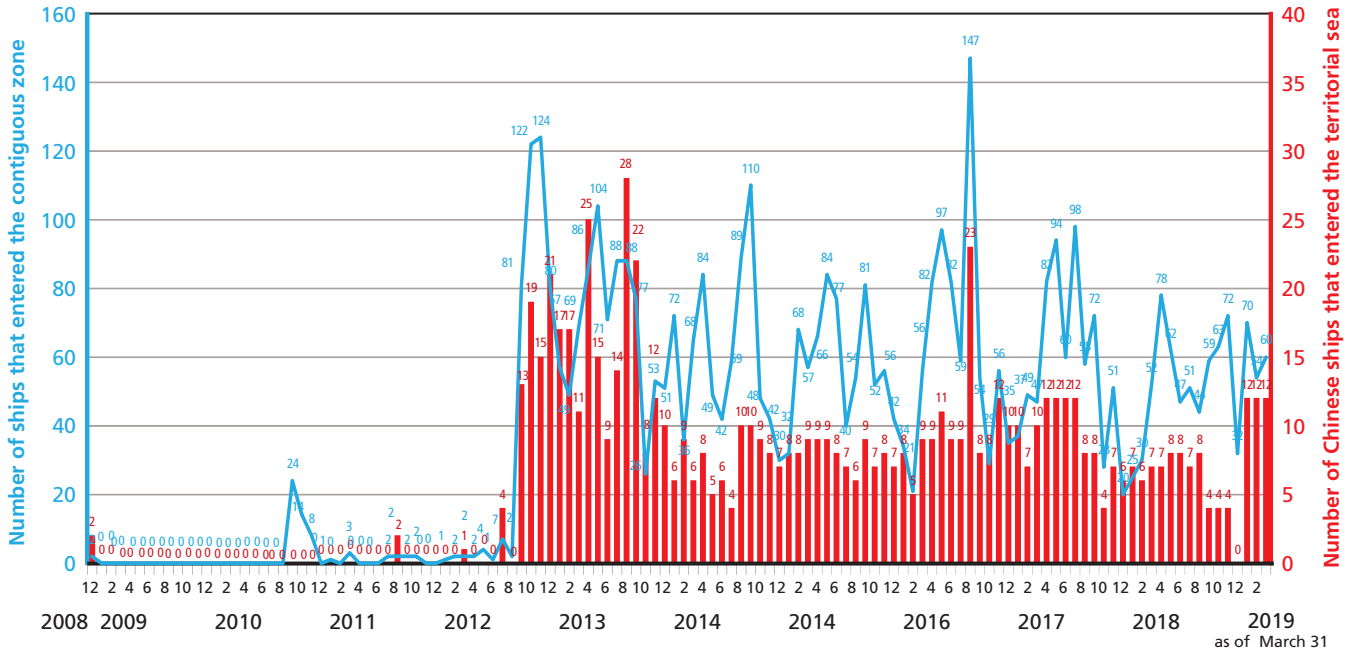
4 Tetsuo Kotani, "Bolstering the U.S. Commitment to the Senkaku Islands," *The Diplomat*, May 25, 2017a.

5 Japanese academic, interview with the authors, January 16, 2018.

6 Tetsuo Kotani, "The East China Sea: Chinese Efforts to Establish a 'New Normal' and Prospects for Peaceful Management," *Maritime Issues*, July 8, 2017b.

7 Adam Liff, "China's Maritime Gray Zone Operations in the East China Sea and Japan's Response," in Andrew S. Erickson and Ryan D. Martinson, eds., *China's Maritime Gray Zone Operations*, Annapolis, Md.: Naval Institute Press, March 2019.

Figure 4.1
Chinese Government Vessels Near the Senkaku Islands



SOURCE: JCG, "The Numbers of Chinese Government and Other Vessels That Entered Japan's Contiguous Zone or Intruded into Territorial Sea Surrounding the Senkaku Islands," chart, March 31, 2019.

Accompanying them were 28 CCG ships that entered Japan's territorial waters and 52 CCG ships that entered the contiguous zone, inundating the area and challenging Japan's ability to respond.[8]

Military Activities

While nonmilitary forces constitute the front line of Chinese attempts to alter the status quo near the Senkakus, PLAN ships have also entered the islands' contiguous zone. The first time that this occurred was in June 2016, when the frigate *Jiangkai I* entered the contiguous zone close to Kuba Island and exited close to Taisho Island.[9] In January 2018, a PLAN nuclear submarine entered the Senkaku Islands' contiguous zone.[10] While these actions are not necessarily illegal based on international law, Tokyo views them as provocative. In one case, a Chinese frigate directed fire-control radar at a Maritime Self-Defense Force destroyer in January 2013 in the EEZ of the Senkaku Islands, and Japanese officials highlighted the incident as an example of provocative behavior by the Chinese military.[11]

China's aircraft also challenge Japanese airspace by regularly conducting air patrols in the ECS. Such aircraft tend to conduct air activity in Japanese airspace but typically do not penetrate the territorial airspace above the Senkaku Islands. The first time that a Chinese government aircraft violated Japanese airspace was in December 2012, when a Chinese State Oceanic Administration Y-12 surveillance plane flew over Uotsuri Island.[12] The next time was in May 2017, when a

---

[8] Japan Prime Minister's Office, "Heisei 28-nen 8-gatsu Jōjun no Chūgoku Kōsen Oyobi Chūgoku Gyosen no Katsudō Jōkyō ni Tsuite" ["Regarding the Situation of Activity by Chinese Fishing Boats and Chinese State-Owned Ships in Early August 2016"], October 18, 2016.

[9] Japan National Security Secretariat, "China's Expanding Activities in East China Sea," undated, provided to the authors on January 15, 2018.

[10] Elaine Lies, "Japan Protests to China over Submarine off Senkaku Islands," *Asahi Shimbun*, January 13, 2018.

[11] "Chinese Officials Admit to MSDF Radar Lock Allegations," *Japan Times*, March 18, 2013.

[12] Japan National Security Secretariat, undated.

drone was launched from a CCG vessel in Japan's territorial waters.[13] China's preferred approach is to deploy air assets through strategically important waterways that are sensitive to Japan but not broach its territorial airspace. For example, in July 2013, a Y-8 airborne early warning aircraft conducted what was the PLA Air Force's first flight through the Miyako Strait.[14] In September 2013, an H-6 bomber conducted its first flight through the same strait. Then, in October, two Y-8 aircraft and two H-6 bombers conducted the same flight pattern for three consecutive days.

Diplomatic and Political Activities

China has pursued a robust diplomatic and political program designed to support its desired narrative. The fundamental stance that China advocates is that the Senkaku Islands have been China's "sacred territory since ancient times," which is "supported by historical facts and jurisprudential evidence."[15] Part of China's campaign links Japanese actions as attempts to undermine the international order established after Imperial Japan's defeat. For example, United Nations Ambassador Li Baodong called Japanese actions "a resistance to the international endeavors against colonialism, an outright denial of the outcomes of victory of the world anti-fascist war, and a grave challenge to the [post–World War II] international order and the international law."[16] In addition to issuing position papers and treating the waters around the islands as traditional fishing grounds, China makes unilateral declarations meant to carry legal import. For example, in its February 1992 Law on the Territorial Sea and the Contiguous Zone, China established a legal basis by which Beijing can exercise sovereignty over its territorial sea and contiguous zone, including that of the

---

13 Japan National Security Secretariat, undated.

14 Japan Ministry of Defense, undated-a.

15 Ministry of Foreign Affairs of the People's Republic of China, "Statement of the Ministry of Foreign Affairs of the People's Republic of China," September 10, 2012.

16 Li Baodong, "Remarks of Rebuke Against Japan's Statement on Diaoyu Dao by Ambassador Li Baodong During the General Debate of the 67th Session of the UN General Assembly," Permanent Mission of the People's Republic of China to the UN, October 16, 2012.

Senkaku Islands.[17] Another prominent example includes the November 2013 declaration of an ADIZ in the ECS that included foreign aircraft rules that are widely believed to be beyond the scope of traditional ADIZ practices.[18]

How Has Japan Responded to Gray Zone Threats from China?

Because of China's increased activities, Japan has instituted several improvements to strengthen its force posture and capabilities. These efforts are supported by strategic messaging and diplomacy to promote Japan's sovereignty.

Japan Coast Guard

As Japan's sole maritime law enforcement agency, JCG is tasked as the lead agency to protect the Senkaku Islands. Given this role, the Japanese government has increased JCG's budget and personnel, resulting in important posture changes and capability upgrades.

Posture Changes

In March 2016, JCG stood up a 12-vessel Senkaku Territorial Waters Guard Unit based on Ishigaki Island (see Figure 4.2). The unit is tasked exclusively with patrolling the waters surrounding the Senkaku Islands. To perform this mission, it is equipped with high-performance patrol ships that include ten newly built 1,500-ton patrol ships based on Ishigaki and two 3,100-ton patrol vessels based in Okinawa.[19] Although all ships can operate helicopters from their decks, only the two on Oki-

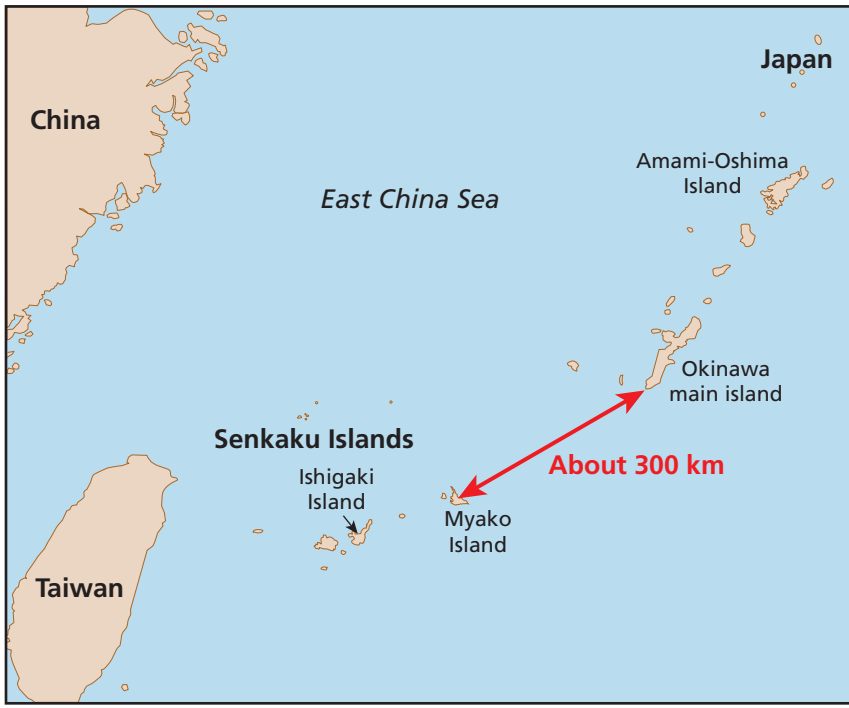
---

[17] Government of the People's Republic of China, Law of the People's Republic of China on the Territorial Sea and the Contiguous Zone, February 25, 1992.

[18] Ministry of National Defense of the People's Republic of China, "Statement by the Government of the People's Republic of China on Establishing the East China Sea Air Defense Identification Zone," *China Daily*, November 23, 2013b; and Ministry of National Defense of the People's Republic of China, "Announcement of the Aircraft Identification Rules for the East China Sea Air Defense Identification Zone of the People's Republic of China," *China Daily*, November 23, 2013a.

[19] Kei Ishinabe, "Article Urges Reinforcing Coast Guard to Counter China over Disputed Senkaku Islands," *Sankei Web-S*, via Open Source Enterprise, February 24, 2017; and JCG, *Annual Report 2016*, Tokyo: Ministry of Land, Infrastructure, Transport and Tourism, 2016, p. 9.

Figure 4.2
Map of the Senkaku and Surrounding Islands



nawa have hangars. For six of the ships at Ishigaki, JCG introduced a multiple crew system in 2016 to raise the utilization rate of three ships to the equivalent of four ships. This is done by taking the crew members needed to operate four ships and assigning them to three ships.[20] Video transmission devices were also installed on all 12 ships to allow them to send instantaneous videos to JCG headquarters and the Prime Minister's Office via satellite circuit.[21] These capabilities were completed in March 2018. The objective was to enable the government to make rapid decisions during any situation.

[20] JCG, 2016, p. 9.

[21] "JCG to Expand Video Transmission on Senkaku Patrols—Graphic," *Yomiuri Shimbun*, via Open Source Enterprise, March 2, 2017.

In October 2016, JCG also upgraded the status of its Miyako Coast Guard Station to a Miyako Coast Guard Office, doubled its patrol staff, and allocated it new patrol vessels—all to further enhance the security around the islands. The new office collaborates with the Senkaku Territorial Waters Guard Unit in situations around the Senkaku Islands, if needed. Otherwise, the Miyako Coast Guard Office is responsible for everything else in the area's waters. Along with the upgraded status came additional resources. Before the station was upgraded, it had only three patrol vessels.[22] Since the upgrade, it was allocated three new enhanced patrol vessels based at Nagayama Port on Irabu Island, which is connected via bridge to Miyako Island. Another three ships were added at the end of fiscal year 2017, and three more were added by the end of fiscal year 2018, bringing the number of patrol boats at Miyako to 12 by March 2019.[23]

JCG has increased training to complement enhancements to capabilities. As of 2017, approximately 1,800 people were assigned to the 11th Regional Coast Guard headquarters.[24] This is a rapid increase from 1,243 people in 2015.[25] To support this increase, JCG is opening a target range on Miyako in 2019. This will be JCG's first training facility not on Honshu, which currently houses three shooting ranges.[26] JCG will also begin training its own pilots for fixed-wing aircraft, pending the procurement of training aircraft and the training of instructors.[27] Although JCG trains its own helicopter pilots, JCG pilots

---

[22] "JCG Deepens Surveillance Capabilities on Miyakojima," *Yomiuri Shimbun*, via Open Source Enterprise, September 17, 2017.

[23] This includes ten small patrol vessels, one medium patrol vessel, and one patrol craft. JCG official, email correspondence with the authors, April 10, 2018.

[24] Documents provided to the authors by JCG Headquarters on January 15, 2018.

[25] "(Reisei, Kizen to Taiō) Senkaku Keibi de Hasegawa Honbuchō Dai-11 Kanku Kaiho" ["'Calm and Resolute Response,' 11th Regional Coast Guard Headquarters Commander Hasegawa About Senkaku Security"], *Yaeyama Nippō*, August 4, 2015.

[26] Ankit Panda, "East China Sea: Japan Coast Guard Plans Miyako Island Facility Upgrades," *The Diplomat*, September 24, 2017.

[27] "JCG to Train Own Pilots Amid Rising Surveillance Demands," *Yomiuri Shimbun*, via Open Source Enterprise, July 19, 2017.

for airplanes have been trained in Maizuru (a Kyoto prefecture) by the Japan Maritime Self-Defense Force.[28]

Capability Improvements

Despite the 375 patrol ships in JCG's fleet, only 137 are larger patrol vessels (*junshisen*), compared with 238 smaller patrol craft (*junshitei*).[29] Although both types are tasked with maintaining ocean security, only the larger patrol vessels operate in the open ocean; the patrol crafts operate in harbors or close to shore.[30] By 2021, JCG plans to increase the number of patrol vessels from 137 to 144.[31] This fleet will include the large patrol vessel with helicopter, ranging from 3,000 to 6,500 tons; the large patrol vessel, ranging from 1,000 to 3,500 tons; the medium patrol vessel, ranging from 350 to 500 tons; the small patrol vessel, ranging from 130 to 220 tons; and one large firefighting boat, at 300 tons.[32] Of these patrol vessels, only 62 are large enough to conduct long-term operations at great distances from shore, such as around the Senkaku Islands.

JCG already has a 24-hour presence around the Senkaku Islands in the water, but by the end of fiscal year 2019, it will complete a system that also gives it 24-hour surveillance in the air. This capability is part of a longer-term effort to bolster JCG's aerial capabilities.[33] In addition

---

[28] "JCG to Train Own Pilots Amid Rising Surveillance Demands," 2017.

[29] JCG, *Heisei 30 Nendo Kaijō Hoan Chō Kankei Yosan Kettei Gaiyō* [*Summary of the FY2018 Budget Decision Regarding the Japan Coast Guard*], Tokyo, December 2017c.

[30] JCG, "Junshisen to Junshitei no Chigai ha Nan Desu ka" ["What Is the Difference Between Patrol Vessels and Patrol Craft?"], JCG 5th Regional Headquarters, June 7, 2010.

[31] JCG, 2017c, p. 12.

[32] Official tonnages for these general classes of ships are more than 700 tons for the large patrol vessel with helicopter; more than 700 tons for the large patrol vessel; more than 350 tons for the medium patrol vessel; more than 350 tons for the small patrol vessel; and more than 300 tons for the large firefighting boat. See JCG, *Japan Coast Guard*, Tokyo: Ministry of Land, Infrastructure, Transport and Tourism, March 2017b, p. 5-6; JCG, "Kaijō Hoan Chō no Sentei" ["JCG Ships"], January 1, 2017a; and Sixth Regional Headquarters Ship Technology Division, "Kaijō Hoan Chō Sentei no Bunrui" ["Classification of Japan Coast Guard Ships"], December 2017.

[33] JCG, 2017c, p. 12.

to a fleet of 32 fixed-wing aircraft, JCG operates 49 helicopters.[34] This fleet of helicopters, operable from JCG patrol vessels, are supported by a maritime surveillance system involving satellites. The system, operational since February 2018, has private satellite operators taking photos of activity in a 2.2-million km^2 area at least twice a day, and the photos are then transmitted to JCG regional headquarters.[35] Because JCG's current system of obtaining images from the Cabinet Secretariat's Satellite Intelligence Center takes time and depends on other agencies for updates, establishing its own system helps JCG quickly collect information and rapidly respond to changing situations.

Strategic Communication and Diplomacy

To counter Chinese activity, the Japanese government employs other nonmilitary tools, including strategic communication and diplomacy. Through these tools, Tokyo takes a multifaceted approach to counter Chinese efforts to change the facts on the ground or the narrative of Chinese sovereignty over the Senkaku Islands.

Strategic Communications

Piercing the ambiguity within which China's gray zone activities thrive has been a central goal to deny China "the benefits of nonattribution, exposing the nature and illegitimacy of their actions, and raising the various costs—political, diplomatic, economic—of such activities."[36] Tokyo's objective is to quickly disseminate information about Chinese activities to show both domestic and international audiences the true nature of China's provocations. This has taken two forms.

The first is visual evidence. Through pictures posted on government websites, Tokyo attempts to lift the veil on Chinese actions to provide physical evidence of its behavior. The Joint Staff Office publishes press statements following any air activity by PLA Air Force aircraft,

---

[34] JCG, 2017c, p. 20.

[35] "JCG to Introduce Maritime Surveillance System Using Satellites," *Yomiuri Shimbun*, via Open Source Enterprise, September 8, 2017.

[36] Brands, 2016.

and the statements can include routes, pictures, and other details.[37] The Ministry of Defense also has a sophisticated webpage that posts pictures and specifications of the PLA Air Force aircraft and interactive maps that show the route of the aircraft.[38] And JCG occasionally posts pictures or videos of CCG vessels.[39]

The second tactic of strategic communication is through detailed information exposing the number and nature of Chinese provocations. For activity on the water, JCG maintains a detailed month-by-month tracking of Chinese government ships entering the contiguous zone and territorial waters around the Senkaku Islands (see Figure 4.1).[40] This tracking is also linked to an English version on the Ministry of Foreign Affairs website.[41] For activity in the air, the Joint Staff Office provides detailed information detailing quarterly trends on the numbers of Japan Air Self-Defense Force (JASDF) scrambles against foreign aircraft.[42] Information of both types is also always included in the annual *Defense of Japan* white paper published by the Ministry of Defense.

Tokyo also engages in strategic communications to frame positive views of Japan and the Senkaku Islands. Following the 2010 fishing trawler incident, there was a "clear awareness of the need" for Japan to

---

37 For example, Japan Joint Staff Office, "Chūgoku Ki no Higashi Shinakai Oyobi Taiheiyō ni Okeru Hikō ni Tsuite" ["Regarding the Flight of Chinese Aircraft in the East China Sea and Pacific Ocean"], press release, March 23, 2018b.

38 Japan Ministry of Defense, "Chūgoku Kōkū Senryoku tō no Waga Kuni Shūhen Kūiki ni Okeru Katsudō ni Tsuite" ["Regarding the Activity in the Airspace Surrounding Our Country by Chinese Air Power"], undated-b.

39 For an example of a video, see JCG, "Senkaku Shotō Shūhen Kaiiki ni Okeru Chūgoku Kōsen Oyobi Chūgoku Gyosen no Katsudō Jōkyō ni Tsuite" ["Regarding the Situation of Chinese State-Owned Ships and Chinese Fishing Vessels Occurring in the Ocean Area Around the Senkaku Islands"], undated.

40 JCG, undated.

41 Japan Ministry of Foreign Affairs, 2018.

42 See, for example, Japan Joint Staff Office, "Heisei 29 Nendo 3 Shihanki Made no Kinkyū Hasshin Jisshi Jōkyō ni Tsuite" ["Regarding the Status of Implementing Scrambles in the 3rd Quarter of FY2017"], press release, January 19, 2018a.

engage in something akin to information warfare.[43] Toward this end, the Ministry of Foreign Affairs created a Public Diplomacy Strategy Division under the director-general for press and public diplomacy in 2012. The division's purpose is to counter Chinese moves by delivering Tokyo's message to the broader international community. But because the Senkaku issue narrowly concentrates on Japanese territory, the division also focuses on broader activities conducted by China.[44] For example, it publishes information on Chinese activities, and it holds public events and manages a section on the Ministry of Foreign Affairs website devoted to explaining Japan's case for various territorial disputes, including over the Senkaku Islands. These efforts are supported by the Cabinet Secretariat's Office of Policy Planning and Coordination on Territory and Sovereignty and the National Security Secretariat.

Diplomacy

Japan's normal diplomatic response to Chinese gray zone activities is to file an official complaint either in Beijing via Japan's representative or with the Chinese ambassador to Japan in Tokyo. According to Japan's Ministry of Foreign Affairs,

> Each time Chinese government vessels intrude into Japan's territorial sea, on-site Japanese patrol vessels demand them to leave, and at the same time, the Japanese government promptly lodges a strong protest against the Chinese Government through diplomatic channels, strongly demanding the vessels leave immediately and that China prevent such an incident from occurring again.[45]

The immediate response is to call a Chinese representative into the Ministry of Foreign Affairs. The more provocative the gray zone action, the more senior the official.[46] Calling the Chinese ambassador to the ministry is considered one of the strongest messages. In addi-

[43] Anonymous, interview with the authors, Tokyo, January 30, 2018.

[44] Anonymous, interview with the authors, Tokyo, January 16, 2018.

[45] Japan Ministry of Foreign Affairs, 2018.

[46] Anonymous, interview with the authors, Tokyo, January 16, 2018.

tion to these public diplomatic demarches, the Ministry of Foreign Affairs engages in private messaging with Chinese interlocuters, including private companies, to explain how Chinese activities hurt bilateral interests.[47]

Japan Self-Defense Forces

As the final line of defense against Chinese gray zone tactics, Japan has the JSDF. In 2010, to strengthen deterrence as a way to prevent escalation, Tokyo shifted its focus away from Cold War–era concerns of an invasion from the north and to the increasing challenges to Japan's Nansei Shotō (or Ryukyu Islands). Under the notion of a "dynamic defense force"—changed in 2013 to "dynamic joint defense force"—the JSDF shifted from the traditional passive deterrent "basic defense force" to one focused on "readiness, mobility, flexibility, sustainability, and versatility."[48] As a result, Tokyo has made a series of changes in the JSDF's force posture and capabilities.

Posture Changes

Japanese leaders are repositioning the JSDF's force posture in the Nansei Shotō.[49] In March 2016, the Japan Ground Self-Defense Force (JGSDF) began operations of a coastal observation unit and logistics facility on Yonaguni, the westernmost inhabited island in the Japanese archipelago. Manned with about 160 personnel, the observation unit is a permanent intelligence-gathering facility that provides constant monitoring of the ECS. The JGSDF plans to open similar facilities on neighboring islands in the coming years. On Amami Ōshima, it will station about 550 infantry personnel by March 2019 to man a logistics facility, a mobile warning and control radar system, and surface-to-air missile and surface-to-ship batteries. On Miyako, between 700 and 800 JGSDF personnel will man similar facilities by the same date. By 2021, another coastal observation unit will be completed on Ishigaki, with a plan to

---

[47] Anonymous, interview with the authors, Tokyo, January 15, 2018.

[48] Japan Ministry of Defense, *National Defense Program Guidelines for FY 2011 and Beyond*, Tokyo, December 17, 2010, p. 7.

[49] The detailed numbers in this paragraph are drawn from documents provided to the authors by the Japanese Embassy and U.S. Army, Japan.

station 500–600 JGSDF personnel there.[50] Accompanying these modernization efforts is an increase in missile batteries in the area to position the JSDF to manage escalation in high-intensity situations.[51]

The JASDF and JGSDF have also undergone force posture changes. The JASDF's efforts have focused largely on its Southwestern Composite Air Division based in Naha, Okinawa, which is responsible for scrambling against Chinese incursions in the Nansei Shotō. Because of the intensity of Chinese incursions, in 2015, the JASDF established the 9th Air Wing in Naha by supplementing the existing 204th fighter squadron with the 304th squadron of F-15s from the 8th Air Wing at Tsuiki Air Base.[52] This was the first new air wing since the 8th Air Wing was established in 1964, and the enhancement effectively doubled the number of fighters dedicated to responding to Chinese incursions. Then, in 2016, the Southwestern Composite Air Division was elevated to become the southern defense area, composed of the 9th Air Wing.[53] The JASDF also established a new airborne early warning and control squadron in Naha in April 2014, composed of four of the JSDF's 13 E-2C Hawkeye aircraft.[54] Together, these changes help the JASDF secure air superiority and enhance Japan's air defense in the critical southwestern region.

To strengthen its island defenses, the JGSDF stood up a 2,100-member Amphibious Rapid Deployment Brigade at the end of March 2018.[55] Once fully complete (date is unspecified), the number of personnel will increase to approximately 3,400.[56] The brigade, headquar-

---

[50] Documents provided to the authors by the Japanese Embassy and U.S. Army, Japan.

[51] Dylan Malyasov, "Japan Deploying Type-3 Missile System in Okinawa Prefecture," *Defense Blog*, August 23, 2016.

[52] Japan Ministry of Defense, *Defense of Japan 2015*, white paper, Tokyo, 2015, p. 228.

[53] Kosuke Takahashi, "JASDF Forms New AEW Squadron in Okinawa," *Jane's Defence Weekly*, April 14, 2014.

[54] Takahashi, 2014.

[55] Japan Ministry of Defense, "Bōuei Daijin Rinji Kisha Kaiken Gaiyō" ["Summary of the Minister of Defense's Special Press Conference"], September 7, 2016.

[56] Koichi Isobe, "The Amphibious Operations Brigade," *Marine Corps Gazette*, Vol. 101, No. 2, February 2017; and retired JGSDF officer, email correspondence with the authors, September 27, 2017.

tered at Ainoura, near Sasebo in Nagasaki prefecture, is the first of three brigades planned for the Western Army.[57] The objective of establishing the brigade is for the JSDF to acquire the capabilities "to land, recapture and secure without delay any remote islands that might be invaded."[58] The 640-strong Western-Area Infantry Regiment, a battalion-sized light infantry regiment established in 2002 to specialize in amphibious operations, will be the core of the Amphibious Rapid Deployment Brigade.

In the next several sections, we turn to our findings on the response to Chinese gray zone tactics in Southeast Asia, including in Vietnam, the Philippines, Indonesia, Singapore, and Australia.

Vietnam

Countries in Southeast Asia have become increasingly concerned about increasing Chinese gray zone activities in the region. Many countries in the region perceive Chinese gray zone tactics as part of a whole-of-government approach incorporating paramilitary, legal, political, administrative, economic, information operation, and cyber actions that seek to change the status quo of territorial disputes in Beijing's favor. In contrast to Japan, however, several countries in Southeast Asia, such as Vietnam and the Philippines, are experiencing consistent, long-term material challenges by China to deny them the use of the living and nonliving resources in their EEZs. For example, Chinese vessels have threatened Vietnamese vessels and warned them not to fish or drill for oil in these areas. Most countries in the region, our field research found, have been ineffective in fashioning a deterrence strategy in response to Chinese gray zone tactics but have undertaken military and diplomatic maneuvers to signal displeasure with such tactics.

Vietnam, in particular, is experiencing perhaps some of the most-challenging and most-formidable aspects of Chinese gray zone tactics in Southeast Asia.

---

[57] Isobe, 2017; and JGSDF officer, email correspondence with the authors, March 19, 2018.

[58] Japan Ministry of Defense, *Medium Term Defense Program (FY2014–FY2018),* Tokyo, December 17, 2013, p. 5.

Types of Gray Zone Threats Faced by Vietnam

In addition to the legal, administrative, economic, and informational tactics mentioned earlier in this report, interviewees highlighted three of the most-challenging and most-immediate gray zone tactics that China has adopted to deny Vietnam's claims in the SCS. The first is China's use of paramilitary forces to assert its claims of sovereignty over the land features and maritime area within its Nine-Dash Line claim in the SCS. Here, *paramilitary* encompasses both CCG and maritime militia vessels. CCG, now the largest coast guard in the world by some metrics, routinely shadows and harasses Vietnamese fishing and coast guard vessels operating in the Paracel Islands, for example.

In many examples of such paramilitary harassment against Vietnamese vessels, China has adopted unprofessional and escalatory tactics that break norms of safety at sea; such tactics include ramming, shouldering, using water cannons, and boarding Vietnamese fishermen's boats and stealing the fish catch.[59] Vietnamese vessels have been the recipient of arguably more rammings at the hands of CCG than any other claimant in the SCS has.[60] During our interviews, the blurred status of CCG—in particular, whether it was under civilian or military control—was also highlighted as a concern for Vietnamese authorities who worry about escalation and use-of-force principles during a clash at sea.[61]

Another form of China's paramilitary coercion that our Vietnamese interviewees mentioned is China's maritime militia, which interviewees regarded as comprising fishing vessels nominally manned by civilian personnel who are, in reality, militiamen under some sort of Chinese state control and whose purpose is to assert Chinese sovereignty over disputed waters (i.e., not fish).[62] Interviewees suggested

---

[59] Elena Bernini, "Chinese Kidnapping of Vietnamese Fisherman in the South China Sea: A Primary Source Analysis," Asia Maritime Transparency Initiative, Center for Strategic and International Studies, September 14, 2017.

[60] "China Ships 'Rammed 1,400 Times by Vietnamese Vessels,'" BBC News, June 9, 2014.

[61] Vietnamese official, interview with the authors, Hanoi, February 6, 2018.

[62] Vietnamese officials and academics, interview with the authors, Hanoi, February 5–6, 2018.

that, because of the aggressiveness of their actions and the plausible deniability of Chinese state support, these maritime militiamen pose as great a challenge to Vietnamese fishermen as CCG does.[63]

The second challenge that interviewees noted was China's use of threats against Vietnamese energy exploration activities in Vietnam's EEZ. China has routinely warned international petroleum companies not to explore or drill for oil anywhere within the Nine-Dash Line. But more-recent threats, including an instance in July 2017 in which China reportedly threatened to take "military action" against Vietnamese bases in the SCS if Vietnam followed through with oil exploration activities, made headlines and forced Talisman Vietnam, a subsidiary of the Spanish energy firm Repsol, to withdrawal from the block.[64] One interviewee noted that Chinese threats against Vietnam's legitimate use of energy resources in its EEZ in the SCS appeared to be more "aggressive" and were preventing Vietnamese and international energy firms from attempting to explore for oil in vast areas of Vietnamese waters.[65]

The third challenge that interviewees noted is China's unprecedented expansion of artificial islands in the SCS and the dual-use facilities that have been built on them.

How Has Vietnam Responded to Gray Zone Threats from China?

Situated near most other countries in Southeast Asia, Vietnam has exhibited a willingness to push back against Chinese coercion in some instances. Its responses have included diplomatic and military actions and postures. On the diplomatic side, Vietnam has been one of the most vocal opponents of Chinese actions to extend its territorial claims in the SCS. For example, Vietnamese representatives frequently bring up China's expansionist claims in public forums, such as at meetings of the Association of Southeast Asian Nations (ASEAN) and the

---

[63] Vietnamese officials and academics, interview with the authors, Hanoi, February 5–6, 2018.

[64] Bill Hayton, "The Week Donald Trump Lost the South China Sea," *Foreign Policy*, July 31, 2017.

[65] Vietnamese official, interview with the authors, Hanoi, February 6, 2018.

Shangri-La Dialogue—Asia's premier annual defense summit, which brings together ministers and delegates from more than 50 countries.

Realizing that it cannot outmatch the numerical superiority of PLA forces in the air and sea domains, Vietnam has sought to develop a larger array of anti-access capabilities to deter Beijing from coercing Vietnam beyond certain thresholds. Recently, Vietnam has acquired six Russian-built *Kilo*-class submarines and 36 Sukhoi Su-30MK2 fighter jets, as well as Bastion-P shore-based anti-ship cruise missiles and S-300 surface-to-air missile batteries.[66] On the paramilitary side, Vietnam has greatly expanded its coast guard presence, fielding a force larger than that of the Philippines, Malaysia, and Indonesia. These paramilitary maritime vessels are lightly armed and conduct maritime law enforcement activities in the SCS in support of Vietnamese maritime rights. These capabilities are not meant to outmatch China's in terms of quantity or quality. Rather, they are meant to provide sufficient deterrent value against China and other nations in the event that a contingency unfolds in Vietnam's maritime space. Vietnam has supplemented these defense articles with an increase in troops, facilities, and infrastructure on its occupied features in the SCS. It has also deployed more than a dozen economic, scientific, and technological service stations (called DK-1 platforms) on several shallow banks and has undertaken modest land reclamation activities on a few of these island features.[67]

A good example of what has worked to deter China, from Vietnam's perspective, was Vietnam's protest of Chinese drilling activities during the Haiyang Shiyou 981 incident in May 2014. In this incident, China deployed an oil exploration rig called the Haiyang Shiyou 981 off of the Paracel Islands in the SCS and within Vietnam's EEZ. Soon after the oil rig was deployed, China established a security cordon of navy, coast guard, and fishing or auxiliary vessels about 10 or 11 nau-

---

[66] Derek Grossman, "Can Vietnam's Military Stand Up to China in the South China Sea?" *Asia Policy*, Vol. 13, No. 1, January 2018.

[67] See Ian Bowers, "Power Asymmetry and the Role of Deterrence in the South China Sea," *Korean Journal of Defense Analysis*, Vol. 29, No. 4, December 2017; and Asia Maritime Transparency Initiative, "Vietnam Builds Up Its Remote Outposts," Center for Strategic and International Studies, August 4, 2017.

tical miles from the rig and actively repelled Vietnamese attempts to enter the area using ramming and shouldering techniques.[68] Over about a month, a tense contest of will ensued: China deployed greater numbers of fishing, maintenance, and supply ships, as well as tug boats and ships, to protect the oil rig, and Vietnam sent its own fishing, coast guard, and naval ships to break the cordon to warn the Chinese to leave the area. The potential for escalation was high.

At one moment during the crisis, a large Chinese fishing trawler rammed and sank a wooden Vietnamese fishing vessel, the crewmembers of which were saved by a nearby Vietnamese coast guard vessel.[69] After more than a month of a tit-for-tat standoff, China withdrew the oil rig earlier than its publicly announced end date, which our interviewees concluded was a "strategic victory" for Vietnam.[70] Vietnam's strategy of "holding the line" sufficiently demonstrated Vietnamese political will to defend its maritime waters while preventing escalation from spiraling out of control.[71]

However, other cases point to strategies that have failed. For example, after several weeks of deliberation during the Talisman Vietnam incident highlighted earlier, the Vietnamese government decided to pull Talisman Vietnam out of the block and plug the well, essentially capitulating to Chinese threats. Several of the officials and academics whom we interviewed expressed remorse for such a decision and suggested that there were limits to Vietnam's willingness to challenge Chinese gray zone tactics in every instance of coercion.[72]

---

[68] Morris, 2017c, pp. 22–23.

[69] Morris, 2017c, pp. 22–23.

[70] Vietnamese officials and academics, interview with the authors, Hanoi, February 5–6, 2018.

[71] Vietnamese officials and academics, interview with the authors, Hanoi, February 5–6, 2018.

[72] Vietnamese officials and academics, interview with the authors, Hanoi, February 5–6, 2018.

The Philippines

Types of Gray Zone Threats Faced by the Philippines

Because of its overlapping claims with China, the Philippines, like Vietnam, bears a large percentage of Chinese gray zone actions. The biggest difference between Vietnam and the Philippines, however, is that the Philippines has a lower base of military capabilities with which to deter China. After the election of President Rodrigo Duterte in 2016, the Philippines now also appears to lack the political will to challenge Chinese actions.

The Chinese tactics that the Philippines faces are similar to those that Vietnam faces. Interviewees highlighted the challenge from China's paramilitary forces in the SCS.

As an example, Filipino officials brought up the Pagasa incident of 2016. Pagasa Island (also known as Thitu Island) is a naturally formed island occupied by the Philippines in the Spratly Island chain in the SCS. There are four sandbars or banks near Pagasa that are unoccupied but whose waters are frequented by Filipino and Chinese fishermen.

According to reports, CCG and maritime militia vessels harassed Philippine maritime law enforcement vessels conducting routine patrols near the sandbars, and various standoffs occurred between August and September 2017.[73] According to a report, China's blue-hulled maritime militia vessels, which had not been spotted there previously, "sounded their sirens" to "ward off or limit any Philippine vessel from coming near [the] sandbars," with Chinese naval and coast guard vessels nearby.[74] One interviewee noted that the case highlights a recent evolution on the part of China to use maritime militia as stand-ins for coast guard vessels yet still be able to deter another country's coast guard vessels from conducting normal operations.[75]

---

[73] Carmela Fonbuena, "5 Chinese Ships Spotted Near Pag-asa Sandbars," *Rappler*, August 15, 2017; and Erwin Colcol, "Chinese Vessels Spotted Near Pag-asa Island, Alejano Says" *GMA News*, October 3, 2017.

[74] Patricia Lourdes Viray, "Chinese Applying New Tactic in Pag-asa Sandbars, Says Alejano," *Philstar News*, October 4, 2017.

[75] Philippine official, interview with the authors, Manila, February 14, 2018.

Like Vietnam, the Philippines has also watched with alarm as China has reclaimed thousands of acres of land on disputed maritime features in the SCS and built military installations on them.[76]

Interviewees noted threats against Filipino economic, legal, administrative, and cyber interests, as well. For example, China has shown a willingness to impose economic costs through the use of trade, aid, investments, and threats of sanctions against the Philippines to influence its behavior in the SCS. This has included a Chinese ban on fruit imports from the Philippines during the Scarborough Shoal standoff in 2012, the issuance of a travel advisory that adversely affected the tourism industry of the Philippines in 2014, and threats against the Philippines' oil and natural gas exploration activities in its EEZ in the SCS, such as near Reed Bank.[77] The Philippines is more dependent on China for exports than China is for Philippine imports and thus has acute vulnerability in this domain.

Despite these and other Chinese actions, most interviewees noted that, since Duterte initiated an "opening up" policy toward China in 2016, there has been a de-escalation of tactics and actions by China toward Philippine assets in the SCS.[78]

How Has the Philippines Responded to Gray Zone Threats from China?

By far the most effective tactic that the Philippines has employed against China to date has been to initiate legal proceedings against Chinese maritime claims in the SCS. The July 2016 PCA ruling, which invalidated China's Nine-Dash Line covering almost the entire SCS, among other findings, was a major victory for the Philippines. The landmark ruling found that China has illegally prevented Filipino fishermen and petroleum companies from extracting living and nonliving resources in the Philippine EEZ and that China had breached international law

---

[76] *Land reclamation* here connotes the process of creating new land from the ocean, riverbeds, or lake beds where no land existed previously. It does not imply a claim to land that existed previously that a nation seeks to take back.

[77] Philippine official, interview with the authors, Manila, February 14, 2018.

[78] Philippine official, interview with the authors, Manila, February 15, 2018.

by infringing on such activities.[79] Although doubts have been raised over China's compliance with the ruling, it represented a victory in clarifying maritime rights under international law and a clear setback for China's attempts to legitimize its claims in the SCS.[80]

Since the ruling, however, President Duterte has chosen not to use the findings to pressure China to stop such activities or to leverage the findings to the Philippines' advantage. Instead, he has chosen a more accommodating approach to Beijing in return for Chinese aid, foreign direct investment, and joint exploration of resources in the SCS. The Philippines' more accommodating approach has brought about a general de-escalation of tensions near the features contested between China and the Philippines, such as in Scarborough Shoal, where Filipino fishermen are now permitted to fish from time to time. This approach also appears to have resulted in fewer actions that have the potential to aggravate tensions. For example, the Philippine Navy has been instructed to no longer board Chinese fishing vessels in most areas of the SCS, and Filipino fishermen are not being harassed and detained as much as they have been in the past.[81]

The Armed Forces of the Philippines have undertaken modest modernization efforts to combat the threat from China. For example, the defense budget has increased over the past several years, and the Philippine government announced plans to spend about $1.7 billion on a five-year military upgrade program beginning in 2018.[82] Although starting from a very low base compared with China, the Philippine

---

[79] PCA, In the Matter of the South China Sea Arbitration Before an Arbitral Tribunal Constituted Under Annex VII to the United Nations Convention of the Law of the Sea Between the Republic of the Philippines and the People's Republic of China, PCA Case No. 2013-19, July 12, 2016,

[80] Anthony Deutsch and Toby Sterling, "China's Legal Setback Could Spur More South China Sea Claims," Reuters, July 14, 2016. On China's compliance with the ruling, see Julian Ku and Chris Mirasola, "Tracking China's Compliance with the South China Sea Arbitral Award: Traditional Fishing Rights Inside the Lagoon at Scarborough Shoal," Lawfare, November 2, 2016.

[81] Philippine official, interview with the authors, Manila, February 15, 2018.

[82] "Duterte Breaks Records with $6.6 Billion Military Budget, Plans to Outspend Most European Countries," *Frontera News*," February 5, 2017.

Navy acquired two frigates from South Korea in 2018 and plans on purchasing more fast-attack patrol vessels in the future.[83] The Navy also announced that Israeli-made surface-to-surface missiles were being installed on three multipurpose attack vessels, among other modernization measures.[84] Nonetheless, the Philippine Navy and Coast Guard are no match for the size and armaments of the Chinese Navy and Coast Guard, and the gap between the two forces has only increased over the past decade.

Indonesia

Types of Gray Zone Threats Faced by Indonesia

By far the biggest concern regarding Chinese gray zone tactics affecting Indonesia is China's increasing use of fishermen and fishing militias in the SCS, which threatens Indonesia's ability to protect its marine resources. In recent years, these militia units have caused skirmishes with Indonesian government and naval vessels in a small maritime area within Indonesia's EEZ that overlaps with China's Nine-Dash Line, north of Natuna Island. China asserts that this area is part of its "traditional fishing grounds," which comprise the entirety of China's Nine-Dash-Line claim. Until recently, Indonesia had not taken a public stance on China's claims, deciding instead to address maritime challenges through bilateral dialogue and through ASEAN. However, creeping Chinese activity in disputed waters led the Indonesian Foreign Ministry in 2016 to publicly challenge Chinese claims by asserting they had "no basis under international law."[85]

Two incursions by China in 2016 illustrated both Beijing's capacity and its intent to threaten Indonesian maritime sovereignty. On

---

[83] Carmela Fonbuena, "PH Not Keen to Buy More Frigates, Opts for Smaller Vessels," *Rappler*, March 26, 2018.

[84] "With Israeli Missiles, Philippine Navy Takes Step Toward Modernizations," *Times of Israel*, May 11, 2018.

[85] Emirza Adi Syailendra, "China in Indonesia's Foreign Policy: Maintaining a Nonbalancing Posture," Singapore: Nanyang Technology University, RSIS Commentary No. 48, September 14, 2017b.

March 19, 2016, Indonesian fisheries authorities captured the Chinese fishing boat *Kway Fey* as it entered the Natuna Island EEZ. The authorities detained the boat for illegal fishing, but as it was being towed back to the Natuna Islands, a CCG vessel physically intervened and rammed the Chinese fishing boat free. The freed boat was taken back to China by CCG, while the Chinese fishing boat's eight crew members, who were then aboard the Indonesian Coast Guard vessel, were transported back to Indonesia for prosecution.[86] A spokesperson for China's foreign ministry protested Indonesia's detention of these fishermen, claiming that the boat had been "in Chinese traditional fishing grounds, not entering Indonesia territorial waters," and demanded the release of the crew members.[87] Indonesia refused, insisting that the boat had been fishing illegally in Indonesia's EEZ. China's actions and promulgation of a concept of "traditional fishing grounds" was seen not only as a violation of Indonesian sovereignty but also an attempt to weaken UNCLOS.[88] Indonesian authorities were also alarmed that a Chinese government ship—in this case, a coast guard vessel—would behave in such an unprofessional and dangerous manner against another country's coast guard vessel.[89]

A second incident occurred in June 2016, when the Indonesian Navy found itself in another standoff with a CCG vessel after opening fire multiple times to detain a Chinese fishing trawler fishing illegally in Natuna waters. The incident featured the second recent occurrence of the Indonesian Navy firing weapons to force Chinese fishing vessels to comply with Indonesian demands to cease operations and allow Indonesian authorities to detain the vessel; in this case, the gunfire led to the injury of one Chinese fisherman.[90] Interviewees noted that the Chinese fishing vessels were equipped and behaving in a way that

---

[86] Haeril Halim, Anggi M. Lubis, and Stefani Ribka, "RI Confronts China on Fishing," *Jakarta Post*, March 21, 2016.

[87] Joe Cochrane, "China's Coast Guard Rams Fishing Boat to Free It from Indonesian Authorities," *New York Times*, March 21, 2016.

[88] Indonesian official, interview with the authors, Jakarta, February 19, 2018.

[89] Indonesian official, interview with the authors, Jakarta, February 20, 2018.

[90] Morris, 2016.

suggested that they were part of the maritime militia, not regular Chinese fishermen.[91] China responded by filing a diplomatic note protesting Indonesia's action.[92] Both of these incidents brought into relief the challenge that China poses to Indonesian sovereignty within Natuna's EEZ and added to creeping mistrust over Chinese intentions among Indonesian policymakers.[93]

China has also used political manipulation and coercion to sow division within ASEAN, undermining the cohesiveness of the regional bloc and Indonesia's leadership position within it. ASEAN is central to Indonesian foreign policy, so challenges to the unity of the bloc are felt strongly by Indonesia. Because the security environment in the region is home to many flashpoints and is exacerbated by increasing U.S.-China rivalry, Indonesia is concerned with maintaining ASEAN's strategic autonomy, which Jakarta has long viewed as a prerequisite for regional autonomy. Indonesia worries that ASEAN members will lean toward Washington or Beijing and prioritize the interests of their great-power allies over their ASEAN partners.[94] This is precisely what happened in the disagreement over ASEAN's 2012 Chairman's statement, when Cambodia reportedly acquiesced to Chinese demands to withhold language critical of Beijing in the SCS, resulting in the failure to issue a joint statement for the first time in the history of ASEAN.[95] Interviews noted China's "strong-arm" tactics to "divide and conquer" within ASEAN since 2012, using its power of economic, political, and military influence to muzzle criticism of China's behavior in the SCS.[96]

---

91 Indonesian officials, interview with the authors, Jakarta, February 19–20 2018.

92 Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Hua Chunying's Remarks on Indonesian Navy Vessels Harassing and Shooting Chinese Fishing Boats and Fishermen," Beijing, June 19, 2016.

93 Indonesian official, interview with the authors, Jakarta, February 19, 2018.

94 Indonesian official, interview with the authors, Jakarta, February 20, 2018.

95 "Asean Nations Fail to Reach Agreement on South China Sea," BBC News, July 13, 2012.

96 Indonesian official, interview with the authors, Jakarta, February 20, 2018.

How Has Indonesia Responded to Gray Zone Threats from China?

Because of Indonesia's historical adherence to a nonaligned foreign policy (what is referred to as *bebas-aktif*, or the *free and active* principle), it is greatly limited in the kinds of actions it can take to counter Chinese gray zone activities. This policy also limits the kinds of diplomatic and military posturing that Indonesia can adopt to express displeasure with Chinese behavior and deter aggression.

The most vocal opponent of Chinese gray actions has been Indonesian Minister of Maritime Affairs and Fisheries Susi Pudjiastuti. After the aforementioned incidents between Indonesia and China in the SCS, for example, she held a news conference in which she criticized Chinese actions as "arrogant" and said that they "sabotaged Indonesian efforts to promote peace in the South China Sea."[97] She also summoned the Chinese ambassador for clarification, an action typically delegated to the Indonesian Ministry of Foreign Affairs.[98]

Soon after the maritime clashes with China, Indonesian President Joko Widodo, known as Jokowi, also responded by visiting the Natuna Islands with several ministers and held a limited cabinet meeting aboard an Indonesia naval vessel.[99] Notably, the move was accompanied by a series of conciliatory statements by Indonesian officials meant to assuage Chinese concerns. Jokowi stated that Indonesia was "still hoping to build a strong diplomatic relationship" with China, while Minister Luhut Binsar Pandjaitan—at the time, the Coordinating Minister for Political, Legal, and Security Affairs—issued a statement assuring Beijing that there were "no hostile intentions against China."[100] The public statements highlight the balancing act that Indonesia plays with China while taking measures to signal disapproval of Chinese coercion when necessary.

---

[97] Cochrane, 2016.

[98] Emirza Adi Syailendra, "A Nonbalancing Act: Explaining Indonesia's Failure to Balance Against the Chinese Threat," *Asian Security*, Vol. 13, No. 3, September 5, 2017a.

[99] "Indonesia's Jokowi Holds Cabinet Meeting on Warship in Disputed Sea," *Kyodo News*, June 23, 2016.

[100] Prima Gumilang, "Indonesia Tegaskan Tak Berniat Konfrontasi dengan China" ["Indonesia Clarifies That It Has No Hostile Intents Towards China"], CNN Indonesia, June 23, 2016.

The Indonesian military has responded in various ways to Chinese gray zone activity, especially after the two incidents with China in 2016. First, the Indonesian Navy took the lead in patrolling the Natuna EEZ to combat increasing incursions by Chinese fishermen; the area had previously been patrolled primarily by Indonesian maritime law enforcement vessels.[101] Second, the military accelerated plans to reinforce deployments in Natuna to defend Indonesian sovereignty, and Indonesia's air force held its largest military exercise near Natuna waters in October 2016.[102] Third, the Indonesian navy and coast guard have invested in patrol vessels to increase their capacity to patrol Indonesian waters.[103] And fourth, in July 2017, Indonesian officials announced that they had renamed the waters northeast of the Natuna Islands, at the far southern end of the SCS, the North Natuna Sea. Indonesian officials were quick to emphasize that they were not renaming the entire SCS, only the part that falls under their claimed EEZ.[104] However, the move can be interpreted as an attempt to use legal recourse to assert the exclusive rights to the living and nonliving resources in this area while tacitly challenging Chinese claims in the process.

Singapore

Types of Gray Zone Threats Faced by Singapore

Unlike the Philippines and Vietnam, Singapore does not have a territorial dispute with China and, as a result, confronts far fewer and less-belligerent gray zone provocations from China. However, most officials and scholars in Singapore noted an increase in Chinese "activism" to compel Singapore to support Chinese interests and not speak

[101] Morris, 2016.

[102] "Indonesia Reinforces Its Command over Natuna Waters Through Military Bases," *Jakarta Post*, September 27, 2016; and Agustinus Beo Da Costa and Randy Fabi, "Indonesia Air Force Holds Its Largest Military Exercise in South China Sea," Reuters, October 4, 2016.

[103] See, for example, Ridzwan Rahmat, "Indonesia Leans Towards Iver Huitfeldt Class for Frigate Acquisition," *Jane's 360*, March 12, 2019.

[104] Tom Allard and Bernadette Christina Munthe, "Asserting Sovereignty, Indonesia Renames Part of South China Sea," Reuters, July 14, 2017.

out against Chinese actions in the SCS. For example, when Singapore issued a statement in support of the PCA ruling in July 2016, in which Singapore called on "all parties to abide by the ruling," China expressed its displeasure to Singapore behind closed doors.[105] Six months later, nine Terrex armored troop carriers of the Singapore Armed Forces were detained in a Hong Kong port for nearly two months, and our interviewees cited this incident as another instance of Chinese gray zone coercion.[106] The vehicles were being shipped from Taiwan to Singapore after a military exercise, and some in Singapore believe that the confiscation was China's signal to Singapore to cease the annual military exercises with Taiwan.[107]

Officials and scholars interviewed for this report highlighted Singapore's "unique" foreign policy identity as a "hub" for multilateral diplomacy in Asia. This identity prompts Singapore, in some instances, to exercise caution and restraint in pushing back too hard against any single major power in the region for fear of being seen as taking sides between the United States and China.[108]

Singapore does have close security ties with the United States, hosting a rotational presence of U.S. Navy P-8 aircraft and littoral combat ships, for example. Interviewees noted that, in the past, China was primarily interested in pursuing economic and political ties with Singapore. Now, however, China is becoming more vocal about wanting closer security ties as well, discussing the issue at recent ASEAN meetings.[109] If China were to request some kind of rotational military presence in Singapore akin to that of the United States, for example,

---

[105] Singaporean official, interview with the authors, Singapore, February 10, 2018. See also "The Hague Ruling: Singapore Urges Parties to Respect Legal and Diplomatic Processes, Exercise Self-Restraint," *Straits Times*, July 12, 2016.

[106] Singapore official, interview with the authors, Singapore, February 9, 2018.

[107] Royston Sim, "Hong Kong to Return 9 SAF Terrex Vehicles to Singapore: Ministry of Foreign Affairs," *Straits Times*, January 24, 2017.

[108] Singaporean academics, interview with the authors, Singapore, February 8, 2018.

[109] Singaporean academic, interview with the authors, Singapore, February 9, 2018.

Singapore would be put "in a bind," given its close military ties with the United States.[110]

Finally, officials and scholars noted a high degree of sensitivity to Chinese economic presence in Singapore, given that many industries in Singapore are owned or run by ethnic Chinese Singaporeans. There is a fear that China might someday use its economic leverage over Singapore to punish it if its leaders undertake policies that Beijing does not like.[111] That has yet to materialize, however.

How Has Singapore Responded to Gray Zone Threats from China?

Singapore has responded to most forms of Chinese pressure or coercion primarily by issuing diplomatic statements supporting the rules-based order, including rhetoric supporting freedom of navigation in the SCS, respecting international law, and supporting free and unimpeded trade. Interviewees noted that, since the 2016 PCA ruling, there has been a shift in Chinese perceptions of the term *rules-based order*: Beijing increasingly views the term as representing a strategy directed at constraining Chinese behavior and damaging China's image in the international community.[112]

Singapore's role as host to the Shangri-La Dialogue is another way that Singapore supports dialogue and forms consensus on many issues of concern regarding China. The forum typically features major policy speeches by ministers of defense and has included some strong language by U.S. and regional defense officials on Chinese actions.[113]

Singapore has also sought to facilitate and bolster U.S. presence in the region. One interviewee highlighted two examples of continuing U.S.-Singapore defense ties: Singapore's granting of access to U.S. Navy littoral combat ships and maritime surveillance aircraft on a rotational basis from the Changi naval base and the construction of

---

[110] Singaporean academic, interview with the authors, Singapore, February 9, 2018.

[111] Retired Singaporean official, interview with the authors, Singapore, February 10, 2018.

[112] Singaporean academic, interview with the authors, Singapore, February 8, 2018.

[113] Joshua Berlinger, "Mattis Takes Hard Line on China in Singapore Speech," CNN, June 2, 2018.

docking facilities capable of hosting a U.S. Navy aircraft carrier.[114] Singapore relies on this U.S. presence to help contribute to regional peace and stability, protect sea lines of communication (such as the Strait of Malacca), and maintain a forward presence in case of humanitarian situations in the area. However, given Singapore's identity as mediator-in-chief in Asia and its desire for all countries to get along and resolve their differences peacefully through dialogue, there are clear limitations to Singapore's willingness to push back against Chinese gray zone actions.

Australia

Types of Gray Zone Threats Faced by Australia

Like Singapore, Australia does not have overlapping territorial or maritime claims with China; therefore, it does not face the types of coercive gray zone threats that the countries in East and Southeast Asia confront. However, Australia does face diplomatic and military pressure as an ally of the United States and when, for example, Australia speaks up in support of the rules-based order; conducts naval operations near the disputed waters of the SCS; pursues an enhanced Quadrilateral Security Dialogue involving Japan, India, and the United States; or speaks out against Chinese violations of human rights or Chinese political activities in Australia.

Chinese gray zone actions over the past few years have laid bare examples of alleged interference by the Chinese state into Australian politics and civil society, which have served to add to a general sense of mistrust over Chinese intentions toward Australia. The role of Chinese covert funding in the education and think-tank system, via either donations or Chinese government–backed initiatives (e.g., Confucius Institutes), has come under scrutiny. Australian media have shed light on the local operations of the Chinese United Front Work Department and other agencies of the Chinese Communist Party inside Australia. The issue came to the fore after the December 2017 resignation of Sam

[114] Singaporean academic, interview with the authors, Singapore, February 9, 2018.

Dastyari, a member of the Australian Parliament, over his connections with Huang Xiangmo, an Australia-based Chinese businessman with apparent links to the Chinese Communist Party, and suspicions of Dastyari being compromised by Chinese Communist Party interests.[115] Cases of Chinese influence in Australian universities, media outlets, and nonprofit organizations have only added to concern that Australia has been compromised by Chinese political subversion activities on Australian soil.[116]

China has also increased its monitoring of Australian naval transit operations in the SCS. In April 2018, the PLAN issued "robust" challenges to three Australian warships traveling to Vietnam.[117] An Australian official whom we interviewed noted an increase in Chinese naval vessels challenging and shadowing Australian warships in the SCS in recent years.[118]

Finally, many interviewees expressed concern about Chinese economic dominance in Asia and China's subsequent ability to use this dominance as an instrument to coerce. As one of China's largest bilateral trade partners, Australia is attuned to the danger of overreliance on Chinese trade and how Beijing can use that overreliance to coerce Canberra in the same way Beijing has used coercion against other countries in Asia.[119]

How Has Australia Responded to Gray Zone Threats from China?

Australia has responded by stepping up diplomatic overtures and enhancing security relationships with allies and partners in the region. On the diplomatic front, Australia has responded by speaking out more

---

[115] Amy Remeikis, "Sam Dastyari Quits as Labor Senator over China Connections," *The Guardian*, December 11, 2017.

[116] "How China's 'Sharp Power' Is Muting Criticism Abroad," *The Economist*, December 14, 2017.

[117] "Australian Warships 'Challenged' by Chinese Navy in South China Sea," *The Guardian*, April 19, 2018.

[118] Australian defense official, interview with the authors, Canberra, February 27, 2018.

[119] Ian Hall, "Is it Time to Push Back Against China's Economic Statecraft?" Australian Institute of International Affairs, February 21, 2018.

forcefully in support of the rules-based order—for example, issuing one of the strongest-worded statements for China and the Philippines to "abide by the [July 2016 PCA] ruling, which is final and binding on both parties."[120] Interviewees noted that China expressed "anger and frustration" toward the Australian government after it issued the statement, which China took as Australia siding with the Philippines on the issue.[121] Another diplomatic overture was former Prime Minister Malcom Turnbull's efforts to rejuvenate the Quadrilateral Security Dialogue, which many interviewees mentioned was due to concern about the long-term strategy of China and efforts at destabilizing the rules-based order.[122]

Partly because of the Dastyari controversy and partly because of a Turnbull-ordered investigation in 2016 on the extent of foreign interference in Australian politics, Australia introduced sweeping legislation in June 2018 to counter foreign interference in domestic politics, with China as the primary target.[123] Legislation that directly calls out Chinese interference in Australian domestic politics stands in contrast to other countries in Asia grappling with issues of foreign interference; these countries have tended to adopt quiet diplomatic acts or discussed such concerns internally in their respective governments.

Finally, Australia's *2017 Foreign Policy White Paper* is notable in its subtle emphasis on Chinese gray zone actions as a challenge to Australian interests. In particular, the following passage was noteworthy for its emphasis on such behavior, without naming China explicitly:

> The international order is also being contested in other ways. Some states have increased their use of "measures short of war"

---

[120] Australian Government, Department of Foreign Affairs and Trade, "Australia Supports Peaceful Dispute Resolution in the South China Sea," media release, Canberra, July 12, 2016.

[121] Australian official, interview with the authors, Canberra, February 26, 2018.

[122] Australian official, interview with the authors, Canberra, February 26, 2018.

[123] Australian Government, National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, No. 67, Canberra, June 28, 2018. See also Stephanie Borys, "China's 'Brazen' and 'Aggressive' Political Interference Outlined in Top-Secret Report," ABC News, May 29, 2018.

> to pursue political and security objectives. Such measures include the use of non-state actors and other proxies, covert and paramilitary operations, economic coercion, cyber attacks, misinformation and media manipulation. In the United Nations, we have seen coordinated efforts to dilute universal human rights standards. Some states are active in asserting authoritarian models in opposition to open, democratic governance. International rules designed to help maintain peace and minimise the use of coercion are also being challenged. Australia's security is maintained primarily through our own strength, our alliance with the United States and our partnerships with other countries. Australia's security and prosperity would nonetheless suffer in a world governed by power alone. It is strongly in Australia's interests to seek to prevent the erosion of hard-won international rules and agreed norms of behaviour that promote global security.[124]

The document concludes with the following statement:

> Like all great powers, China will seek to influence the region to suit its own interests. As it does, a number of factors suggest we will face an increasingly complex and contested Indo–Pacific.[125]

On the defense front, partly in response to calls for Australia to contribute to a peaceful and stable Indo-Pacific, Australian air force aircraft regularly conduct surveillance flights in the SCS, typically as part of bilateral or multilateral exercises in Southeast Asia. In addition, the Australian Navy has been conducting "presence operations" in the SCS with more frequency over the past few years.[126]

---

[124] Australian Government, *2017 Foreign Policy White Paper*, Canberra, 2017, p. 24.

[125] Australian Government, 2017, p. 26.

[126] "Australia Warships Sent to South China Sea for Military Exercises," *Daily Telegraph*, September 18, 2017.

Overall Findings: Field Research in East and Southeast Asia

Japan

Japan believes that it is engaged in an increasingly high-stakes competition with China over activities that Japan sees as subversive and coercive efforts to change the status quo of territorial sovereignty and administrative control of the Senkaku Islands and nearby areas. There is a consensus within policymaking circles in Japan that it has been largely effective at managing China's gray zone challenges by deterring China from taking more-provocative actions challenging Japanese sovereignty within Senkaku waters and airspace, such as landing on or attempting to capture the islands. At the same time, there is an acknowledgment that Japan has not been effective at preventing all types of Chinese gray zone activities. Despite JCG's persistent presence, for example, it has not been able to stop China; rather, its activities have successfully contained Chinese intrusions to "several hours."[127] Similarly, CCG has not escalated its activities to include provocative acts, such a ramming, shouldering, or harassing other countries' law enforcement or fishing vessels in the SCS, and JCG has successfully expelled Chinese fishing boats that enter the Senkakus' territorial waters without incident.

However, overall trends do not bode well for Japan. Recent CCG patrols have featured the presence of vessels that are more heavily armed. Chinese maritime militia vessels continue to penetrate the Senkaku territorial sea with increasing regularity. Although Japan can continue to play defense against Chinese probing tactics, a change in China's strategy in favor of more, better-armed, and more-provocative penetrations by CCG and maritime militia vessels could strain Japan's capacity to respond without increasing the potential for conflict.

The same is true for responses from the Japan Ministry of Defense and JSDF. Although there is a general consensus in Japan's defense establishment that modernization efforts within the various JSDF services make the forces better postured, trained, and equipped to handle

[127] Japanese military official, interview with the authors, Tokyo, January 15, 2018.

escalation dominance with China, Chinese activities challenging Japanese sovereignty have continued in scale and scope.[128]

Southeast Asia

In recent years, countries in Southeast Asia have grown increasingly wary of China gray zone aggression in the SCS. These activities include the use of law enforcement and maritime militia vessels in an unprofessional and escalatory manner to deter or, in some cases, deny the use of living and nonliving resources in the SCS. Such CCG tactics as bumping, shouldering, ramming, and using water cannons against other nations' coast guard and fishing vessels were highlighted as particularly destabilizing. Interviewees also highlighted the use of a maritime militia, whose vessels, personnel, and training are largely believed to be under the authority of the Chinese state. China's unprecedented expansion of artificial islands in the SCS and subsequent construction of logistics, maintenance, and storage facilities, along with airstrips, harbors, ports, and armament platforms, have fundamentally shifted the balance of power and capability to control the SCS in favor of China. Finally, China's use of economic coercion and political subversion within all of the countries that we examined are challenging norms of statecraft and confidence-building in the region.

For the most part, countries in Southeast Asia have identified the challenge from Chinese gray zone activities and seek to deter further attacks when feasible and appropriate, but the countries remain constrained by their military capacity to deter and by nonaligned foreign policy orientations that prevent more-forceful displays of confrontation.

---

[128] Japanese official, interview with the authors, Tokyo, January 18, 2018.

CHAPTER FIVE

Responding to the Gray Zone Challenge: A Strategic Concept

Much of the literature about the gray zone challenge has focused on identifying and characterizing the problem. Some analysts have proposed U.S. responses but focused on the idea of deterring gray zone aggression, not offering a framework for responding in all dimensions—namely, military, diplomatic, informational, and economic.[1] Rather than recommending that the United States merely remain on the defensive, we recommend a more comprehensive approach by going on the offensive—and adopting a whole-of-government approach to the problem.

In evaluating response options for gray zone activities, we first sought to develop a general strategic concept that would allow the United States to go beyond case-by-case reaction, knitting together individual actions to achieve more-meaningful results over the long term. Such a strategic concept must explicitly state the claims or assumptions that form the basis for the concept, embody a basic theory of success, and offer a framework for designing policies that put the strategy into effect. Each of the main sections in this chapter treats one of these criteria, and the analysis and recommendations in this chapter are grounded primarily in the lessons of our field research. In the final

[1] For useful analysis on gray zone responses in Asia, see John Schaus, Michael Matlaga, Kathleen H. Hicks, Heather A. Conley, and Jeff Rathke, "What Works: Countering Gray Zone Coercion," Center for Strategic and International Studies, CSIS Briefs, July 16, 2018; Hal Brands and Zack Cooper, "Getting Serious About Strategy in the South China Sea," *Naval War College Review*, Vol. 71, No. 1, Winter 2018; and James R. Holmes and Toshi Yoshihara, "Deterring China in the 'Gray Zone': Lessons of the South China Sea for U.S. Alliances," *Orbis*, Vol. 61, No. 3, May 2017.

chapter, Chapter Six, we highlight specific ways that the United States can respond based on these overarching principles.

Principles Governing a Strategy

We used our research into the character of the gray zone challenge and, in developing a strategic concept, derived nine principles that should guide the U.S. response.

The first and most important strategic principle is that *the United States should not merely seek to mitigate losses in the gray zone but also aim to gain strategic advantage*. In almost all areas of gray zone competition, the United States remains in a relatively advantageous moral and material position vis-à-vis the primary aggressors of Russia and China. The United States, therefore, should leverage all tools of statecraft to improve its relative position while controlling risks of escalation.

The second principle flows directly from the first: *In seeking strategic advantage, the United States should be proactive rather than reactive in its approach to the gray zone challenge*. Part of the problem is that the United States has been ceding initiative to others. Within the span of just a few years, China has reclaimed more than 3,000 acres of land in the SCS and exerted increasing control of the sea and airspace of this vast area of water. The speed with which China reclaimed these islands caught everyone, including the United States, off guard. Furthermore, Chinese civilian, government, and military vessels have significantly enlarged their presence in the ECS and SCS in an attempt to discourage or deny other nations from operating unimpeded in contested waters. Russia has greatly expanded the scale and sophistication of political manipulation campaigns against Western governments and NATO. Reacting proactively to a larger set of coercive Russian and Chinese actions will help deter future aggression.

Third, and relatedly, *a core element of successful gray zone strategy is the ability to respond quickly to new provocations*. The United States and its allies and partners will need to answer potential gray zone initiatives quickly and decisively without waiting weeks or even days. This requirement demands strong policy and crisis coordination mecha-

nisms that can allow quick responses. It points to the importance of developing and exercising scenarios before gray zone crises occur so that decisionmakers and analysts can game out possible answers and lay the groundwork for fast reactions. Only through forward presence with the capacity to respond rapidly will the United States and its allies have the necessary capabilities on hand for swift action.

Fourth, *the United States should attempt to lead through multilateral processes and institutions even while being prepared for "go-it-alone" responses when U.S. leadership is essential to marshal a response*. Leading multilaterally can be difficult because the gray zone actions examined in this study affect U.S. allies and partners in more-direct ways than they affect the United States, and those countries have greater national interests at stake; in addition, the countries will have constraints on their responses that limit any joint action. Furthermore, some gray zone aggression is specifically tailored to bog down multilateral responses—for example, tactics for which culpability is misattributed or that are below conventional military activity (complicating a NATO response to Russia) or tactics that incite a general unwillingness to undertake overtly aggressive policies (complicating an ASEAN response to China). On the other hand, our field research strongly supports the conclusion that Russian and Chinese gray zone coercion activities have generated such significant threat perceptions in both regions that, in many cases, the targeted countries either cannot or do not want to respond to the gray zone tactics for fear of upsetting the aggressor. These growing threat perceptions can be a major U.S. competitive advantage because the targeted countries seek to block and counter Chinese and Russian aggressive actions in the gray zone and look to the United States to help. Therefore, the United States should seek to rally multilateral institutions, alliances, and coalitions of the willing to push back against Russia and China. But the United States should also be willing to adopt a broader array of unilateral actions or actions that smaller numbers of partners may be willing to participate in, taking into account risks of escalation and other issues.

This leads to a fifth and related principle: *U.S. responses must be aligned with local partners to the greatest extent possible*. This principle may pose a significant constraint on U.S. actions because, as noted

earlier, many states in both Europe and Asia have different views about the degree of threat posed by Russia and China, the degree of confrontation they are willing to undertake, and the level of partnership they will accept with the United States. The United States must therefore strike the right balance between (1) these differing views and hesitations about escalation and (2) the need for more-forceful responses that might deter gray zone actions but might, in the process, alienate possible allies. The United States must push back hard enough to make a difference but not so hard that it antagonizes local partners.

Sixth, *any strategy for responding to gray zone aggression must balance excessive risks of escalation—including military, diplomatic, and economic aspects—with the reality that, to be effective, countering gray zone aggression demands some degree of risk tolerance*. A dominant U.S. objective in responding to gray zone activity is to avoid major war. However, to achieve lasting gains against gray zone behavior, the United States and its allies must be willing to put a certain amount of escalation risk on the line in pursuit of gray zone deterrence and response. Some of the policy responses that we propose in the next chapter include, for example, out-of-area measures in response to local gray zone actions, which introduce escalation concerns. Such risk-related responses, however, are proposed simply in the spirit of offering a menu of options on a continuum of escalation potential. In developing a more detailed strategy for gray zone responses, the United States cannot assume that more-powerful and blunt pushback is always the best strategy; managing the threat posed to Russia and China, and overall escalation risks, must be a leading goal of the process.

Seventh, *gray zone tactics are a symptom of broader regional ambitions and grievances and cannot be addressed outside that context*. Both Russia and China are pursuing specific goals—and dealing with specific threat perceptions—in their regions. Gray zone techniques are only one tool being used to pursue those goals. U.S. gray zone responses are about accomplishing small wins in specific areas to send a signal, not about containing an adversary in all domains. Thus, the United States is not going to solve the underlying cause of the gray zone dispute (for example, sovereignty of disputed territory)

with either Russia or China by undertaking new or innovative tactical responses.

An eighth principle underpinning this proposed strategic concept is that *Russia and China continue to value their status as legitimate and respected members of the international system*.[2] They are not yet willing to abandon concern about such status in exchange for unrestrained aggressive opportunities in the gray zone or other realms. This reality provides the United States with significant leverage by making Moscow and Beijing sensitive to the public costs of overtly aggressive actions in these spheres and potentially vulnerable to powerful information campaigns designed to make them pay a reputational cost for those actions.

Finally, ninth, *not all gray zone aggression has equal significance for the security of regional allies and partners or for global norms*. A Chinese paramilitary assault on the Senkaku Islands would constitute a direct threat to the sovereignty of an ally, whereas Russian efforts to cultivate political influence and to shape narratives in regional countries are of a less immediate concern that must be dealt with over time. Gray zone threats are not all created alike, and neither are their responses. Some gray zone threats require immediate action, while others may require long-term persistent dissuasion through political messaging.

Working Toward a Strategy: A Theory of Success

Any meaningful strategic concept to gain strategic advantage must be based on a theory of success—an argument for why specific policies are likely to produce desired outcomes. Some causal link must bind means to ends, explaining why the actions undertaken as part of the strategy will lead to or support those ends. The theory of success that we propose in this analysis is grounded in the nine principles listed in

[2] See Andrew Radin and Clinton Bruce Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017; and Timothy Heath, Michael J. Mazarr, and Astrid Stuth Cevallos, *China and the International Order*, Santa Monica, Calif.: RAND Corporation, RR-2423-OSD, 2018.

the previous section. Those principles describe a situation in which the following are true:

- Russia and China are using gray zone techniques as a way of expressing dissatisfaction with aspects of the regional power and territorial status quo.
- Both are employing such tactics precisely because they want to express those desires and demands without completely alienating themselves from the international community and undermining their claim to great-power status and privileges.
- All significant regional players see these activities as a threat and have a significant—though, in many cases, constrained—appetite for U.S. leadership of responses.
- The gray zone encompasses a wide spectrum of activities that pose consistent short- or long-term risks, and the various levels of threat must be carefully distinguished.
- Many of those tactics take place in such realms as competing over narratives, gaining political influence, and managing economic relations in which the United States and its allies and partners have, or ought to have, natural advantages.

These aspects of the gray zone context suggest the potential value of a theory of success that builds on the essential post–World War II U.S. grand strategic posture: building, leading, and speaking in the collective name of an informal community of status-quo states committed to international norms and rules. In other words, the concept of a rules-based order remains a highly appealing concept to rally support in Europe and Asia and offers the United States an opportunity to significantly strengthen its hand in the unfolding competition by using reactions to Chinese and Russian aggressiveness as the basis for strengthened regional postures. In the process, U.S. strategy can make clear to Beijing and Moscow the costs they are incurring as a result of these strategies.

Pushing the envelope on responses—that is, manipulating the risk of escalation for coercive leverage—can serve U.S. and allied purposes in some cases but not all. On the one hand, both Russia and

China seek to avoid outright military clashes with the United States. The whole point of their gray zone approaches is to remain below the threshold of armed conflict. Thus, in some cases, more-escalatory U.S. responses could serve to call the bluff of Russia and China by forcing them to either change course or out-escalate the United States and its allies; our field research indicates that the latter option is unlikely in most instances. On the other hand, a strategic concept based solely around using every gray zone provocation as an invitation to out-escalate Russia and China would be neither prudent nor effective. Any escalatory steps obviously carry certain risks of unintended or accidental conflict. More than that, the United States will not be able to adopt a blanket approach of pushing the envelope in risk for several reasons. First, U.S. allies and partners will often have even less risk tolerance than Russia or China does. If the allies and partners are not on board, it may be politically and operationally difficult for the United States to undertake escalatory coercion on its own. Second, both Russia and China, but especially the latter, might welcome an opportunity to teach U.S. allies and partners a lesson closer to the threshold of warfare. Should Japan, for example, dispatch naval assets to counteract CCG coercion of the Senkaku Islands, Beijing might see an opportunity to engage in a limited clash that leaves Japan wounded and chastened. Finally, if the United States becomes the catalyst of escalation or seen as overly belligerent, it risks losing its position as the defender, creating international reactions that blame the United States for the danger of war and lose sight of the original Russian or Chinese provocations.

Thus, the theory of success underlying the strategic concept that we propose could be stated as the following:

> The combination of intensified multilateral pressure, the identification of specific red lines, the credible commitment of U.S. military and economic power, and expanded diplomatic efforts to address Chinese and Russian concerns can shift the risk and cost calculus for certain gray zone actions onto the aggressor, partly by playing to Chinese and Russian desires to preserve their international status and avoid regional balancing.

To produce a comprehensive strategic concept, the United States can join this theory of success with direct actions to gain advantage in persistent areas of competition.

An important consideration in this space is that the Russian and Chinese reactions to U.S. gray zone responses will be a function of the strategic context and the recipient of gray zone aggression. If China's relations with Japan are especially bad, for example, and nationalist sentiment is running at a fevered pitch in China, Beijing may feel empowered—and compelled—to respond more violently to Japanese pushback than it would at times of more-stable relations. Response options, therefore, will vary depending on the situation and geopolitical context at the time.

The theory of success that we propose here aims to marry enhanced multilateral cooperation with U.S. diplomatic and military power to change the balance of costs and risks affecting perceptions in Moscow and Beijing. That basic dynamic would be used to *deter* the most dangerous gray zone adventurism and to *dissuade* many other actions in this sphere over time. To achieve both of those objectives, the United States can take *context-setting initiatives* to shape the strategic environment. And finally, because those efforts will not prevent all gray zone activities, the United States should work with allies and partners to *enhance resilience and build tools for competitive success* against less-aggressive, more-gradual gray zone tactics, which are likely to remain persistent.

A Concept for Gaining Strategic Advantage in the Gray Zone

Not all gray zone activities are alike. Responses to more-aggressive gray zone activities will not necessarily mirror responses to more-gradual, persistent initiatives. Any strategic concept for the gray zone therefore must distinguish among the various levels and design its responses accordingly. Table 5.1 lays out a three-part categorization of gray zone activity levels, which can help to scope responses.

Table 5.1
Levels of Gray Zone Activities

Level	Characteristics	Examples
Aggressive	• Direct quasi-military or military action • Usually attributable • Significant threat to territorial integrity or sovereignty • Forces an immediate binary choice in response • Often a clear violation of international law	Seizing of new territory in the ECS or SCS; kinetic force against NATO troops or nations or against Japanese or Philippine troops or assets
Moderate	• Direct action, though often in nonmilitary form • Usually attributable • Goal is establishing claims and coercion • Does not immediately threaten territorial integrity • Legal status of actions is highly contested	Estonia cyberattack; ramming of vessels in the ECS and SCS; fishing boat swarms; declaring an ADIZ in the SCS; economic coercion; closing of borders
Persistent	• Broad-based, low-level routine actions as part of a campaign • Does not clearly violate any international law or norms • Ongoing pattern rather than individual events • Often done in a way that clouds attribution	Broad disinformation or messaging efforts; Chinese passage through Senkaku territorial seas; Chinese maritime militia presence in disputed waters

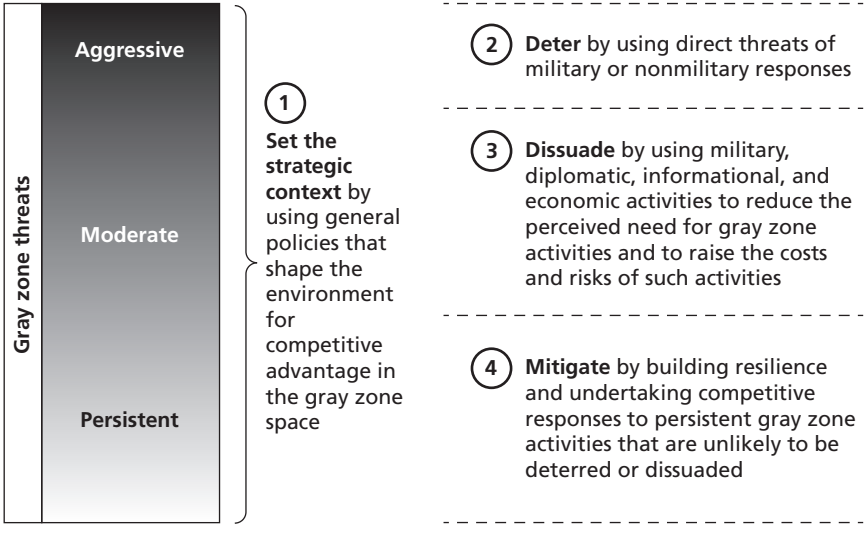
Admittedly, the dividing lines between the levels will not be precise or well defined in all cases. Rather, they are designed to convey three general conceptual ideas rather than three clearly defined baskets. The three general types of gray zone activities are (1) *aggressive* actions, at one end of the spectrum, that the United States should seek to deter; (2) *persistent* actions, at the opposite end of the spectrum, that it must live with but can compete against; and (3) *moderate* actions in the middle that the United States should actively seek to discourage over time. These distinctions then become the basis for the response concept.

The gray zone actions within these three categories—aggressive, moderate, and persistent—aim to achieve different objectives using different tools over varying time frames. This division of gray zone activities points to one especially critical implication and a theme that our

research suggests is essential to any U.S. response strategy. The United States and its allies, partners, and friends *must decide what actions they will resolutely not tolerate* in the gray zone environment. Determining which possible forms or specific examples of gray zone tactics fit into the first category in Table 5.1 (aggressive) is arguably the central task facing U.S. planners. Because of the difficulty in stopping gradual, sometimes unattributable actions involving secondary interests, identifying the actions that the United States will seek to deter is the one reliable way to draw a boundary around the possible effects of gray zone encroachment.

With these broad levels of gray zone tactics, we offer a four-part framework for responding to gray zone threats, shown in Figure 5.1. As seen in the figure, the proposed strategic concept first calls for a whole-of-government approach utilizing geopolitical, military, and economic actions to shape the strategic context. Second, it proposes that the United States should identify a small number of aggressive forms of gray zone tactics to deter with explicit, credible threats of military or nonmilitary responses. Third, it seeks to dissuade a wider

Figure 5.1
Overarching Strategic Concept for Responding to Gray Zone Threats



range of moderate gray zone activities over time. Finally, it calls for mitigating persistent threats by building a capability for resilience and competitive responses to tactics that cannot be deterred or dissuaded.

This framework necessarily simplifies what is and will remain a more complex reality in which the United States and others are engaged in the simultaneous pursuit of a full range of approaches and objectives whose boundaries are often obscure. These approaches include deterring, discouraging, and dissuading gray zone aggression; punishing actions that do occur; creating cost-imposing dynamics that shape intentions; improving resilience to deny the goals of gray zone activities; and coercing an end to ongoing activities. The purpose of the framework is not to create rigid categories for all response options but rather to convey the basic strategic concept involved. In particular, the strategy is built around four complementary efforts: to shape a context supportive of U.S. and partner objectives; to deter a handful of very extreme forms of gray zone aggression; to dissuade the day-to-day use of more-elaborate gray zone techniques; and to sustain resilience in the lower-level, ongoing competition areas. Within that set of endeavors, many strategies will necessarily be employed on specific issues.

Next, we describe each of the strategic concept's four aspects in more detail.

1. Set the Strategic Context

The gray zone competition is long term, gradual, and aimed at broad geopolitical goals. It is therefore different from strategic tasks (such as deterring interstate aggression), which—at least typically—depend on local factors for their success. The gray zone challenge is an integral component of the wider geopolitical and strategic competition. Setting the overall strategic context for success, therefore, is a critical component of any gray zone strategy.

In setting that context, the United States should have four objectives. It should reinforce its credibility and reliability as a partner of local states receiving the brunt of gray zone provocations (without offering a blank check for those states to spark crises and expect unconditional U.S. support). It should strengthen the global narrative about the extent to which gray zone actions undermine the rules-

based international order, and it should intensify international reactions to Russian or Chinese aggression. It should take multiple steps to stabilize and, where possible, mitigate the intensity of the strategic competition—by promoting or buttressing confidence-building measures and continuing to support international institutions and agreements, such as the United Nations and arms-control treaties—to reduce the risk of escalation from gray zone clashes. And finally, the United States must enhance the U.S. government's institutional oversight of the gray zone challenge.

Our research suggests several specific initiatives that could contribute to these objectives. First, to reinforce the credibility of U.S. regional roles, the United States could do the following:

- Continue to reaffirm, through regular senior leader statements and official policy documents, the U.S. commitment to formal allies in Europe and Asia and back these statements with enhanced participation in bilateral and multilateral forums to deal specifically with such gray zone tactics as cyberattacks and disinformation.
- Enhance U.S. levels of participation in other regional institutions, including the EU and ASEAN.
- Modestly enhance U.S. forward posture levels in or near Germany, Poland, Japan, and the SCS to signal U.S. commitment.
- Continue to expand on a robust set of exercises, train-and-advise missions, and rotational presence operations in Europe and Asia, particularly those devoted explicitly to gray zone contingencies.

Second, to shape the global narrative on gray zone activities, the United States could take the following diplomatic and informational steps to highlight the risks of gray zone aggression:

- The United States could undertake a major diplomatic initiative, coordinated through the State Department and U.S. embassies, to reinforce the international legal implications of gray zone aggression. This theme should become a significant focus of U.S. diplomatic dialogues in both bilateral diplomacy and multilateral forums (e.g., Group of Twenty, EU, ASEAN, Quadrilateral Secu-

rity Dialogue). A lead example in Asia is the use of the 2016 PCA ruling to demonstrate the verdict of international law on specific Chinese claims in the SCS.

- Such a formal diplomatic initiative could be matched with support for parallel Track 1.5 dialogues throughout both regions to promote discussion of the issues among scholars, researchers, journalists, and officials.[3]
- As part of the initiative, the United States could recruit diplomatic partners in each region willing to be forthright about gray zone risks and provocations and to serve as an ongoing bridge, in diplomatic contacts and policy development, between the United States and more-reluctant partners. In Asia, such partners might include Australia and Japan; in Europe, Great Britain and Sweden.
- The United States could undertake a major public diplomacy campaign to shape the global narrative on gray zone aggression and make the issue, including the development of country strategies, a priority effort of global U.S. public diplomacy. This would include highlighting, during heads-of-state and minister of defense meetings in Asia and Europe, the destabilizing nature of gray zone activities that threaten all nations, large and small. It would also include official and public outreach in key countries affected by the phenomenon, as well as other nations. In the process, the United States could support the establishment of multilateral, nongovernmental institutes in Asia and Europe focused on gray zone transparency—publishing video, photographs, and other evidence of ongoing aggression; cataloguing events; creating social media tools to allow local individuals to document activities; and conducting analysis.[4]

---

[3] *Track 1.5 diplomacy* is a term used to describe discussions that involve a combination of official and nonofficial actors engaged in conflict resolution in an informal setting.

[4] We acknowledge the potential that increased transparency of gray zone transgressions may exacerbate the problem if there are no effective U.S. or allied responses. However, the benefit of publicizing and documenting gray zone aggression over time outweighs the danger of not responding in every instance, in our opinion.

Third, the United States should take steps to stabilize relations with China and Russia in ways that reduce the escalatory risks of gray zone confrontations and, beyond that, work to address these rivals' security concerns in ways that make it less likely that they see a need to undertake more-aggressive gray zone actions. This strategy may be more possible in Europe, where Russia's conception of its natural role is somewhat less dominant than China's vision for itself in Asia. It remains to be seen how much room there is for such accommodation with China, given its elaborate goals for regional hegemony; at a minimum, however, such efforts would signal to other regional actors that the United States is making every effort to reduce the intensity of gray zone competition before becoming more aggressive itself. This effort would therefore set the context for some of the specific measures proposed to deter and dissuade certain gray zone actions (discussed later). Moreover, as in the Helsinki process in the 1970s, for example, such agreements can be useful in getting rivals to endorse principles—such as sovereign noninterference and human rights—that help justify strong pushback to their aggressive activities. Specific examples of context-setting measures in this category include the following:

- Initiating new dialogues designed to generate improved regional security architectures that respect basic national security requirements of both countries. Such agreements, formal or informal, could take the form of agreements on deployment of military forces and capabilities, mutual commitments on political noninterference, and reaffirmations of norms of nonaggression.
- Expanded support for and engagement with regional conflict management forums and processes, including the North Pacific Coast Guard Forum, the ASEAN Code of Conduct negotiations, and NATO-Russia notification and communication mechanisms.
- Continued support for military-to-military forums and dialogues to establish clear rules of engagement and communication mechanisms to prevent unwanted crisis escalation.

Fourth, to enhance the institutional support for ongoing gray zone operations within the U.S. government, the United States should take the following steps:

- Establish a formal institutional home for strategy coordination and implementation. This could be housed in various places in the U.S. government, although the logical home is at either the State Department or the National Security Council. A fairly simple option for this requirement would be a presidentially directed interagency strategy with a senior director from the National Security Council serving as coordinator. A more institutionally robust option would be to create a dedicated office, akin to the Office of the Special Representative for Afghanistan and Pakistan, to develop concepts and strategies and oversee interagency implementation.
- Through presidential direction and departmental instructions, make gray zone strategy implementation a leading priority for regional offices in the Departments of State and Defense and a major component of relevant embassy country strategies.
- Establish regional implementation offices for Europe and Asia—that is, small command-like structures headed by regional coordinators who report to the interagency strategy coordination office and who serve as parallels to the military combatant commands for gray zone activities.
- Direct that Defense Department force development offices and the Department of State consider gray zone contingencies in the process of generating force requirements and diplomatic initiatives.
- Work with the military services to emphasize gray zone issues in career development, training and education, and the funding and support for technologies, capabilities, and experimental force design and concepts tailored to the gray zone.

A significant and underappreciated challenge in preparing for and undertaking gray zone responses is overcoming the bureaucratic barriers both within the allied or partner nation and between the United States and these nations. Silos between the countries' major national security agencies, tightly held mission areas of specific departments

(including classified information), civil-military tensions, and other factors can obstruct timely responses in some cases.

2. Deter Extreme or Highly Destabilizing Gray Zone Threats

The second component of the framework suggests that the United States and its regional allies and partners can attempt to deter a small number of the most-extreme, aggressive gray zone actions that border on outright attacks necessitating a military response. In so doing, the United States can help prevent the most-significant threats to U.S. and allied interests in this sphere and the most-perilous risks of escalation.[5]

In developing the framework, we relied on parallel RAND research on the requirements for deterrence in general and for deterring the most-aggressive gray zone activities.[6] That work suggests several key deterrence criteria that can potentially be satisfied for several of the most-extreme gray zone activities. Deterrence requirements that are typically challenging to meet in the gray zone include (1) having clarity in what will be deterred and what the deterring country will do in response and (2) ensuring that the aggressor believes that the country making the deterrence threat has the will to carry it out. These can be nearly impossible to meet for low-level, gradual, sometimes unattributable actions in the gray zone (i.e., the persistent threats from Table 5.1), but they can be met for more-significant actions.

These deterrence policies, as well as the policies associated with the dissuade and mitigate elements of the framework, would be tightly integrated with the context-setting activities described earlier. Any U.S. initiative to stress the international law aspects of the issue and gather multilateral support, for example, would feed naturally into the deterrent policies that we identify next, especially nonmilitary deterrence. Such an initiative would create the basis for recruiting support for deterrent policies.

---

[5] These actions closely match the concept that Ryan Martinson and Andrew Erickson have termed "definitive" actions in the gray zone; see Ryan D. Martinson and Andrew Erickson, "Re-Orienting American Sea Power for the China Challenge," *War on the Rocks*, May 10, 2018.

[6] The research will be described in a future report by Michael J. Mazarr, Joseph Cheravitch, Jeffrey W. Hornung, and Stephanie Pezard.

We employed three criteria to identify gray zone activities that justify policies of direct deterrence. First, the activities had to involve military or paramilitary aggression of some sort, in an overt and identifiable manner. Second, they had to involve threats to U.S. treaty allies or broad-based regional peace. And third, they had to reflect a significant risk of escalation to larger conflict. We acknowledge that some of the gray zone actions that we identified constitute clear acts of military aggression and thus move beyond the below-the-threshold actions typically associated with gray zone behavior. Therefore, the value of identifying such a list is to distill (from a wider range of actions) the quasi–gray zone or paramilitary activities that are unambiguously unacceptable to U.S. and allied leaders.

Based on those criteria, we identified the following actions toward the United States, its allies, or its partners that are considered clear violations of regional peace and security:

- Chinese paramilitary assault on the Senkaku Islands, which the United States has already clarified as being covered by the U.S.-Japan treaty relationship
- Chinese attack (with its military or coast guard units) on Philippine government or military vessels or aircraft operating in the SCS, thereby triggering the mutual-defense provisions in Article V of the U.S.-Philippine Mutual Defense Treaty[7]
- Russian military or paramilitary aggression against NATO members (e.g., paramilitary infiltration of the Baltic states accompanied by sabotage)
- Chinese kinetic attack against military vessels or occupied features of other claimants in the SCS.[8]

---

[7] U.S. defense of Philippine military or government assets under attack, even if operating in disputed territory in the SCS, does not equate to supporting the Philippines' position on sovereignty. See Article IV and V of Republic of the Philippines and the United States, *Mutual Defense Treaty Between the Republic of the Philippines and the United States of America*, Washington, D.C., August 30, 1951.

[8] Note that attacks on non-U.S. allies, while not invoking a mutual defense treaty, would nonetheless be regarded as a grave threat to peace and stability in the Asia-Pacific and would most likely be met with some sort of U.S. military response.

In addition, the United States should identify and publicize a second bin of actions that would generate immediate and significant *economic, informational, and diplomatic costs* for the aggressor in the region and beyond, with the possibility of limited U.S. or allied military response in certain instances. Our review of gray zone contingencies suggests the following four candidates for such a roster of gray zone actions:

- Chinese land reclamation at Scarborough Shoal
- Chinese declaration and enforcement of an ADIZ over the entire SCS
- Chinese seizure of new features in the SCS
- large-scale cyberattack of U.S. allies or partners, including
  - rendering critical public services inoperable or otherwise ineffective
  - swaying the outcome of a democratic election (based on forensic evidence)
  - threatening the domestic welfare in Europe or Asia.

To make its deterrence threats credible, the United States could take several other actions. Deterrence requires clarity and consistency, so once these targets of U.S. deterrent policy are in place, they must be reaffirmed in consistent public statements from senior U.S. officials. This is especially true of gray zone contingencies because potential aggressors have many reasons to believe that the United States might not respond. Whatever issues are selected for direct deterrence, they should be clearly enumerated and placed in public policy and strategy documents.

A critical component of any deterrence strategy involves close coordination with allies and partners. Joint response options involve first and foremost developing consensus on which gray zone actions fall into the "extreme aggression" bin and which do not. For the ones that are identified as falling outside of extreme aggression but within the second bin of aggression, joint response options must be discussed during bilateral visits. This requirement cannot be overemphasized. This would include highlighting, during heads-of-state and minister of

defense meetings in Asia and Europe, the destabilizing nature of gray zone activities and proposing new or expanded U.S. responses to be considered with the ally or partner.[9] Once the gray zone activities in these two narrow bands are decided, national security bureaucracies at all levels must hone bilateral communication mechanisms to ensure efficient and timely responses, considering the strategic communications, diplomatic, military, and economic dimensions of policymaking.[10]

To strengthen the will and capability to fulfill these threats, the United States should conduct a larger set of exercises with allies and partners to test responses to gray zone scenarios. This could include local military demonstrations—such as flyovers of Scarborough Shoals and Second Thomas Shoal, transit operations in the ECS, and additional rotational forces circulating through the Baltics—specifically targeted to reinforce the credibility of the enumerated deterrent threats. These types of activities, as well as specific U.S. playbook-type responses, are discussed in more detail in Chapter Six.

Finally, the United States can make modest investments in capabilities designed to support such gray zone contingencies. The United States could benefit from an enhanced ability to respond with paramilitary forces short of formal military escalation, including coast guard and law enforcement capabilities. It could also sell more advanced weapons to allies and partners in identified deterrent situations.

3. Dissuade Moderate Gray Zone Threats over Time

Not all, or even very many, gray zone activities are subject to rapid and powerful signals of deterrence. Many individual actions do not rise to the level of justifying a retaliatory response. Some cannot be clearly attributed to specific aggressors. In some cases—as we describe in the next section—this suggests that the only answer is ongoing competition, which means building resilience against certain gray zone tactics

---

[9] During our field research in Asia, for example, government officials expressed interest in understanding specific actions that the United States was willing to take jointly with the partner nation to deter gray zone aggression.

[10] A good example of discussions underway for joint responses is the U.S.-Japan operational plan for a Senkaku Islands contingency. See "Japan and U.S. to Formulate Armed Response to China Threat to Senkakus: Sources," *Japan Times*, November 4, 2018.

and creating tools to effectively compete in what will be a persistent series of moves and countermoves. Our analysis suggests that there is a category in between the aggressive and persistent threats—gray zone activities that the United States cannot reliably deter but should nonetheless attempt to make less common over time. For this category of gray zone actions, the required response is long-term *dissuasion* designed to both raise the costs for the aggressors and reduce the perceived necessity of the actions.

As noted earlier, there is no clear dividing line at either the upper or lower boundary of this category of gray zone activities (the moderate level in Table 5.1). Some observers, for example, might include the coercive harassment of fishing vessels in the SCS or disinformation attacks on democratic stability in Europe in the category of high-end (aggressive) gray zone actions that must be directly deterred. We find that, in most cases, neutralizing such activities does not necessitate immediate and aggressive counter-responses but rather long-term dissuasion campaigns.

Even more-comprehensive debates could take place about the dividing line at the lower end of this middle category. Activities at the low end of the gray zone (persistent threats) demand persistent responses and competition because they cannot be deterred or dissuaded. But distinguishing the gray zone actions that fit in the moderate category—not significant or blatant enough to call forth direct countermeasures but too serious to allow on a persistent basis—is a difficult and subjective challenge.

Our analysis suggests three criteria that can help identify gray zone activities that fall into this category. First, this category involves activities that are in some way hostile or coercive but short of the significant actions represented by the aggressive category. In most instances, such actions are persistent but low-level destabilizing acts rather than short, sharp, aggressive actions. Second, actions in this category have some significance for international rules or norms beyond the local case. Third, in many cases—for example, cyberattacks or disinformation campaigns—the culpability of the aggressor is not clear at the outset and thus takes time to ascertain. Based on those criteria, we propose the following actions that the United States should seek to dis-

suade over time, through a campaign of gradual pressure that increases the costs and reduces the perceived need for them:

- violent or hostile coercive actions by civilian actors or coast guard vessels against ships or aircraft operating in international waters or airspace (e.g., water cannon attacks on fishing vessels, ramming, or other unsafe approaches to patrol vessels or aircraft)
- threats against claimants in the SCS to not undertake oil or natural gas exploration activities in their own EEZs
- large-scale disinformation campaigns that sow confusion or discord in a democratic country.

Once the actions constituting the moderate level are defined, a strategy of dissuasion could have three primary components. First, a comprehensive approach to dissuasion must *include efforts to address, where feasible, the security concerns of potential aggressors*. During the Cold War, for example, the United States worked to allay Soviet concerns over Berlin and Cuba as part of broader strategies to constrain Soviet behavior: It was as critical to demonstrate to Moscow that aggression or provocations were unnecessary as it was to threaten retaliation. The same has been true in U.S. policy toward Taiwan, which has used reassurances about U.S. opposition to unification to dissuade more-violent Chinese actions.

Dissuading these mid-range gray zone activities over time, therefore, should include efforts to recognize Russian and Chinese security concerns within a framework of global rules and norms. The specific form this might take is beyond the scope of this analysis; it could embody regional territorial settlements, arms control, or mechanisms of mutual restraint (such as the ASEAN Code of Conduct). Such efforts will not resolve all the relevant issues immediately but can help create legitimate avenues for their resolution that would further discredit gray zone coercion.

The second component of a strategy of dissuasion is to *create consistent, sustained global pressure on gray zone aggression*. The more the United States can build a global coalition in support of these efforts, the greater the price gray zone aggressors can be made to pay in diplomatic

and geopolitical terms. The basis for this consensus exists already, our field research suggests, in the rising gray zone threat perceptions of key regional countries. Increasingly, the United States should work with others to make clear that major-power status and prestige is contingent on responsible behavior in this realm. In the process, it can build on existing regional dialogues, such as the U.S.-French dialogue on discouraging Russian political meddling and the U.S.-Japan dialogue on dissuading Chinese aggression. This component of the dissuasion strategy flows directly from the context-setting diplomatic initiative mentioned earlier.

Finally, the third component of the dissuasion strategy is to *gradually increase the costs imposed in response to persistent, serious gray zone aggression*. The United States could convey the message that continued pressure in these areas would generate a rising set of responses. The United States could, for example, threaten to withhold economic and political benefits and thus create multiple points of leverage on targeted activities. Here, economic levers, such as sanctions, should be considered. As demonstrated with sanction regimes against Russia and Iran, for example, targeted sanctions against specific individuals or companies involved in gray zone activities can have significant impact of the targeted country.

The United States could also promise, if such activities continue, to support partners building security capabilities and military forces optimized for gray zone contexts. Examples include helping train and equip Polish Territorial Defense Force and Baltic civilian resistance groups, as well as supporting the development of coast guard capabilities among regional claimants in the SCS.[11] The United States could donate ships for regional coast guard use, as it has begun to do, and identify roles that U.S. forces could perform to ease the burden on local forces.

---

[11] See, for example, David A. Shlapak, "Deterring Russian Aggression in the Baltic States: What It Takes to Win," Santa Monica, Calif.: RAND Corporation, CT-467, March 1, 2017; Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018; and Stephen J. Flanagan, Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin, *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance*, Santa Monica, Calif.: RAND Corporation, RR-2779-OSD, 2019.

At the same time, the United States could demonstrate an ability to impose greater costs over time by demonstrating the capability of its information tools to shape the global narrative on such issues.[12] This would require an enhancement of U.S. public diplomacy and marketing or outreach tools and techniques.

4. Mitigate Persistent Threats by Building Resilience and Competitive Advantage

In the mitigate element of the strategy, we recognize that a considerable proportion of gray zone activity takes place at the lower end of the threat spectrum and is generally viewed as part and parcel of an ongoing geopolitical competition (i.e., the persistent threats in Table 5.1). Nations will not surrender such tools as low-level cyber manipulation, military shows of force, assertion of perceived claims to territory, or cultivation of friendly political actors in other societies. Such ongoing gray zone clashes demand a fourth part of an overarching U.S. response—efforts to make the United States and its allies and partners resilient against such activities and to build tools for competitive success.

The specific requirements of this part of the strategy will unfold over time. We highlight, from our field research, three areas of resilience that could benefit from additional investments and multilateral coordination.

First is a coordinated campaign on disinformation and influence operations, whether in Europe or Asia, with shared strategies to enhance the information resilience of democracies and other partners. The efforts could draw lessons from France's seemingly successful efforts before its 2017 election, which included programs to con-

---

[12] For more on role of media, the global narrative, and its association with national security, see Michael J. McNerney, Ben Connable, S. Rebecca Zimmerman, Natasha Lander, Marek N. Posard, Jasen J. Castillo, Dan Madden, Ilana Blum, Aaron Frank, Benjamin J. Fernandes, In Hyo Seol, Christopher Paul, and Andrew Parasiliti, *National Will to Fight: Why Some States Keep Fighting and Others Don't*, Santa Monica, Calif.: RAND Corporation, RR-2477-A, 2018; and Jennifer Kavanagh and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, Calif.: RAND Corporation, RR-2314-RC, 2018.

fuse attackers, conduct counter-messaging, monitor social media, and work closely with media companies. These programs can also support NGOs involved in combating disinformation.[13] Similar activities could be pursued in Asia to help counteract Chinese narrative-shaping, social media, and influence-seeking operations.[14] They will be stronger, and draw U.S. allies and partners more closely together, if they are coordinated, multilateral efforts.

The second form of resilience is the coordination and alignment of the multiple cyber commands, cells, and initiatives now underway in many U.S. allies and partners. In the process, the United States can offer direct support to cyber defenses in partner states. This recommendation is more relevant in Europe than in Asia, but even in Asia, cyber coordination can be an important tool for deepening partnerships.

The third and final form of resilience emphasized by countries in our field research was cooperation among intelligence and counterintelligence agencies on influence-seeking and disruption activities. For example, the United States and allies could increase participation in the NATO Counterintelligence Centre of Excellence in Poland.

Organizing the Response: Institutional Reforms

A multicomponent strategy like the one outlined in the previous section will be of limited utility if the U.S. government continues to lack a clear coordinating function with the responsibility for overseeing a renewed effort to gain strategic advantage in the gray zone. An important part of any gray zone response strategy, therefore, is undertaking institutional reform.

Although the organization of the U.S. government for gray zone activities was not a central focus of this analysis, we considered several

---

[13] See, for example, CORRECTIV, undated.

[14] A good example of an organization that pursues these tasks is the Asia Maritime Transparency Initiative, which is part of the Center for Strategic and International Studies, based in Washington, D.C.

alternative options and constraints. A major difficulty, given the current organization of key U.S. national security departments and agencies, is that no one home for a gray zone management function is ideal. The National Security Council is not an operational body and has a small staff devoted to coordinating policy rather than running multicomponent campaigns. The State Department has personnel and funding shortfalls and lacks interagency coordination authorities. It also often lacks the institutional mindset needed for aggressive countermeasures. Finally, placing a gray zone coordinating function solely at the Defense Department risks encouraging a dominant focus on military tools, which would not reflect the character of the challenge.

In considering alternatives for a fresh approach, we considered two basic options. One can be described as the *thin option* and would use a presidentially directed strategy, perhaps issued in the form of a National Security Presidential Directive or other White House order, as the foundation of the approach. The order would outline the elements of a gray zone response concept and direct the actions of specific departments and agencies in support. It would then be coordinated by the National Security Council, under a senior director office devoted to the purpose.

Another alternative can be described as the *thick option*. This option would require assembling a more purpose-built office in the U.S. government, with a significant devoted staff, to run counter–gray zone campaigns. It could be headed by a presidential special representative with the highest subcabinet rank and a direct reporting line to the president. We looked at the National Counterterrorism Center for insights into launching a new, focused organization, although that model is designed to promote information-sharing and strategic operational planning more than the operational control of the strategy. This more elaborate option for institutional change could even include the development of regional implementation offices—the equivalent of military combatant commands—to run the gray zone campaigns in those areas (at a minimum, in Europe and Asia).

Whatever option is chosen, the U.S. government can take several accompanying steps to give the gray zone strategy the necessarily profile in national security planning. These steps include the following:

- Make the issue a special focus in Department of State and Department of Defense regional offices, ensuring the necessary staff support to track evolving gray zone activities on their own terms.
- Require that responses to gray zone activities be included as a prominent theme in relevant embassy country strategies.
- Require military service initiatives to emphasize gray zone issues in, for example, career development; training and education; and the funding and support for technologies, capabilities, and experimental force design and concepts tailored to the gray zone.

CHAPTER SIX

A Menu of Options for Responding to Gray Zone Threats

As a final component of the study, we considered a range of specific options that the United States might employ in response to Russian or Chinese gray zone actions. To arrive at the options proposed here, we initially derived options from the literature review and general research at the outset of the project, debated and sharpened the list in brainstorming sessions with other RAND subject-matter experts, and then refined the list based on the detailed discussions that took place during our field research in Asia and Europe. These options could be used as part of the deterrent, dissuasive, and mitigation aspects of the strategy laid out in the previous chapter. The list would accumulate over time as the United States and its allies and partners gain more experience with the gray zone challenge and develop more concepts for responding.

In this study, we did not attempt to build a scripted playbook that specified responses to every plausible Russian or Chinese action. The reality of gray zone competition is too fluid for that, and specific contexts will demand different responses to the same action. In this chapter, we aim to begin assembling a menu of response options from which U.S. officials can choose in such situations.

Each of the sections in this chapter offers a brief contextual discussion and then provides the response options in a table. We evaluate each option in three ways: its potential advantages and benefits, its potential risks and costs, and other considerations derived from our research. In no case do we make a final evaluation of the advisability of any given option in a particular situation; that will depend on the specific circumstances when each response takes place.

In our analysis, we considered a range of distinct categories of responses: local and proportionate, local and disproportionate, and distant from the local dispute and potentially asymmetric. A response option set for any given gray zone activity could include elements from each of these categories.

The option of nonlocal, asymmetric responses—expanding the gray zone competition by hitting back in unrelated issues and places—seems attractive in theory. It ought to provide additional leverage by confronting Moscow and Beijing with the potential for additional diplomatic or economic costs. In practice, though, our analysis suggests that efforts to expand the competition can easily become counterproductive and are warranted only when local responses are regarded as ineffective. This is not to suggest that no such activities can be part of a gray zone response; indeed, they might be especially appropriate when they are designed to focus informational and diplomatic efforts on the gray zone issue and thus impose nonmilitary costs. But efforts to impose direct harm must be treated with great caution because second-front operations can lead down a slippery slope and potentially to armed conflict.

These criteria offer guidance in selecting and combining the response options described in this chapter. To be clear, the numbering of options does not indicate prioritization, an order of preference, or a sequence. We employ it simply for ease of reference.

Military Response Options

The first category of response options offers and examines ways in which the United States and its allies and partners can respond to gray zone aggression using the military tools of statecraft (Table 6.1). Military tools would be relevant across the range of gray zone threats but would be especially important in the deterrent component of the strategy. As suggested in Table 6.1, however, most of the military capabilities appropriate to the strategy do not involve combined-arms formations employed to conduct major warfare.

These options point to several roles that military capabilities can play in the overall gray zone strategy. They include fulfilling the baseline regional deterrence missions, keeping major aggression off the table, and offering the primary muscle behind deterrent threats in the strategy. Military forces would be primarily responsible for train, advise, and human capital development missions. As is the case today, military offices would lead in sustaining security assistance relationships with key countries, working to equip partners with desired capabilities. Finally, military assets would lead in sharing intelligence among militaries for a common operational picture, partly through the role of intelligence, surveillance, and reconnaissance (ISR) systems and other monitoring assets.

Table 6.1
Military Response Options

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
1. Undertake direct military confrontation with hostile forces when they take direct aggressive, kinetic action. Examples: U.S. Navy and Air Force response to an invasion of the Senkaku Islands; U.S. Navy and Air Force support for Philippine maritime assets under attack; U.S. special operations assets deployed to the Baltic states or Poland to confront Russian infiltration efforts	• Most direct and effective way to respond to the most-extreme, aggressive gray zone activities • Only way to guarantee that Russia or China will not gain influence incrementally • Essential to enforce true red lines • U.S. role required because local partners lack the ability to win these fights on their own • Conveys broader signal of U.S. determination and reinforces deterrence of other such aggressions • Sends a strong signal of U.S. commitment to allies, partners, and treaty obligations, and other countries will take note of that commitment	• Risk of escalation if U.S. forces exchange fire with Russian or Chinese forces or if the gray zone aggressor does not back down • Can be muted or exacerbated if one or both sides use paramilitary assets • Danger of leading to a "death by a thousand cuts" if the aggressors force a constant series of responses	• Allies and partners may constrain such options if they are reluctant to engage in a direct confrontation, and the U.S. will seldom be able to act if the allies and partners back away • In some cases, this option may be mandated by treaty • Will be appropriate for only the most-provocative and most-threatening actions against the U.S. and its allies

Table 6.1—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
2. Station specific, permanent new military capabilities in key locations. Examples: Anti-ship missile units in Japan and the Philippines; joint bases in Okinawa; enhanced Air Force capabilities in the Pacific, especially Japan; ISR assets in Southeast Asia; anti-tank and suppression of enemy air defense capabilities in Eastern Europe	• Demonstrates U.S. commitment to regional deterrence • Demonstrates commitment to allies • Enhances local capabilities for responding rapidly to more-aggressive gray zone actions	• Risk of escalatory military action • Opportunity cost: Any permanent deployment imposes an ongoing tax on U.S. global force posture • Increases U.S. links to situations with a higher certainty of being drawn into conflict	• Challenge is identifying the sweet spot of boosted capabilities that pose little provocation risk • Few allies and partners may be interested in such direct presence
3. Deploy modest forces—military, law enforcement (coast guard), civilian—on a rotational or temporary basis to signal U.S. commitment. Examples: U.S. Navy escort of Philippine oil-exploration or drilling in the Philippines' legally recognized EEZ; U.S. Stryker brigade combat team movements in Eastern Europe; added U.S. Coast Guard or U.S. Navy transits in the ECS and SCS (joint passing exercises with Japan in the ECS); U.S. Coast Guard joint fisheries patrols with partner nations in the SCS; Pacific Pathways–style force deployments	• Demonstrates U.S. commitment without the risks and costs of permanent deployments • Creates opportunities for joint, combined training and military-to-military relationship-building • Demonstrates commitment to the rule of law (for example, helping the Philippines assert maritime rights under the UNCLOS)	• Opportunity cost: Financial costs and impact to readiness by pulling units from training and imposing wear and tear on equipment • U.S. power vacuum may be exacerbated once its presence ends • May create escalatory risk if undertaken during a crisis	• U.S. may want to expand paramilitary options in its tool bag; right now, rivals have a significant advantage in this space, forcing an escalatory decision to respond with traditional military forces

Table 6.1—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
4. Develop tailored military units for gray zone contingencies. Examples: United Kingdom's 77th Brigade; a move to devote two or three of the planned U.S. Security Force Assistance Brigade units to gray zone contingencies; creation of specialized civil affairs and special operations units for context; expanded U.S. Coast Guard or Coast Guard–like assets; navy vessels reflagged as Coast Guard	• Enhances the quality and effectiveness of responses to gray zone tactics • Signals commitment to respond • Many types of units would create opportunities for working closely with partners	• Direct cost of units, training, equipment • Opportunity cost: Personnel and resources devoted to gray zone–specialized units would be less available for other contingencies	
5. Conduct specific, discrete military or paramilitary transit or movement operations to signal intent. Examples: Enhanced Coast Guard, Navy, or Air Force Pacific presence operations or freedom of navigation operations in disputed areas of the SCS	• Reaffirms U.S. commitment to international legal standards governing freedom of movement • Benefits from an international legal foundation	• Some escalatory potential if Russia or China responds aggressively • Direct costs if not part of normal operations	• U.S. does not want to exceed regional partners' degree or frequency of such activities

Table 6.1—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
6. Conduct operations to relieve or replace local partners to free assets for responding to gray zone provocations. Examples: ISR assets supporting Japan in the ECS; replacements for the Baltic states' contributions to peacekeeping operations	• Enhances local response without direct U.S. involvement • Underwrites U.S. support for relationships	• Opportunity cost: U.S. forces would be drawn from other missions • Even indirect involvement would be seen by Russia or China as provocative in some cases	• ISR support to Japan was the leading example from our field research
7. Announce new exercises, training missions, and port visits to targeted countries and others in the region. Examples: Added train-and-advise missions with Eastern European countries; maritime exercises in Southeast Asia; formation of a joint maritime task force in Asia; U.S.-Japan response exercises focused on island defenses	• Reinforces partnerships and, in the case of exercises, allows the U.S. and partners to rehearse responses • Demonstrates U.S. commitment without the permanent presence of forces	• Direct and opportunity costs of exercises can detract from readiness for combined arms combat missions • Can provide opportunities for Russia and China to engage in propaganda against the U.S. role and presence	• Must be scoped to the partner's comfort level; in some cases, exercises may be relatively modest

Table 6.1—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
8. Enhance or signal preparedness to conduct operations. Examples: Funding of an improved logistical base, infrastructure (e.g., recent NATO efforts), a basing system, and headquarters capabilities as a signal of readiness to conduct operations across the threat spectrum; improved scenario development and timely coordination mechanisms	• Enhances the ability to conduct military operations • Improves the ability to respond quickly in gray zone situations • Possibly enhances allied and partner ties • Enhances the credibility of U.S. commitments	• In some cases, significant direct financial costs • Potential for some tension with allies and partners if they view the efforts as excessive	
9. Develop added scenarios and contingencies that focus on gray zone situations as part of the Defense Department planning process. Examples: Identification of leading scenarios in which Russia or China would make gray zone advances (e.g., China in the Second Thomas Shoal or Senkakus; Russia in the Balkans or Poland)	• Focuses Defense Department and interagency attention on formalized gray zone scenario development • Helps generate requirements for capabilities relevant to the gray zone	• Opportunity cost of senior leader and bureaucratic time devoted to gray zone scenarios versus other scenarios	• Could be outsourced to federally funded research and development centers

Table 6.1—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
10. Supply or sell new military or paramilitary capabilities to targeted countries. Examples: Transfer of aging maritime assets to Asian nations for coast guard use; sale of advanced ISR to Eastern European and Asian nations, artillery and armored vehicles to Poland, coastal defense cruise missiles and data link architecture to Vietnam	• Signals U.S. commitment to help countries respond • Enhances the deterrent capabilities of partners • Enhances partners' ability to conduct specific gray zone response actions	• Potential to provoke Russia or China, depending on the character, amount of equipment, and country to which the capabilities are transferred • Provides a possible target for Russian or Chinese propaganda	• Multiple U.S. arms export restrictions affect the degree and character of this option
11. Undertake new human capital development initiatives with affected countries. Examples: International Military Education and Training funding for professional military education students; professional military education courses from U.S. institutions offered in affected countries; funding for student fellowships in national security areas	• Low cost • Low chance of provoking rivals • Builds long-term relationships with affected countries • Enhances the capabilities of partners	• Little immediate effect on gray zone operations; is more symbolic and long term	• There can be practical limits, such as the availability of military education slots and partner country students with English-language skills

Table 6.1—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
12. Generate regional military responses to the growing threat. Examples: public commitments to combat gray zone aggression through the Quadrilateral Security Dialogue arrangement; EU actions to boost presence in the East; multilateral defense statements and deployments	• Signals U.S. commitment through involvement in arrangements • Encourages multilateral ties in regions • Provides a mechanism for imposing costs • Signals that the U.S. will spur regional balancing in response to every gray zone initiative	• Direct costs if the U.S. participates in or sponsors activities • Responses could spiral out of control, especially if an ally or partner has a greater risk tolerance than the U.S. does	• Dependent on the appetite of regional partners
13. Implement additional regional covert operations to counteract gray zone activities. Examples: Special operations initiatives in Eastern Europe; covert political initiatives in Southeast Asia	• Provides quiet leverage that will be noticed by Russia and China without major public confrontation • Typically inexpensive • Offers the potential for cooperative activities with local partners that may be reticent to show public displays of deterrence	• Potentially significant political risk if exposed • Escalatory risk; could spark unplanned local clashes • Could antagonize allies who feel left out or manipulated	• Will have a limited role in the overall strategy, given public aspects

Table 6.1—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
14. Conduct new regional humanitarian assistance, disaster relief, and military aid missions to signal presence and deepen regional collaboration. Examples: Quick responses to regional humanitarian disasters, such as earthquakes and typhoons	• Shows U.S. presence in the most widely supported light • Little risk of escalatory dynamics • May not detract from readiness if employing units for intended purposes • Offers the opportunity to work in tandem with Russian and Chinese humanitarian assistance and disaster relief efforts	• Little coercive value in the gray zone context	• Can be an integrated component of the overall public diplomacy campaign

Diplomatic Response Options

In many ways, the diplomatic responses to any gray zone provocation will set the context for all other responses. These response options (outlined in Table 6.2) can benefit from both the deterrent- and reassurance-oriented diplomatic initiatives proposed in the context-setting element of this strategy (see Chapter Five), which are designed to shape the environment to be more responsive to gray zone aggression while also promoting confidence-building measures with Russia and China, where feasible.

Table 6.2
Diplomatic Response Options

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
1. Undertake a major diplomatic push in the region to generate a reaction to provocation or aggression. Examples: Efforts to generate EU or NATO condemnations or an ASEAN statement	• Deepens cooperative links among partners in countering gray zone aggression • Less provocative than military moves	• Limited results could illustrate weaknesses and gaps in coalitions • Countries may be reluctant to commit in the abstract	• Will be useful only if specific initiatives gain traction in particular cases; not likely in all cases
2. Solidify and improve the timeliness of bilateral and multilateral mechanisms for quick responses. Examples: Channels of communication; designated intermediaries for responding rapidly	• Addresses one of the key issues in gray zone responses—timeliness • Improves partner and ally coordination and perceived U.S. commitments • Generates enhanced communication in crisis to avoid miscalculation	• Modest direct financial cost • Some small risk that partners or allies could use the mechanism to support aggressive actions	• Especially important in situations where Russia or China might see opportunity for gray zone faits accomplis, grabbing territory before the U.S. and allies can consult on a response (e.g., Baltic states, Senkaku Islands)
3. Conduct outreach in the region to reassure partners of the U.S. intent to support. Examples: Diplomacy aimed at allies; inclusion of explicit statements in diplomatic documents (e.g., summit announcements, defense consultative memoranda)	• Strengthens the basis for gray zone responses • Deepens multilateral engagement	• Statements could be counterproductive in the absence of actions to back them up	• Needs to be coordinated with concrete steps to pair diplomacy with action

Table 6.2—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
4. Conduct protests at global and regional organizations. Examples: Efforts to raise an issue at the United Nations Security Council or General Assembly, within the EU, or at ASEAN or other organizations; efforts with partners to keep an issue on the agendas of institutions	• Plays to Russian and Chinese concern for status and regional standing • Low cost • Little risk of escalation	• Unlikely to have a significant effect • Countries with a more neutralist posture may not support the efforts wholeheartedly	• Important part of an overall diplomatic campaign, but extensive efforts are needed to lay the groundwork for initiatives before they formally begin
5. Undertake civilian human capital development initiatives. Examples: Diplomats brought to the U.S. to take professional military education or Foreign Service Institute courses; local courses offered by contractors; general ministry training	• Low cost • Low chance of provoking rivals • Builds long-term relationships with affected countries • Enhances the capabilities of partners	• Significant expansion would have some cost, which would trade off against other potential investments • In very select cases in which China and Russia are determined to avoid any U.S. influence, could be seen as aggressive	• Little immediate effect on gray zone operations; long-term rather than short-term effects • May be capacity limitations and political constraints on such initiatives with some partners

Table 6.2—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
6. Support and engage with multilateral fusion centers on gray zone matters. Examples: U.S. funding for the European Centre of Excellence for Countering Hybrid Threats; Baltic-related centers of excellence; academic initiatives	• Relatively low cost • Promotes multilateral coordination and empowers local partners • Nonprovocative • Offers opportunities to draw Russia and China into discussions • Can help build communities of interest on specific issues that can energize responses when events occur • Can help share best practices (e.g., Nordic comprehensive security models)	• Some opportunity cost of funding and time spent by U.S. officials	• May not have a direct, measurable effect on gray zone activities in the short term
7. Engage and increase support for regional multilateral crisis avoidance and consultation organizations. Examples: North Pacific Coast Guard Forum; Organization for Security and Co-operation in Europe's Forum for Security Co-operation; NATO-Russia Council	• Promotes multilateral dialogue on issues • Contributes to raising the issue's overall profile • Sustains mechanisms to work directly with Russia and China • Solidifies U.S. regional commitments	• Small opportunity cost of a U.S. role • Some financial cost in some cases • Risk that Russia and China could turn the forums to their advantage	• Would be closely integrated with the general diplomatic and informational initiatives outlined earlier

Table 6.2—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
8. Engage legal organizations, where appropriate. Examples: Combined efforts with international legal institutions and NGOs; formal or informal advisement of allies and partners on international legal precedent and recourse	• Can help generate formal support in the context of international law • Inherently multilateral in character • Low cost • Low risk of escalation	• Unlikely to achieve major coercive value on its own • China and Russia are adept at lawfare responses, so there is a risk that the contest may not benefit the U.S. • Risks highlighting the lack of U.S. commitment to key international legal standards (e.g., U.S. has not ratified the UNCLOS)	• May require the U.S. to compromise on its opposition to some legal frameworks (e.g., International Criminal Court, UNCLOS) • In some cases, allies or partners would not favor this response (e.g., Japan may view the legal route as legitimizing the idea that China has a valid claim to the Senkaku Islands)
9. Renew efforts to revive resource-sharing agreements to reduce tensions even though essential claims are not yet resolved. Examples: 2008 proposal on ECS resource claims; SCS fishing agreements	• If successful, reduces the risk of direct conflict over claims • Deferral of major issues helps the U.S. preserve the status quo • U.S. involvement reinforces its commitment to the region and establishes the U.S. as a catalyst of stability	• Some modest diplomatic opportunity cost • Risk of failure, and if efforts do not work, it could intensify hostilities	

Table 6.2—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
10. Renew diplomatic outreach to Russia and China to reaffirm the desire to resolve issues. Examples: U.S. diplomats' travel to capitals; conversations between heads of state; renewed military-to-military connections	• Could help dampen the escalation risks of more-aggressive responses • Could reduce the pressure for Russia and China to conduct gray zone activities • May help persuade allies that the U.S. is putting forward a good faith effort to prioritize de-escalation with Russia and China	• Russia and China could turn the process into demands for appeasement of regional ambitions • Outreach to the gray zone aggressor may persuade allies that the U.S. is abandoning them	• Tension-reducing measures can be pursued quickly, but broader settlements will require extensive negotiations over the long term • All of these efforts are placed in the shadow of the context-setting reassurance initiatives

Informational Response Options

The context for the long-term gray zone competition is being set by informational initiatives designed to promote a broad narrative about the ongoing strategic competition. Promoting U.S. and allied perspectives on that narrative on a day-to-day basis is part of the context-setting strategic actions proposed earlier. In response to specific gray zone activities, the United States can employ significantly expanded information operations, for a brief time or over a longer period. These operations can include both referencing the specific action and targeting unrelated issues to impose additional costs on the aggressor. Table 6.3 outlines the informational response options.

Table 6.3
Informational Response Options

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
1. Undertake regional and global information campaigns: Publicize aggression, name and shame. Examples: NATO East StratCom Task Force for cooperation in strategic communications; NGO activities (e.g., on maritime transparency)	• Helps build global consensus against gray zone initiatives • Combined with formal statements and resolutions, can build a deterrent force against future actions • Relatively low cost and low risk of escalation • Opportunity to bring NGOs into the joint activities	• Potential that increased transparency of gray zone transgressions may exacerbate the problem if there is no effective U.S. or allied response • Might make the aggressor appear more powerful than it is, serving its interests (e.g., U.S. reaction to Russian election meddling)	
2. Conduct an information campaign in a targeted state to react to gray zone coercion and shape orientation. Examples: Information operations to reduce the appeal of Russian narratives among Russian-speaking populations in Eastern Europe; campaigns in the Philippines and Vietnam to counteract Chinese appeals to local populations	• Counteracts local effects of Russian or Chinese information operations • Builds robustness and reduces vulnerabilities in the targeted country	• If handled by a local partner, the effort may have limitations, but the U.S. role may be provocative and counterproductive; if the effort is conducted by the U.S., the targeted state's population is likely to perceive it as very intrusive, so it could backfire against the U.S. and the local government	• Should be a natural extension of ongoing information operations developed in a general strategy to set context • To avoid backlash, the U.S. could merely offer assistance to efforts undertaken by local partners

Table 6.3—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
3. Anticipate political meddling and blunt the effects with information operations planned in advance. Example: France's actions before its 2017 election (e.g., warning the public and extensively monitoring social media); U.S. intelligence support to allies with warnings	• Increases resilience against political disinformation • Promotes multilateral coordination	• Opportunity cost of the diplomatic effort needed to establish such operations	• Many of these efforts would be unique to each nation, but some multilateral coordination could help • Some partners may be unwilling to participate in extensive planning before an event for fear of provoking Russia or China
4. Accelerate public diplomacy and narrative-shaping initiatives on unrelated issues to impose costs on the aggressor. Examples: Efforts to highlight Chinese human rights abuses in Tibet and Xinjiang and Russian abuses in Chechnya; promotion of the benefits of the rule of law, human rights, and democracy	• Can appear to impose costs beyond the local gray zone dispute • Signals a U.S. ability to broaden the information fight	• Risk of sparking an escalatory cycle of information operations • May anger or alienate countries involved in the unrelated dispute • May play into fears that the U.S. government actively promotes the destabilization of sensitive internal matters in China and Russia	• Unclear how to distinguish these efforts from ongoing public diplomacy efforts • Hard to establish the costs imposed as a clear consequence for gray zone activities

Table 6.3—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
5. Launch a fast-turn, multilateral informational response to capitalize on Russian or Chinese gray zone overreaching. Examples: Germany's response to the fabricated "Lisa case"	• Helps intensify the counterproductive character of some Russian and Chinese gray zone actions • Strengthens U.S. partnerships with affected countries • Nonprovocative • Capitalizes on natural antibodies to gray zone disinformation in targeted societies	• Likely requires standing capabilities, which would involve some cost • Could be seen as intrusive by partners if led or dominated by the U.S.	
6. Enact legal reforms to control the effect of disinformation. Examples: German and EU laws related to social media	• Restricts the effect of the information components of gray zone activities • Relatively low cost	• Differences on such issues exacerbate divisions between the U.S. and its allies • Approach would be fought by defenders of free speech, and U.S. support might backfire at home • Unintended consequences are still unclear	• Too early to assess the effects of the new European laws (e.g., Germany's law went into effect in January 2018)

Table 6.3—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
7. Improve coordination among cyber resilience and response organizations. Examples: NATO cooperation in the WannaCry ransomware attack; links across multiple European and Asian fusion centers; the February 2018 bilateral cyber dialogue between the U.S. and France	• Enhanced resilience • Multilateral links reinforce partnerships	• Some risk of information leaks • Counterintelligence risk	• Enhanced cyber responses are already underway throughout Europe and, to some degree, in Asia; the U.S. could increase its participation and investment in the joint coordination of these enhanced responses

Economic Response Options

Economic response options offer opportunities to impose costs, sometimes highly targeted ones, with less risk of escalation to outright conflict than military responses offer. The economic responses can be more inflexible than other options, however, especially when they include legislatively mandated sanctions (or aid packages) that become difficult to reverse if Russia or China were to cease a given gray zone activity. Moreover, the United States and many allies have relatively little fiscal room for maneuver; thus, the potential for very significant economic packages—as distinct from sanctions and punishments—may be modest. Table 6.4 outlines the economic response options that we identified.

Table 6.4
Economic Response Options

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
1. Impose immediate, formal economic sanctions on the aggressor. Examples: Targeted sanctions; secondary sanctions against firms involved in gray zone activities, such as Chinese engineering firms or fisheries companies involved in the SCS, Russian energy investments in Ukraine, and Russian state-sponsored media or propaganda arms in Eastern Europe	• Smaller escalatory risk than military steps • Imposes persistent costs that go beyond the single moment • Can be targeted to specific companies or even individuals involved in gray zone activities	• Congressionally mandated sanctions can become very difficult to remove and can establish a permanently hostile relationship • More effective when taken collectively, but this requires a heavy diplomatic effort, including potentially lengthy debates with allies • Can prompt economic retaliation in kind, causing an escalatory cycle	• May be difficult to design packages that go beyond the current sanctions against Russia and yet avoid a significant escalatory spiral • Regional states will be extremely reluctant to challenge China with economic measures because of their dependence on China • History suggests that this response will be generally ineffective in reversing actions already taken
2. Offer aid and compensatory economic benefits to targeted countries. Examples: Support to Baltics nations if they absorb Russian economic punishment	• Defensive measure that is not provocative • Signals U.S. commitment • Can counteract some impacts of gray zone aggression	• Significant costs if any meaningful offset is to be achieved • May set an unwanted precedent for U.S. financial support	• U.S. could recruit multilateral support for a pooled fund for this purpose (e.g., a NATO fund)

Table 6.4—Continued

Response Option	Advantages and Benefits	Costs and Risks	Other Considerations
3. Impose informal but clear economic consequences. Examples: Delay or withholding of investments, business relationships, or partnerships for so-called technical reasons	• Less risk of economic escalation than with overt sanctions • Can complement behind-the-scenes diplomacy • Sends signals to the business community of Russia or China about consequences of gray zone provocations	• Still some risk of a spiral of mutual economic sanctions • Significant potential cost to U.S. and allied businesses • Related political cost	• May be difficult to sustain, given costs to businesses
4. Deny the aggressor participation in key economic institutions. Examples: Ejection of countries from the International Monetary Fund, the World Bank, or the Bank for International Settlements	• Imposes a significant and ongoing cost in economic and status terms • Reflects multilateral judgment	• Risk of starting a cascade of collapsing institutions • Pushes gray zone aggressors into creating a more formal alternative institutional architecture	

Illustrative Cases: Using Response Options to Promote U.S. Interests

As noted earlier, we did not seek to create a rigid, determinative playbook of specific responses for specific gray zone provocations. Each case of gray zone activity is likely to be unique, so the correct set of responses to a given action will depend on the circumstances at the time. Nonetheless, to demonstrate how the response-selection process can work and to give a sense of the sorts of response packages that might be enabled by our menu of options, we chose three potential examples of gray zone actions: Chinese swarming attacks in the Senkaku Islands, Chinese operations to reclaim Scarborough Shoal, and accelerated Russian cyber and disinformation attacks seeking to undermine the Polish government. We chose these three scenarios because we assessed that they are relatively plausible over the next ten to 20 years and because each gray zone target is a U.S. ally or member of an alliance network, thereby permitting a larger spectrum of U.S. policy responses. In each of the following sections, we describe the potential scenario and suggest a possible U.S. response, including the objectives of the response and the specific options combined in that package. In each case, we considered responses in three categories: immediate, local responses to deny gains from the gray zone actions; immediate but distant, cost-imposing actions to punish the gray zone aggressor; and long-term responses that use the action to advance the general U.S. gray zone strategy.

These proposed response menus are informed by findings from our field research; general research into gray zone techniques; and the results of two half-day tabletop exercises at RAND's office in Arlington, Virginia, at the end of May and beginning of June 2018.

Chinese Swarming Attacks in the Senkaku Islands

In the first example, we considered a situation in which a Chinese paramilitary fleet composed largely of civilian vessels with a few CCG ships carries out swarming attacks in the Senkaku Islands, in one case putting ashore several hundred supposed Chinese fishermen armed with small weapons. In this scenario, the Chinese government brands the action a "patriotic expression of nationalist sentiment" and, although the government claims that it "did not approve of" citizens taking the law into their own hands, its promised naval response would have taken weeks to organize.

This scenario constitutes one of the most elaborate potential gray zone provocations. Table 6.5 draws from the menu of options outlined in Tables 6.1 through 6.4 to propose a response designed to achieve the broad objectives of the U.S. gray zone strategy. The top part of the table outlines the objectives of this package of responses, and the bottom part shows the immediate, local responses; the immediate but distant, cost-imposing responses; and the long-term responses.

Table 6.5
Response Package for Chinese Paramilitary Aggression Against the Senkaku Islands

U.S. Objectives		
• Repel the attempted Chinese takeover of one or more Senkaku Islands, with Japan in the lead and the U.S. in a support role. • Reaffirm the U.S. security commitment to Japan and strengthen the regional credibility of U.S. promises. • Impose costs to deter future similar Chinese actions. • Use the event to strengthen the U.S. position in the region. • Avoid unnecessary degrees of escalation in confrontation.		
Immediate, Local Responses	**Immediate but Distant, Cost-Imposing Responses**	**Long-Term Responses**
1. Offer direct support for a Japanese response to attack by providing logistics, ISR, and a joint command and advise role. 2. Deploy U.S. Navy and Air Force capabilities over the horizon for signaling; be prepared to intervene alongside Japanese military forces if requested. 3. Reaffirm publicly that the U.S. considers the Senkakus covered by Article V of the U.S.-Japan Mutual Defense Treaty, and protest Chinese use of force. 4. Engage U.S. and regional NGOs to broadcast details of events, including photos and videos.	1. Raise the issue at the United Nations Security Council as an example of violating international laws and norms. 2. Build on the context-setting diplomatic campaign to rally global responses and protests—notably, among Chinese trading partners. 3. Signal the economic price of the aggression (e.g., U.S. joint ventures with Chinese businesses delayed; U.S. foreign direct investment to China on hold). 4. Build on the context-setting informational strategy and energize regional outrage; convince other nations that they could be the next target. 5. Express the legitimacy of Japanese claims of sovereignty over the Senkakus.	1. Announce new permanent U.S. military bases near the Senkakus (assuming Japan supports such a move). 2. Announce a new research and development program with Japan on related military technology. 3. Begin talks on a new set of military exercises in the region. 4. Develop a medium-term regional information operations strategy to deepen reactions. 5. Establish regular diplomatic contacts throughout the region to use the event to deepen U.S. relationships.

Chinese Operations to Reclaim Scarborough Shoal

This scenario—China's attempted reclamation of Scarborough Shoal in the SCS—represents a move with potentially major ramifications for the balance of forces in the SCS. We highlighted this scenario because of its impact on regional peace and stability, especially given China's assurances that it does not seek to change the status quo in the SCS. Chinese reclamation activities have arguably done more harm to stability in the region than any other move in recent years. This is because China has reclaimed more than 3,000 acres of land on its three largest occupied features in the Spratly Islands and built large military facilities, ports, airfields, and support stations to deploy military assets on these artificial islands. In the past few years, China has deployed surface-to-air missiles, land-based cruise missiles, and military transport aircraft on these islands, and it has deployed combat aircraft to its occupied features in the Paracel Islands.

Meanwhile, Scarborough Shoal lies in an isolated northeast quadrant of the disputed Spratly Islands and is thus perhaps even more important to China's objectives. Were China to dredge Scarborough Shoal and build dual-use facilities capable of hosting military operations, it would be a game changer for the region.[1] For starters, it would put at risk Metro Manila and military bases on the western part of mainland Philippines—some of which station U.S. troops—because Scarborough Shoal is far closer than China's three largest reclaimed islands in the Spratlys. But it would also significantly enhance China's ability to patrol an ADIZ if it chose to unveil one in the future. That is why, from Beijing's perspective, Scarborough Shoal is one of the most coveted pieces of territory for China's next artificial island-building campaign.

For this scenario, we envision a situation in which U.S. or allied countries obtain intelligence that China is preparing to reclaim more features in the SCS, and we presume that at least one and probably more claimants have requested assistance from the United States. Table 6.6 outlines the objectives of the response and a possible menu of actions.[2]

---

[1] Zhao Lei, "Island-Maker' Dredger Will Top Asia Rankings," *China Daily*, June 15, 2018.

[2] For a related paper that provides more-detailed analysis of the response package to reclaim Scarborough Shoal, see Lyle J. Morris, *A U.S. Option Playbook for Contingency Planning to Reclaim Scarborough Shoal*, Santa Monica, Calif.: RAND Corporation, PE-335-RC, 2019.

Table 6.6
Response Package for Chinese Operations to Reclaim Scarborough Shoal

U.S. Objectives		
• Prevent China from making any unilateral changes to the status quo in the SCS. • Prevent China from further consolidating control through the construction and militarization of artificial islands in the SCS. • Reaffirm the U.S. security commitment to the Philippines under the Mutual Defense Treaty. • Rally partners in the region behind destabilizing Chinese actions.		
Immediate, Local Responses	**Immediate but Distant, Cost-Imposing Responses**	**Long-Term Responses**
1. Conduct a flyover exercise near the disputed feature. 2. Offer material support, such as logistics and ISR, for regional states in their responses. 3. Engage U.S. and regional NGOs to broadcast details of events, including photos and videos. 4. Direct a U.S. diplomatic protest to China on the basis of international law and norms. 5. Sanction Chinese engineering firms involved in dredging activity. 6. Threaten a blockade of Chinese vessels near the disputed feature.	1. Build on the context-setting diplomatic campaign to rally regional and global responses and protests. 2. Work with regional partners to signal the major economic price of the aggression, including sanctions. 3. Build on the context-setting informational strategy and energize the regional response. 4. Announce new military activities and exercises in the SCS with other claimants, such as Vietnam. 5. Commence a second front of deterrence activities, such as greater U.S. naval presence in the Taiwan Straits. 6. Announce plans for new U.S. arms sales to Taiwan.	1. Announce a new security assistance program for affected countries, including new arms sales. 2. Initiate talks, such as at the Quadrilateral Security Dialogue, on joint exercises with other claimants and nonclaimants in the Asia-Pacific. 3. Initiate talks with regional partners and allies on establishing new U.S. military bases in Southeast Asia. 4. Invoke international law by supporting new cases against Chinese claims with the International Tribunal for the Law of the Sea. 5. Establish regular diplomatic contacts throughout the region to use the event to deepen U.S. relationships and sharpen soft balancing. 6. Propose or offer to fund new International Military Education and Training slots for military and diplomatic students from the affected nations in U.S. professional military education.

Russian Cyber and Disinformation Attacks Seeking to Undermine the Polish Government

The third and final scenario depicts a situation of less intense gray zone aggression—Russian use of information operations to undermine and destabilize the Polish government on an ongoing basis. The objectives of the U.S. response to this scenario differ from those of the responses to more-elaborate gray zone provocations. Here, the objectives are to reduce the impact of the local attack and use it to build long-term resilience and cost imposition to deter future attacks. Table 6.7 outlines the specific objectives and a potential set of responses.

Table 6.7
Response Package for Russian Cyber and Disinformation Attacks Seeking to Undermine the Polish Government

U.S. Objectives		
• Deny the perception of Russia's ability to fundamentally affect government or democratic processes in Eastern Europe. • Avoid unnecessary degrees of escalation in confrontation; avoid direct military engagements if possible. • Reaffirm the U.S. security commitment to NATO and strengthen regional credibility of U.S. promises. • Impose costs to deter future similar Russian actions. • Use the event to strengthen the U.S. position in the region.		
Immediate, Local Responses	**Immediate but Distant, Cost-Imposing Responses**	**Long-Term Responses**
1. Offer direct support, such as intelligence-sharing and forensics of the activities, for the Polish government in dealing with potential costs from the information operations. 2. Publicly announce at a NATO meeting that NATO is considering reinterpreting Article V to cover certain extreme circumstances of cyber aggression against a NATO member. 3. Engage NATO Centres of Excellence and cyber commands in a coordinated effort to assist. 4. Engage U.S. and regional NGOs to broadcast details of events; develop forensics of the attacks, aimed at attribution. 5. Direct a U.S. diplomatic protest to Russia. 6. Temporarily deploy U.S. cyber units or experts to assist the Polish response.	1. Impose sanctions on Russian entities in Poland with EU participation. 2. Build on the context-setting diplomatic campaign to rally regional and global responses and protests. 3. Build on the context-setting informational strategy to shape the narrative of the event. 4. Announce new military partnership activity with Poland (e.g., an exercise with a cyber focus). 5. Perform a modest cyber probe of Russian systems, taking care to impose only minimal damage to keep the response proportionate and avoid escalatory cyber countermoves. 6. Announce a proposal for new deployments of U.S. and NATO troops in other Eastern European countries.	1. Increase exchanges between cyber and forensic cyber specialists within Polish and U.S. government agencies. 2. Begin negotiations on expanded security assistance programs for Poland. 3. Invoke international law and submit the findings of Russian meddling to international legal bodies. 4. Increase funding for educational programs that send students from Poland to study in the United States.

Conclusion

Through this study, we sought to assess the character of the gray zone challenge from China and Russia, describe a potential concept for governing U.S. responses, and lay out a detailed menu of potential response options from which U.S. leaders can choose in dealing with specific competitor actions or emerging events and crises. Beyond those details, this research offers one overarching conclusion: The most urgent requirements today are to view this range of challenges as a coherent and integrated set and develop an overall strategic concept to guide long-term U.S. and partner responses. Specific responses undertaken outside the context of a strategic concept could waste resources and produce counterproductive results. More than developing any specific capability or undertaking any particular action, the United States will be fully positioned for this intense competition below the threshold of war only when it truly organizes itself—its thinking, its whole-of-government coordination, and its regional implementation—for the challenge.

References

"A New Orthodox Church Next to the Eiffel Tower Boosts Russian Soft Power," *The Economist*, December 5, 2016. As of June 4, 2018: https://www.economist.com/blogs/erasmus/2016/12/ecclesiastical-diplomacy

Abrams, Steve, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections*, Vol. 15, No. 1, Winter 2016, pp. 5–31.

Alexander, David, and Pete Sweeney, "U.S., Chinese Warships Narrowly Avoid Collision in the South China Sea," Reuters, December 13, 2013. As of November 3, 2017: http://www.reuters.com/article/us-usa-china-ships/u-s-chinese-warships-narrowly-avoid-collision-in-south-china-sea-idUSBRE9BC0T520131214

Ali, Idrees, and Megha Rajagopalan, "China Demands End to U.S. Surveillance After Aircraft Intercept," Reuters, May 19, 2016.

Allard, Tom, and Bernadette Christina Munthe, "Asserting Sovereignty, Indonesia Renames Part of South China Sea," Reuters, July 14, 2017.

Altman, Daniel, *Red Lines and Faits Accomplis in Interstate Coercion and Crisis*, dissertation, Boston, Mass.: Massachusetts Institute of Technology, 2015.

———, "By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries," *International Studies Quarterly*, Vol. 61, No. 4, December 1, 2017, pp. 881–891.

Amann, Melanie, and Pavel Lokshin, "German Populists Forge Ties with Russia," *Spiegel Online*, April 27, 2016. As of June 5, 2018: http://www.spiegel.de/international/germany/german-populists-forge-deeper-ties-with-russia-a-1089562.html

Applebaum, Anne, "Russia's New Kind of Friends," *Washington Post,* October 16, 2015.

"Asean Nations Fail to Reach Agreement on South China Sea," BBC News, July 13, 2012.

Asia Maritime Transparency Initiative, "Vietnam Builds Up Its Remote Outposts," Center for Strategic and International Studies, August 4, 2017.

Auchard, Eric, and Joseph Menn, "Facebook Cracks Down on 30,000 Fake Accounts in France," Reuters, April 13, 2017.

Australian Government, *2017 Foreign Policy White Paper*, Canberra, 2017. As of June 6, 2018:
https://www.fpwhitepaper.gov.au/

———, National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018, No. 67, Canberra, June 28, 2018.

Australian Government, Department of Foreign Affairs and Trade, "Australia Supports Peaceful Dispute Resolution in the South China Sea," media release, Canberra, July 12, 2016.

"Australia Warships Sent to South China Sea for Military Exercises," *Daily Telegraph*, September 18, 2017.

"Australian Warships 'Challenged' by Chinese Navy in South China Sea," *The Guardian*, April 19, 2018.

Ayrault, Jean-Marc, "Questions au Gouvernement," Paris: Assemblée Nationale, February 15, 2017.

Babiš, Andrej, letter to the editor, *Washington Post*, October 23, 2015.

Baker, Mark, "Drinking Games," *Foreign Policy*, July 29, 2015.

Barno, David, and Nora Bensahel, "Fighting and Winning in the 'Gray Zone,'" *War on the Rocks*, May 18, 2015.

Batashvili, David, "Russia Troop Deployments Menace Georgia," *Civil Daily News Online*, April 4, 2017.

Bayer, Lily, "Czech Police Recommend Charges Against Prime Minister in Fraud Case," *Politico*, April 17, 2019. As of June 4, 2019:
https://www.politico.eu/article/
andrej-babis-czech-police-recommend-charges-against-prime-minister-fraud-case

B.C., "Cyber-Attack in the Czech Republic: Thieves in the Night," *The Economist*, March 13, 2013. As of August 3, 2018:
https://www.economist.com/eastern-approaches/2013/03/13/thieves-in-the-night

Beauchamp-Mustafaga, Nathan, Cristina L. Garafola, Astrid Stuth Cevallos, and Arthur Chan, "China Signals Resolve with Bomber Flights over the South China Sea," *War on the Rocks*, August 2, 2016.

Beauchamp-Mustafaga, Nathan, Derek Grossman, and Logan Ma, "Chinese Bomber Flights Around Taiwan: For What Purpose?" *War on the Rocks*, September 13, 2017.

Bennett, Cory, "Hackers Breach the Warsaw Stock Exchange," *The Hill*, October 24, 2017.

Bensahel, Nora, "Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex," Foreign Policy Research Institute, February 13, 2017.

Beo Da Costa, Agustinus, and Randy Fabi, "Indonesia Air Force Holds Its Largest Military Exercise in South China Sea," Reuters, October 4, 2016.

Berlinger, Joshua, "Mattis Takes Hard Line on China in Singapore Speech," CNN, June 2, 2018.

Bernini, Elena, "Chinese Kidnapping of Vietnamese Fisherman in the South China Sea: A Primary Source Analysis," Asia Maritime Transparency Initiative, Center for Strategic and International Studies, September 14, 2017.

Berry, Lynn, and David Rising, "Putin, Merkel Spar in Russia over Election Meddling," Associated Press, May 2, 2017.

Beuth, Patrick, Marc Brost, Peter Dausend, Steffen Dobbert, and Götz Hamann, "War Without Blood," *Zeit Online*, February 26, 2017. As of June 7, 2018: http://www.zeit.de/digital/internet/2017-02/bundestag-elections-fake-news-manipulation-russia-hacker-cyberwar

Blanchard, Ben, "Amid Sea Disputes, China to Set Up Maritime 'Judicial Center,'" Reuters, March 12, 2016.

Blanchard, Ben, and Manuel Mogato, "China Decries Attempts to 'Read Too Much into' Passport Map Row," Reuters, November 28, 2012.

"Blasts Cut Georgia Gas, Electricity Supplies," CNN, January 22, 2006.

Bodine-Baron, Elizabeth, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian Social Media Influence*, Santa Monica, Calif.: RAND Corporation, RR-2740-RC, 2018. As of February 20, 2019: https://www.rand.org/pubs/research_reports/RR2740.html

Bohlen, Celestine, "Russia Cuts Gas Supply to Estonia in a Protest," *New York Times*, June 26, 1993.

Borger, Julian, Andrew MacDowall, and Shaun Walker, "Serbia Deports Russians Suspected of Plotting Montenegro Coup," *The Guardian*, November 11, 2016.

Borys, Stephanie "China's 'Brazen' and 'Aggressive' Political Interference Outlined in Top-Secret Report," ABC News, May 29, 2018.

Bowers, Ian, "Power Asymmetry and the Role of Deterrence in the South China Sea," *Korean Journal of Defense Analysis*, Vol. 29, No. 4, December 2017, pp. 551–573.

Bradsher, Keith, "Amid Tension, China Blocks Vital Exports to Japan," *New York Times*, September 22, 2010.

Brands, Hal, "Paradoxes of the Gray Zone," Foreign Policy Research Institute, February 5, 2016.

Brands, Hal, and Zack Cooper, "Getting Serious About Strategy in the South China Sea," *Naval War College Review*, Vol. 71, No. 1, Winter 2018, pp. 13–31.

Burgers, Tobias, and Scott N. Romaniuk, "Hybrid Warriors: China's Unmanned, Guerilla-Style Warfare in Asia's Littorals," *The Diplomat*, February 16, 2017.

Burke, Edmund J., and Astrid Stuth Cevallos, *In Line or Out of Order? China's Approach to ADIZ in Theory and Practice*, Santa Monica, Calif.: RAND Corporation, RR-2055-AF, 2017. As of June 04, 2018: https://www.rand.org/pubs/research_reports/RR2055.html

Byrne, Andrew, "Shootout Raises Fear over Russian Ties to Hungary's Far Right," *Financial Times*, November 27, 2016.

Cavas, Christopher P., "China's 'Little Blue Men' Take Navy's Place in Disputes," *Defense News*, November 2, 2015.

CERT Polska, *Security Landscape of the Polish Internet in 2016*, Warsaw, Poland, 2016.

Chaire Castex de Cyberstratégie, "Observatoire de l'Infosphère Russophone," webpage, undated. As of June 5, 2018: http://www.cyberstrategie.org/?q=fr/observatoire-infosphere-russophone

Chamonikolas, Krystof, "Czech Republic Says Russian Hackers Were 'Very Active' There in 2016," *Bloomberg*, October 24, 2017. As of August 3, 2018: https://www.bloomberg.com/news/articles/2017-10-24/russian-fancy-bear-hackers-seen-very-active-in-prague-in-2016

Chandler, Mark, "Czech Election Result: EU Panics as Populist Zeman Wins—and He Welcomes EU Referendum," *Express*, January 27, 2018. As of July 31, 2018: https://www.express.co.uk/news/world/910776/Czech-election-result-latest-poll-2018-Milos-Zeman-Jiri-Drahos-president

Chang, Amy, Ben FitzGerald, and Van Jackson, *Shades of Gray: Technology, Strategic Competition, and Stability in Maritime Asia*, Washington, D.C.: Center for a New American Security, March 2015.

Chebil, Mehdi, "France Takes Steps to Prevent an Election Hack Attack," *France 24*, January 16, 2017.

"China Ships 'Rammed 1,400 Times by Vietnamese Vessels,'" BBC News, June 9, 2014.

"China Slaps New Fees on Mongolian Commodity Exporters Amid Dalai Lama Row," Reuters, November 30, 2016.

"China Travel Warning Hits PH Tourism Industry," *Philippine Inquirer*, September 23, 2014.

"Chinese Officials Admit to MSDF Radar Lock Allegations," *Japan Times*, March 18, 2013.

"Chinese Warships Criticized for Crossing Waters Near Japan Island," Associated Press, October 17, 2012.

Chisinau, T. J., "Why Has Russia Banned Moldovan Wine?" *The Economist*, November 25, 2013.

Chivers, C. J., "Georgia Reopens Old Gas Line to Ease Post-Blast Shortage," *New York Times*, January 24, 2006a.

———, "A Russian 'Wine Blockade' Against Georgia and Moldova," *New York Times*, April 6, 2006b. As of June 1, 2018: http://www.nytimes.com/2006/04/06/world/europe/06russia.html

Clark, Colin, "CJCS Dunford Calls for Strategic Shifts; 'At Peace or at War Is Insufficient,'" *Breaking Defense*, September 21, 2016.

Cochrane, Joe, "China's Coast Guard Rams Fishing Boat to Free It from Indonesian Authorities," *New York Times*, March 21, 2016.

Colcol, Erwin, "Chinese Vessels Spotted Near Pag-asa Island, Alejano Says," *GMA News*, October 3, 2017.

Connell, Michael, and Sarah Vogler, *Russia's Approach to Cyber Warfare*, Arlington, Va.: CNA, Occasional Paper Series, DOP-2016-U-014231-1Rev, March 2017.

Cooke, Kieran, "Georgia's Wine Frozen Out by Russia," BBC News, November 30, 2006.

CORRECTIV, homepage, undated. As of February 4, 2019: https://correctiv.org/en/

"Cyber Security Office to Assist in Presidential Election," *Prague Monitor*, January 5, 2018.

"Cyber Security to Be Newly Taught at Czech Army's University," *Prague Daily Monitor*, March 5, 2018. As of August 3, 2018: http://www.praguemonitor.com/2018/03/05/cyber-security-be-newly-taught-czech-armys-university

Czech Ministry of Defence, *Defense Strategy of the Czech Republic*, Prague, 2017.

"Czech Television Rejects Zeman's Attacks on Media," *Prague Daily Monitor*, March 9, 2018. As of August 3, 2018: http://praguemonitor.com/2018/03/09/czech-television-rejects-zemans-attack-media

"Czech PM Andrej Babis Stripped of Immunity Amid Fraud Charges," BBC News, January 19, 2018.

"Czechs Not Buying Russian Energy Claims," United Press International, July 15, 2008. As of August 3, 2018: https://www.upi.com/Czechs-not-buying-Russian-energy-claims/17071216145462

Daley, Suzanne, and Maïa de la Baume, "French Far Right Gets Helping Hand with Russian Loan," *New York Times*, December 1, 2014.

Damrosch, Lori Fisler, and Bernard H. Oxman, "Agora: The South China Sea," *American Journal of International Law*, Vol. 107, No. 1, January 2013, pp. 95–97.

Daniels, Laura, "How Russia Hacked the French Election," *Politico*, April 23, 2017.

Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007.

Deeks, Ashley, Sabrina McCubbin, and Cody M. Poplin, "Addressing Russian Influence: What Can We Learn from U.S. Cold War Counter-Propaganda Efforts?" Lawfare, October 25, 2017.

Defense Science Board, *Summer Study on Capabilities for Constrained Military Operations*, Washington, D.C.: U.S. Department of Defense, December 2016.

Deutsch, Anthony, and Toby Sterling, "China's Legal Setback Could Spur More South China Sea Claims," Reuters, July 14, 2016.

Devenport, Tara, "Island-Building in the South China Sea: Legality and Limits," *Asian Journal of International Law*, Vol. 8, No. 1, January 2018, pp. 76–90.

Dizon, Nikko, "AFP Uses Couriers to Foil China Spies," *Philippine Inquirer*, April 29, 2014.

Dupuy, Florian, and Pierre-Marie Dupuy, "A Legal Analysis of China's Historic Rights Claim in the South China Sea," *American Journal of International Law*, Vol. 107, No. 1, January 2013, pp. 124–141.

"Duterte Breaks Records with $6.6 Billion Military Budget, Plans to Outspend Most European Countries," *Frontera News*, February 5, 2017.

Dyner, Anna Maria, "The Importance of the Zapad 2017 Exercise," Polish Institute of International Affairs, Bulletin No. 86 (1026), September 21, 2017.

Dyomkin, Denis, "Putin Says Romania, Poland May Now Be in Russia's Cross-Hairs," Reuters, May 27, 2016.

Dziennik Urzedowy Ministra Obrony Narodowej, "W Sprawie Powołania Pełnomocnika Ministra Obrony Narodowej do Spraw Bezpieczeństwa Cyberprzestrzeni," Decyzja Nr 38/MON, February 24, 2012.

Echevarria, Antulio J., "How Should We Think About 'Gray-Zone' Wars?" *Infinity Journal*, Vol. 5, No. 1, Fall 2015, pp. 16–20.

Eckert, Paul, "Dismantled U.S. Spy Plane Flown Out of China," ABC News, July 3, 2001.

Eddy, Melissa, and Mark Scott, "Delete Hate Speech or Pay Up, Germany Tells Social Media Companies," *New York Times*, June 30, 2017.

Editorial Board, "Beware: The Russian Bear Is Getting Bolder," *Washington Post*, December 1, 2016.

Emmott, Robin, and Andrius Sytas, "Russia's Zapad War Games Unnerve the West," Reuters, September 13, 2017.

Erickson, Andrew S., "Understanding China's Third Sea Force: The Maritime Militia," Fairbank Center Blog, Harvard University, September 8, 2017.

Erickson, Andrew S., and Conor M. Kennedy, "Irregular Forces at Sea: Not 'Merely Fishermen'—Shedding Light on China's Maritime Militia," Center for International Maritime Security, November 2, 2015.

———, "Trailblazers in Warfighting: The Maritime Militia of Danzhou," Center for International Maritime Security, February 1, 2016.

EU vs Disinformation, "Europe Threatened by Nuclear Cloud," *Disinformation Review*, March 16, 2017. As of July 31, 2018:
https://euvsdisinfo.eu/europe-threatened-by-nuclear-cloud

European Commission, "Security and Defence: Significant Progress to Enhance Europe's Resilience Against Hybrid Threats—More Work Ahead," press release, Brussels, July 19, 2017.

European Union External Action, "EU Launches Exercise to Test Crisis Management Mechanisms in Response to Cyber and Hybrid Threats," press release, Brussels, September 28, 2017.

European Values, *Policy Shift Overview: How the Czech Republic Became One of the European Leaders in Countering Russian Disinformation*, Prague, October 5, 2017.

Fabius, Laurent, "La Politique Étrangère de la France: Quelle Autonomie pour Quelle Ambition?" speech before the French Senate, October 15, 2015.

Flanagan, Stephen J., Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin, *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance*, Santa Monica, Calif.: RAND Corporation, RR-2779-OSD, 2019. As of March 20, 2019:
https://www.rand.org/pubs/research_reports/RR2779.html

Fonbuena, Carmela, "5 Chinese Ships Spotted Near Pag-asa Sandbars," *Rappler*, August 15, 2017.

———, "PH Not Keen to Buy More Frigates, Opts for Smaller Vessels," *Rappler*, March 26, 2018.

Freier, Nathan P., *Outplayed: Regaining Strategic Initiative in the Gray Zone*, Carlisle, Pa.: U.S. Army War College, Strategic Studies Institute, June 2016.

Friar, Karen, "5 Things to Know About the Billionaire 'Czech Donald Trump' Who Just Won a General Election," *MarketWatch*, October 23, 2017.

Galeotti, Mark, "Russia's Hybrid War as a Byproduct of a Hybrid State," *War on the Rocks*, December 6, 2016.

Gao, Charlie, "This Is How Poland Plans to Fight Russia in a War," *National Interest*, March 8, 2018.

"Georgia, U.S. Criticize New Russian-Abkhaz Military Force," Radio Free Europe/Radio Liberty, November 23, 2016.

German Federal Government, *White Paper on German Security Policy and the Future of the Bundeswehr*, Berlin, July 2016.

Government of the People's Republic of China, Law of the People's Republic of China on the Territorial Sea and the Contiguous Zone, February 25, 1992.

Green, Michael, Kathleen Hicks, Zack Cooper, John Schaus, and Jake Douglas, *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Washington, D.C.: Center for Strategic and International Studies, May 9, 2017.

Grigas, Agnia, *Beyond Crimea: The New Russian Empire*, New Haven, Conn.: Yale University Press, 2016.

Grossman, Derek, "Can Vietnam's Military Stand Up to China in the South China Sea?" *Asia Policy*, Vol. 13, No. 1, January 2018, pp. 113–134.

Gumilang, Prima, "Indonesia Tegaskan Tak Berniat Konfrontasi dengan China" ["Indonesia Clarifies That It Has No Hostile Intents Toward China"], CNN Indonesia, June 23, 2016.

"The Hague Ruling: Singapore Urges Parties to Respect Legal and Diplomatic Processes, Exercise Self-Restraint," *Straits Times*, July 12, 2016.

Halim, Haeril, Anggi M. Lubis, and Stefani Ribka, "RI Confronts China on Fishing," *Jakarta Post*, March 21, 2016.

Hall, Ian, "Is It Time to Push Back Against China's Economic Statecraft?" Australian Institute of International Affairs, February 21, 2018.

Hammes, Thomas X., *The Sling and the Stone: On War in the 21st Century,* St. Paul, Minn.: Zenith Press, February 17, 2006.

Hancocks, Paula, "S. Korea: Chinese Fisherman Kill Coast Guard Member," CNN, December 12, 2011.

Harding, Luke, "WikiLeaks Cables Claim Russia Armed Georgian Separatists," *The Guardian*, December 1, 2016.

———, "'Deny, Distract and Blame': How Russia Fights Propaganda War," *The Guardian*, May 3, 2018.

"Has Russia Called Georgia's Bluff over Stated Desire to Improve Relations?" Radio Free Europe/Radio Liberty, March 16, 2018.

Hayton, Bill, "The Week Donald Trump Lost the South China Sea," *Foreign Policy*, July 31, 2017.

Heath, Timothy, Michael J. Mazarr, and Astrid Stuth Cevallos, *China and the International Order*, Santa Monica, Calif.: RAND Corporation, RR-2423-OSD, 2018. As of January 30, 2019: https://www.rand.org/pubs/research_reports/RR2423.html

Heijmans, Philip, "Europe's New Cold War: Fake News," *U.S. News and World Report*, January 18, 2017. As of July 31, 2018: https://www.usnews.com/news/best-countries/articles/2017-01-18/czech-republic-forms-unit-to-detect-fake-news-sites

Hénin, Nicolas, *La France Russe: Enquête sur les Réseaux de Poutine*, Paris: Fayard, 2016.

Higgins, Andrew, "In Philippines, Banana Growers Feel Effect of South China Sea Dispute," *Washington Post*, June 10, 2012.

———, "In Russia's 'Frozen Zone,' a Creeping Border with Georgia," *New York Times*, October 23, 2016.

Hoffman, Frank, "The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War," in Dakota L. Wood, ed., *2016 Index of U.S. Military Strength*, Washington, D.C.: Heritage Foundation, 2015, pp. 25–36.

Holmes, James R., and Toshi Yoshihara, "Deterring China in the 'Gray Zone': Lessons of the South China Sea for U.S. Alliances," *Orbis*, Vol. 61, No. 3, May 2017, pp. 322–339.

"How China's 'Sharp Power' Is Muting Criticism Abroad," *The Economist*, December 14, 2017.

"How We Debunked Rumours That Macron Has an Offshore Account," *France 24*, May 5, 2017.

"Indonesia Reinforces Its Command over Natuna Waters Through Military Bases," *Jakarta Post*, September 27, 2016.

"Indonesia's Jokowi Holds Cabinet Meeting on Warship in Disputed Sea," *Kyodo News*, June 23, 2016.

International Crisis Group, "Moldova's Uncertain Future," *Europe Report*, No. 175, August 17, 2006.

International Energy Agency, *Energy Policies of IEA Countries: Poland 2016 Review*, Paris, January 25, 2017.

International Security Advisory Board, *Report on Gray Zone Conflict*, Washington, D.C.: U.S. Department of State, January 3, 2017.

Ishinabe, Kei, "Article Urges Reinforcing Coast Guard to Counter China over Disputed Senkaku Islands," *Sankei Web-S*, via Open Source Enterprise, February 24, 2017.

Isobe, Koichi, "The Amphibious Operations Brigade," *Marine Corps Gazette*, Vol. 101, No. 2, February 2017

Jackson, Van, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflicts Before War," *Naval War College Review*, Vol. 70, No. 3, Summer 2017.

Jančárik, Peter, Adam Reichardt, Roman Shutov, and Ivana Smoleňová, eds., *Countering Pro-Russian Disinformation: Current Challenges and the Way Forward*, seminar summary, Prague: Prague Security Studies Institute, May 31, 2016.

Janda, Jakub, "Czech Intelligence Alarmed by Russian 'Threat,'" *EUobserver*, September 2, 2016. As of July 31, 2018:
https://euobserver.com/opinion/134890/

———, "How Czech President Miloš Zeman Became Putin's Man," *Observer*, January 26, 2018. As of July 31, 2018:
http://observer.com/2018/01/
how-czech-president-milos-zeman-became-vladimir-putins-man/

Janda, Jakub, and Veronika Víchová, "The Kremlin's Hostile Influence in the Czech Republic: The State of Play," Warsaw Institute, August 10, 2017. As of August 3, 2018:
https://warsawinstitute.org/kremlins-hostile-influence-czech-republic-state-play

"Japan and U.S. to Formulate Armed Response to China Threat to Senkakus: Sources," *Japan Times*, November 4, 2018.

Japan Coast Guard, "Senkaku Shotō Shūhen Kaiiki ni Okeru Chūgoku Kōsen Oyobi Chūgoku Gyosen no Katsudō Jōkyō ni Tsuite" ["Regarding the Situation of Chinese State-Owned Ships and Chinese Fishing Vessels Occurring in the Ocean Area Around the Senkaku Islands"], undated.

———, "Junshisen to Junshitei no Chigai ha Nan Desu ka" ["What Is the Difference Between Patrol Vessels and Patrol Craft?"], JCG 5th Regional Headquarters, June 7, 2010.

———, *Annual Report 2016*, Tokyo: Ministry of Land, Infrastructure, Transport and Tourism, 2016.

———, "Kaijō Hoan Chō no Sentei" ["JCG Ships"], January 1, 2017a.

———, *Japan Coast Guard*, Tokyo: Ministry of Land, Infrastructure, Transport and Tourism, March 2017b.

———, *Heisei 30 Nendo Kaijō Hoan Chō Kankei Yosan Kettei Gaiyō* [*Summary of the FY2018 Budget Decision Regarding the Japan Coast Guard*], Tokyo, December 2017c.

———, "The Numbers of Chinese Government and Other Vessels That Entered Japan's Contiguous Zone or Intruded into Territorial Sea Surrounding the Senkaku Islands," chart, March 31, 2019.

Japan Joint Staff Office, "Heisei 29 Nendo 3 Shihanki Made no Kinkyū Hasshin Jisshi Jōkyō ni Tsuite" ["Regarding the Status of Implementing Scrambles in the 3rd Quarter of FY2017"], press release, January 19, 2018a.

———, "Chūgoku Ki no Higashi Shinakai Oyobi Taiheiyō ni Okeru Hikō ni Tsuite" ["Regarding the Flight of Chinese Aircraft in the East China Sea and Pacific Ocean"], press release, March 23, 2018b.

Japan Ministry of Defense, "China's Activities Surrounding Japan's Airspace," webpage, undated-a. As of November 3, 2017: http://www.mod.go.jp/e/d_act/ryouku/

———, "Chūgoku Kōkū Senryoku tō no Waga Kuni Shūhen Kūiki ni Okeru Katsudō ni Tsuite" ["Regarding the Activity in the Airspace Surrounding Our Country by Chinese Air Power"], undated-b.

———, *National Defense Program Guidelines for FY 2011 and Beyond*, Tokyo, December 17, 2010.

———, *Medium Term Defense Program (FY2014–FY2018),* Tokyo, December 17, 2013. As of February 1, 2019: http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/Defense_Program.pdf

———, *Defense of Japan 2015*, white paper, Tokyo, 2015.

———, "Bōuei Daijin Rinji Kisha Kaiken Gaiyō" ["Summary of the Minister of Defense's Special Press Conference"], September 7, 2016.

———, "Statistics on Scrambles Through Fiscal Year 2016," press release, April 13, 2017. As of November 3, 2017: http://www.mod.go.jp/js/Press/press2017/press_pdf/p20170413_02.pdf

Japan Ministry of Foreign Affairs, "Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response," webpage, April 5, 2018. As of July 1, 2018: https://www.mofa.go.jp/region/page23e_000021.html

Japan National Security Secretariat, "China's Expanding Activities in East China Sea," undated, provided to the authors January 15, 2018.

Japan Prime Minister's Office, "Heisei 28-nen 8-gatsu Jōjun no Chūgoku Kōsen Oyobi Chūgoku Gyosen no Katsudō Jōkyō ni Tsuite" ["Regarding the Situation of Activity by Chinese Fishing Boats and Chinese State-Owned Ships in Early August 2016"], October 18, 2016.

JCG—*See* Japan Coast Guard.

"JCG Deepens Surveillance Capabilities on Miyakojima," *Yomiuri Shimbun*, via Open Source Enterprise, September 17, 2017.

"JCG to Expand Video Transmission on Senkaku Patrols—Graphic," *Yomiuri Shimbun*, via Open Source Enterprise, March 2, 2017.

"JCG to Introduce Maritime Surveillance System Using Satellites," *Yomiuri Shimbun*, via Open Source Enterprise, September 8, 2017.

"JCG to Train Own Pilots Amid Rising Surveillance Demands," *Yomiuri Shimbun*, via Open Source Enterprise, July 19, 2017.

Johnstone, Chris, "Czech PM and President Reassert EU and NATO Membership Commitment," Radio Praha, February 9, 2018. As of July 31, 2018: http://www.radio.cz/en/section/curraffrs/czech-pm-and-president-reassert-eu-and-nato-membership-commitment

Kavanagh, Jennifer, and Michael D. Rich, *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*, Santa Monica, Calif.: RAND Corporation, RR-2314-RC, 2018. As of February 20, 2019: https://www.rand.org/pubs/research_reports/RR2314.html

Kazianis, Harry, "China's Expanding Cabbage Strategy," *The Diplomat*, October 29, 2013. As of July 31, 2018: https://thediplomat.com/2013/10/chinas-expanding-cabbage-strategy/

Kelly, Lidia, "Poland Signs $4.75 Billion Deal for U.S. Patriot Missile System Facing Russia," Reuters, March 28, 2018.

Kennedy, Conor M., and Andrew S. Erickson, *China's Third Sea Force, the People's Armed Forces Maritime Militia: Tethered to the PLA*, Newport, R.I.: U.S. Naval War College, China Maritime Studies Institute, China Maritime Report No. 1, March 2017.

Kim Kyung-rok, "THAAD Deployment Causes South Korea's Biggest Ever Services Deficit with China," *The Hankyoreh*, August 6, 2017. As of November 3, 2017: http://english.hani.co.kr/arti/english_edition/e_national/805682.html

King, Esther, "Russian Hackers Targeting Germany: Intelligence Chief," *Politico*, November 29, 2016.

Kinstler, Linda, "Can Germany Fix Facebook? A New Law Seeks to Protect 'Human Dignity' on the Internet," *The Atlantic*, November 2, 2017.

Kirby, Paul, "Russia's Gas Fight with Ukraine," BBC News, October 31, 2014.

Knight, Ben, "Putin Associate Opens Russia-Friendly Think Tank in Berlin," *Deutsche Welle*, July 1, 2016. As of July 31, 2018: https://www.dw.com/en/putin-associate-opens-russia-friendly-think-tank-in-berlin/a-19372110

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, Calif.: RAND Corporation, RR-1498-A, 2017. As of February 1, 2019: https://www.rand.org/pubs/research_reports/RR1498.html

Korns, Stephen W., and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Vol. 38, No. 4, Winter 2009.

Kotani, Tetsuo, "Bolstering the U.S. Commitment to the Senkaku Islands," *The Diplomat*, May 25, 2017a.

———, "The East China Sea: Chinese Efforts to Establish a 'New Normal' and Prospects for Peaceful Management," *Maritime Issues*, July 8, 2017b.

Kragh, Martin, and Sebastian Åsberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case," *Journal of Strategic Studies*, Vol. 40, No. 6, 2017, pp. 773–816.

Kramer, Andrew E., "More of Kremlin's Opponents Are Ending Up Dead," *New York Times*, August 20, 2006.

———, "Czechs See Oil Flow Fall and Suspect Russian Ire on Missile System," *New York Times*, July 12, 2008.

Ku, Julian, and Chris Mirasola, "Tracking China's Compliance with the South China Sea Arbitral Award: Traditional Fishing Rights Inside the Lagoon at Scarborough Shoal," Lawfare, November 2, 2016.

———, "The South China Sea and China's 'Four Sha' Claim: New Legal Theory, Same Bad Argument," Lawfare, September 25, 2017.

Kucinskas, Audrey, "Fustigés par Macron, RT et Sputnik, des Medias 'Stratégiques' pour la Russie," *Express*, June 9, 2017. As of June 5, 2018: https://www.lexpress.fr/actualite/medias/fustiges-par-macron-rt-et-sputnik-des-medias-strategiques-pour-la-russie_1913402.html

Larrabee, F. Stephen, Stephanie Pezard, Andrew Radin, Nathan Chandler, Keith Crane, and Thomas S. Szayna, *Russia and the West After the Ukrainian Crisis: European Vulnerabilities to Russian Pressures*, Santa Monica, Calif.: RAND Corporation, RR-1305-A, 2017. As of February 1, 2019: https://www.rand.org/pubs/research_reports/RR1305.html

Leloup, Damien, "Législatives: Les Français de l'Étranger Privés de Vote Électronique pour des Raisons de Sécurité," *Le Monde*, March 6, 2017.

Levesque, Greg, "China's Evolving Economic Statecraft," *The Diplomat*, April 12, 2017.

Li Baodong, "Remarks of Rebuke Against Japan's Statement on Diaoyu Dao by Ambassador Li Baodong During the General Debate of the 67th Session of the UN General Assembly," Permanent Mission of the People's Republic of China to the UN, October 16, 2012.

Libicki, Martin C., "It Takes More Than Offensive Capability to Have an Effective Cyberdeterrence Posture," testimony before the House Committee on Armed Services, Washington, D.C., March 1, 2017.

Lies, Elaine, "Japan Protests to China over Submarine off Senkaku Islands," *Asahi Shimbun*, January 13, 2018.

Liff, Adam, "China's Maritime Gray Zone Operations in the East China Sea and Japan's Response," in Andrew S. Erickson and Ryan D. Martinson, eds., *China's Maritime Gray Zone Operations*, Annapolis, Md.: Naval Institute Press, March 2019.

Lomidze, Irakli, "Cyber Attacks Against Georgia," briefing slides, Tbilisi, Georgia: Ministry of Justice of Georgia, Data Exchange Agency, 2011.

Lopatka, Jan, "Czech 'Hybrid Threats' Center Under Fire from Country's Own President," Reuters, January 4, 2017.

Lungu, Karina, "Transnistria: From Entropy to Exodus," European Council on Foreign Relations, September 1, 2016. As of May 31, 2018: http://www.ecfr.eu/article/essay_transnistria_from_entropy_to_exodus

"Macron Annonce un Projet de Loi pour le Contrôle des 'Fausses Informations,'" *France 24*, January 3, 2018.

Malyasov, Dylan, "Japan Deploying Type-3 Missile System in Okinawa Prefecture," *Defense Blog*, August 23, 2016.

Markoff, John, "Before the Gunfire, Cyber Attacks," *New York Times*, August 12, 2008.

Martinson, Ryan D., and Andrew Erickson, "Re-Orienting American Sea Power for the China Challenge," *War on the Rocks*, May 10, 2018.

Matthews, Owen, "The Kremlin's Campaign to Make Friends," *Newsweek*, February 16, 2015. As of July 31, 2018: https://www.newsweek.com/2015/02/27/kremlins-campaign-make-friends-307158.html

Mattis, Peter, "Russian and Chinese Political Interference Activities and Influence Operations," in Richard J. Ellings and Robert Sutter, eds., *Axis of Authoritarians: Implications of China-Russia Cooperation*, Seattle, Wash.: National Bureau of Asian Research, October 2018.

Max Planck Institute, *Independent International Fact-Finding Mission on the Conflict in Georgia: Report*, Vol. I, Heidelberg, Germany, September 2009.

Mazarr, Michael J., *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, Carlisle Barracks, Pa.: U.S. Army War College, Strategic Studies Institute, December 2, 2015.

McAuley, James, "French President Macron Blasts Russian State-Owned Media as 'Propaganda,'" *Washington Post*, May 29, 2017.

McElroy, Damien, "South Ossetian Police Tells Georgians to Take a Russian Passport, or Leave Their Homes," *The Telegraph*, August 30, 2008.

McGuiness, Damien, "Russia Steps into Berlin 'Rape' Storm Claiming German Cover-Up," BBC News, January 27, 2016.

McNerney, Michael J., Ben Connable, S. Rebecca Zimmerman, Natasha Lander, Marek N. Posard, Jasen J. Castillo, Dan Madden, Ilana Blum, Aaron Frank, Benjamin J. Fernandes, In Hyo Seol, Christopher Paul, and Andrew Parasiliti, *National Will to Fight: Why Some States Keep Fighting and Others Don't*, Santa Monica, Calif.: RAND Corporation, RR-2477-A, 2018. As of February 20, 2019: https://www.rand.org/pubs/research_reports/RR2477.html

Mehta, Aaron, "In Russia's Zapad Drill, Poland Sees Confirmation of Its Defense Strategy," *Defense News*, December 6, 2017.

Meick, Ethan, and Nargiza Salidjanova, *China's Response to U.S. Korean Missile Defense System Deployment and Its Implications*, Washington, D.C.: U.S.-China Economic and Security Review Commission, July 26, 2017.

Meister, Stefan, "The 'Lisa Case': Germany as a Target of Russian Disinformation," *NATO Review Magazine*, undated.

Menabde, Girogi, "Russian Military Absorbs 'Army of South Ossetia,'" *Eurasia Daily Monitor*, Vol. 14, No. 38, March 21, 2017. As of August 3, 2018: https://jamestown.org/program/russian-military-absorbs-army-south-ossetia

Meyer-Minnemann, Lorenz, *Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience*, Washington, D.C.: Johns Hopkins School of Advanced International Studies, Center for Transatlantic Relations, undated.

Ministry of Foreign Affairs of Georgia, homepage, undated. As of August 3, 2018: http://www.mfa.gov.ge/Home.aspx?lang=en-US

———, *First Quarterly Report (January–March 2017) of the Ministry of Foreign Affairs of Georgia on the Human Rights Situation in the Occupied Regions of Georgia*, Tbilisi, Georgia, 2016.

Ministry of Foreign Affairs of the People's Republic of China, "Statement of the Ministry of Foreign Affairs of the People's Republic of China," September 10, 2012. As of February 1, 2019: https://www.fmprc.gov.cn/mfa_eng/topics_665678/diaodao_665718/t968188.shtml

———, *Position Paper of the Government of the People's Republic of China on the Matter of Jurisdiction in the South China Sea Arbitration Initiated by the Republic of the Philippines*, Beijing, December 7, 2014. As of February 1, 2019: https://www.fmprc.gov.cn/nanhai/eng/snhwtlcwj_1/t1368895.htm

———, "Foreign Ministry Spokesperson Hua Chunying's Remarks on Indonesian Navy Vessels Harassing and Shooting Chinese Fishing Boats and Fishermen," Beijing, June 19, 2016.

Ministry of National Defense of the People's Republic of China, "Announcement of the Aircraft Identification Rules for the East China Sea Air Defense Identification Zone of the People's Republic of China," *China Daily*, November 23, 2013a.

———, "Statement by the Government of the People's Republic of China on Establishing the East China Sea Air Defense Identification Zone," *China Daily*, November 23, 2013b.

Ministry of National Defence of Poland, *The Concept of Defence of the Republic of Poland*, Warsaw, May 2017.

Mohan, Megha, "Macron Leaks: The Anatomy of a Hack," BBC News, May 9, 2017.

Moore, Malcom, "Mackerel War Between China and South Korea Sees Fisherman Shot Dead," *The Telegraph*, October 10, 2014.

Morris, Lyle J., "Indonesia-China Tensions in the Natuna Sea: Evidence of Naval Efficacy over Coast Guards?" *The Diplomat*, July 5, 2016.

———, "The New 'Normal' in the East China Sea," *The Diplomat*, March 2017a.

———, "The Era of Coast Guards in the Asia Pacific Is upon Us," Asia Maritime Transparency Initiative, Center for Strategic and International Studies, March 8, 2017b.

———, "Blunt Defenders of Sovereignty: The Rise of Coast Guards in East and Southeast Asia," *Naval War College Review*, Vol. 70, No. 2, Spring 2017c, pp. 78–103.

———, *A U.S. Option Playbook for Contingency Planning to Reclaim Scarborough Shoal*, , Santa Monica, Calif.: RAND Corporation, PE-335-RC, 2019. As of June 28, 2019: https://www.rand.org/pubs/perspectives/PE335.html

Morrison, Thea, "Georgia Not to Purchase Gas from Russia in 2018," *Georgia Today*, January 9, 2018. As of August 3, 2018: http://georgiatoday.ge/news/8714/Georgia-Not-To-Purchase-Gas-from-Russia-in-2018

Motet, Laura, "Visites, Financements: Le Front National et la Russie, une Idylle Qui Dure," *Le Monde*, November 18, 2016.

Murray, Craig, and Kimberly Hsu, *China's New Fishing Regulations Seek to Justify and Consolidate Control in the South China Sea*, Washington, D.C.: U.S.-China Economic and Security Review Commission, January 27, 2014.

Murray, Williamson, and Peter R. Mansoor, eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, New York: Cambridge University Press, July 9, 2012.

National Cyber and Information Security Agency, homepage, undated. As of August 3, 2018:
https://www.govcert.cz/

Nauert, Heather, "United States Welcomes Georgia Peace Initiative," Washington, D.C.: U.S. Department of State, Office of the Spokesperson, April 4, 2018.

Nemtsova, Anna, "The Next NATO Ally Russia Is Trying to Disrupt," *Daily Beast*, January 12, 2017. As of July 31, 2018:
https://www.thedailybeast.com/the-next-nato-ally-russia-is-trying-to-disrupt

Newnham, Randall E., "Oil, Carrots, and Sticks: Russia's Energy Resources as a Foreign Policy Tool," *Journal of Eurasian Studies*, Vol. 2, No. 2, July 2011, pp. 134–143.

Nichol, Jim, *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests*, Washington, D.C.: Congressional Research Services, RL34618, March 3, 2009.

Noack, Rick, "Cyberattack on French Presidential Front-Runner Bears Russian 'Fingerprints,' Research Group Says," *Washington Post*, April 25, 2017a.

———, "He Used to Rule Germany. Now, He Oversees Russian Energy Companies and Lashes Out at the U.S." *Washington Post*, August 12, 2017b.

———, "Czech Elections Show How Difficult It Is to Fix the Fake News Problem," *Washington Post*, October 20, 2017c.

Nossiter, Adam, David E. Sanger, and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *New York Times*, May 9, 2017.

Ogawa, Satoshi, "Lessons Learned from Senkaku War Games," *Japan Times*, May 7, 2017.

O'Sullivan, Donie, and Dylan Byers, "Exclusive: Fake Black Activist Accounts Linked to Russian Government," CNN, September 28, 2017. As of May 31, 2018:
http://money.cnn.com/2017/09/28/media/blacktivist-russia-facebook-twitter/index.html

Organisation for Economic Co-operation and Development, "Fossil Fuel Support Country Note: Czech Republic," Paris, April 2019.

Organization for Security and Co-operation in Europe, *Istanbul Document 1999*, Istanbul, January 2000.

Osborn, Andrew, "Moscow Accused of Using Gas Prices to Bully Georgia," *The Independent*, November 3, 2006.

Osborne, Samuel, "Russia Deploys Nuclear-Capable Missiles to Border with Poland and Lithuania" *The Observer*, February 7, 2018.

Panda, Ankit, "East China Sea: Japan Coast Guard Plans Miyako Island Facility Upgrades," *The Diplomat*, September 24, 2017.

Paul, Chris, and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, Santa Monica, Calif.: RAND Corporation, PE-198-OSD, 2016. As of February 1, 2019: https://www.rand.org/pubs/perspectives/PE198.html

PCA—*See* Permanent Court of Arbitration.

Permanent Court of Arbitration, In the Matter of the South China Sea Arbitration Before an Arbitral Tribunal Constituted Under Annex VII to the United Nations Convention of the Law of the Sea Between the Republic of the Philippines and the People's Republic of China, PCA Case No. 2013-19, July 12, 2016.

Pennetier, Marine, "Under Threat, France Grooms Army Hackers for Cyber Warfare," Reuters, April 5, 2017.

People in Need, Czech Republic, homepage, undated. As of August 3, 2018: https://www.clovekvtisni.cz/en

Philipp, Joshua, "Chinese Military Said to Be Massing Near the Vietnam Border (+Photos)," *Epoch Times*, May 18, 2014.

Pierce, William G., Douglas G. Douds, and Michael A. Marra, "Countering Gray Zone Wars: Understanding Coercive Gradualism," *Parameters*, Vol. 45, No. 3, Autumn 2015.

"Poland Plans Paramilitary Force of 35,000 to Counter Russia," BBC News, June 3, 2016.

"Poland Targeted by Spate of Cyberattacks: Defence Minister," Radio Poland, October 18, 2017.

"Polish President Andrzej Duda Calls for Stop to Nord Stream 2 Gas Pipeline," *Deutsche Welle*, October 23, 2018.

Polityuk, Pavel, Oleg Vukmanovic, and Stephen Jewkes, "Ukraine's Power Outage Was a Cyber Attack: Ukrenergo," Reuters, January 18, 2017. As of May 31, 2018: https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA

Polyakova, Alina, Marlène Laruelle, Stefan Meister, and Neil Barnett, *The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom*, 3rd ed., Washington, D.C.: Atlantic Council, November 2016.

Popp, George, and Sarah Canna, *The Characterization and Conditions of the Gray Zone*, Boston, Mass.: NSI Inc., Winter 2016.

Priest, Dana, "Lessons from Europe's Fight Against Russian Disinformation," *New Yorker*, July 24, 2017.

Protasowicki, Igor, Slawomir Czepielewski, Krzysztof Ksiezopolski, and Witold Jurasz, *Bezpieczenstwo Energetyczne RP*, Warsaw, Poland: Narodowe Centrum Studiów Strategicznych, 2016.

Qingqing, Chen, and Huang Ge, "China Begins Summer Fishing Moratorium," *Global Times*, May 1, 2017.

Quénelle, Benjamin, "Le 'Margerie,' Homage Posthume à un 'Ami,'" *Les Echos*, March 31, 2017.

Rácz, András, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, Helsinki: Finnish Institute of International Affairs, Report 43, June 16, 2015.

Radin, Andrew, and Clinton Bruce Reach, *Russian Views of the International Order*, Santa Monica, Calif.: RAND Corporation, RR-1826-OSD, 2017. As of June 6, 2018:
https://www.rand.org/pubs/research_reports/RR1826.html

Radziunas, Jan, "Anaconda 2018 Exercise in Poland Is a Preparation for War," *Modern Diplomacy*, December 13, 2017. As of August 3, 2018:
https://moderndiplomacy.eu/2017/12/13/
anaconda-2018-exercise-in-poland-is-a-preparation-for-war

Rahmat, Ridzwan, "Indonesia Leans Towards Iver Huitfeldt Class for Frigate Acquisition," *Jane's 360*, March 12, 2019. As of June 4, 2019:
https://www.janes.com/article/87175/
indonesia-leans-towards-iver-huitfeldt-class-for-frigate-acquisition

RAND Corporation, "Information Operations," webpage, undated. As of May 31, 2018:
https://www.rand.org/topics/information-operations.html

Ratner, Ely, "Course Correction: How to Stop China's Maritime Advance," *Foreign Policy*, July/August 2017.

"(Reisei, Kizen to Taiō) Senkaku Keibi de Hasegawa Honbuchō Dai-11 Kanku Kaiho" ["'Calm and Resolute Response,' 11th Regional Coast Guard Headquarters Commander Hasegawa About Senkaku Security"], *Yaeyama Nippō*, August 4, 2015.

Remeikis, Amy, "Sam Dastyari Quits as Labor Senator over China Connections," *The Guardian*, December 11, 2017.

Republic of France, *Defence and National Security Strategic Review 2017—Key Points*, Paris, 2017a.

———, *Revue Stratégique de Défense et de Sécurité 2017*, Paris, 2017b.

———, *Revue Stratégique de Cyberdéfense*, Paris: General Secretariat of Defense and National Security, February 12, 2018.

Republic of the Philippines and the United States, *Mutual Defense Treaty Between the Republic of the Philippines and the United States of America*, Washington, D.C., August 30, 1951.

Roberts, Anthea, "China's Strategic Use of Research Funding on International Law," Lawfare, November 8, 2017.

Robinson, Linda, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, and Katya Migacheva, *Modern Political Warfare: Current Practices and Possible Responses*, Santa Monica, Calif.: RAND Corporation, RR-1772-A, 2018. As of February 1, 2019: https://www.rand.org/pubs/research_reports/RR1772.html

Rozhlas, Český, "Czech President Attacks Public Television Broadcaster, Calls for Debate over Its Future," *Hello Czech Republic*, May 13, 2016. As of August 3, 2018: http://www.czech.cz/en/Kultur/Czech-president-attacks-public-television-broadcas

Rumer, Eugene, "Moldova Between Russia and the West: A Delicate Balance," Carnegie Endowment for International Peace, May 23, 2017.

"Russia 'Was Behind German Parliament Hack,'" BBC News, May 13, 2016.

"Russia Hackers: German Spy Chief Kahl Warns of Election Disruption," BBC News, November 29, 2016.

Ryan, Missy, and Dan Lamothe, "Pentagon: Chinese Naval Ship Seized an Unmanned U.S. Underwater Vehicle in South China Sea," *Washington Post*, December 17, 2016.

Santora, Marc, "Czech Republic Re-Elects Milos Zeman, Populist Leader and Foe of Migrants," *New York Times*, January 27, 2018.

Schadlow, Nadia, "Peace and War: The Space Between," *War on the Rocks*, August 18, 2014.

Schaus, John, Michael Matlaga, Kathleen H. Hicks, Heather A. Conley, and Jeff Rathke, "What Works: Countering Gray Zone Coercion," Center for Strategic and International Studies, CSIS Briefs, July 16, 2018.

Schrader, Matt, "China's Media on the South China Sea Ruling," *The China Story*, September 20, 2016.

Shaban, Hamza, Craig Timberg, and Elizabeth Dwoskin, "Facebook, Google and Twitter Testified on Capitol Hill. Here's What They Said," *Washington Post*, October 31, 2017.

Shalal, Andrea, "Germany Challenges Russia over Alleged Cyberattacks," Reuters, May 4, 2017.

Shlapak, David A., "Deterring Russian Aggression in the Baltic States: What It Takes to Win," Santa Monica, Calif.: RAND Corporation, CT-467, March 1, 2017. As of February 20, 2019:
https://www.rand.org/pubs/testimonies/CT467.html

Shugart, Thomas, "China's Artificial Islands in the South China Sea Are Bigger (and a Bigger Deal) Than You Think," *War on the Rocks*, September 21, 2016.

Siders, Michele, "Response to Georgian Deputy Foreign Minister David Dondua," Vienna: U.S. Mission to the Organization for Security and Cooperation in Europe, April 12, 2018.

Sim, Royston, "Hong Kong to Return 9 SAF Terrex Vehicles to Singapore: Ministry of Foreign Affairs," *Straits Times*, January 24, 2017.

Sixth Regional Headquarters Ship Technology Division, "Kaijō Hoan Chō Sentei no Bunrui" ["Classification of Japan Coast Guard Ships"], December 2017.

Smoleňová, Ivana, *The Pro-Russian Disinformation Campaign in the Czech Republic and Slovakia*, Prague: Prague Security Studies Institute, June 2015.

Smoleňová, Ivana, Barbora Chrzová, Iveta Várenyiová, Dušan Fischer, Dániel Bartha, András Deák, András Rácz, and Andrzej Turkowski, *United We Stand, Divided We Fall: The Kremlin's Leverage in the Visegrad Countries*, Prague: Prague Security Studies Institute, November 2017.

Sobczak, Pawel, and Lidia Kelly, "Attacks on U.S.-linked Polish Sites Back Higher Cyber Spending: Minister," Reuters, March 15, 2017.

Solovyov, Dmitry, "Russia Deploys Missiles to Protect Georgia Rebels," Reuters, August 11, 2010.

Solsvik, Terje, "Norway Signs Deal to Help Resume Salmon Exports to China," Reuters, May 23, 2017.

Stelzenmüller, Constanze, "The Impact of Russian Interference on Germany's 2017 Elections," testimony before the U.S. Senate Select Committee on Intelligence, June 28, 2017.

Stent, Angela, *The Limits of Partnership: U.S.-Russian Relations in the Twenty-First Century*, Princeton, N.J.: Princeton University Press, 2014.

Stubbs, Jack, and Alexander Winning, "Russia Approves Detailed Sanctions Against Turkey over Downed Plane," Reuters, December 1, 2015.

Świątkowska, Joanna, Izabela Albrycht, and Dominik Skokowski, *National Cyber Security Organisation: Poland*, Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence, 2017.

Syailendra, Emirza Adi, "A Nonbalancing Act: Explaining Indonesia's Failure to Balance Against the Chinese Threat," *Asian Security*, Vol. 13, No. 3, September 5, 2017a.

———, "China in Indonesia's Foreign Policy: Maintaining a Nonbalancing Posture," Singapore: Nanyang Technology University, RSIS Commentary No. 68, September 14, 2017b.

Szary, Wiktor, and Eric Auchard, "Polish Airline, Hit by Cyber Attack, Says All Carriers Are at Risk," Reuters, June 22, 2015.

Szpala, Marta, "Russia in Serbia—Soft Power and Hard Interests," Warsaw: Center for Eastern Studies, Commentary No. 150, October 27, 2014.

Szymanski, Konrad, "Russia's Gas Pipeline Threatens European Unity," *Financial Times*, October 21, 2016.

Tait, Robert, "Czech Cyber-Attack: Russia Suspected of Hacking Diplomats' Emails," *The Guardian*, January 31, 2017.

Takahashi, Kosuke, "JASDF Forms New AEW Squadron in Okinawa," *Jane's Defence Weekly*, April 14, 2014.

Tarar, Ahmer, "A Strategic Logic of the Military Fait Accompli," *International Studies Quarterly*, Vol. 60, No. 4, December 2016, pp. 742–752.

Taylor, Adam, "An Alleged Rape Sparked Tensions Between Russia and Germany. Now Police Say It Was Fabricated," *Washington Post*, January 29, 2016.

"There Are Plans and No Cheap Gas: How Poland Is Trying to Become a Gas Hub," *EurAsia Daily*, November 22, 2017. As of August 3, 2018: https://eadaily.com/en/news/2017/11/22/there-are-plans-and-no-cheap-gas-how-poland-is-trying-to-become-a-gas-hub

TOL Education, "Become an Expert Fact Checker and Hoax Buster!" course description, 2018. As of August 3, 2018: http://toleducation.org/courses/become-an-expert-fact-checker-and-hoax-buster-2/

Toucas, Boris, "Peut-on 'Hacker' Unde Démocratie? Election Présidentielle Américaine et Cyberpuissance Russe," French Ministry of Foreign Affairs, Center for Analysis, Forecasting, and Strategy, January 4, 2017.

Untersinger, Martin, "Cyberattaques: La France Menace de 'Mesures de Rétorsion' Tout Etat Qui Interférerait dans l'Élection," *Le Monde*, February 15, 2017.

Uras, Alessandro, "The South China Sea and the Building of a National Maritime Culture," *Asian Survey*, Vol. 57, No. 6, December 2017, pp. 1008–1031.

"U.S. Condemns Russian Military Deal with Georgian Breakaway Region," Radio Free Europe/Radio Liberty, January 26, 2018.

U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018.

U.S. Holocaust Memorial Museum, "Protocols of the Elders of Zion," Holocaust Encyclopedia, undated. As of November 14, 2017: https://encyclopedia.ushmm.org/content/en/article/protocols-of-the-elders-of-zion

"U.S. Navy: Chinese Warships Maneuvered in 'Unprofessional' Manner," CBS News, May 30, 2018.

U.S. Senate Committee on Foreign Relations, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, Washington, D.C.: U.S. Government Printing Office, January 10, 2018.

U.S. Special Operations Command, *The Gray Zone*, white paper, September 9, 2015.

Vaissié, Cécile, *Les Réseaux du Kremlin en France*, Paris: Les Petits Matins, March 2016.

Van Creveld, Martin, *The Transformation of War: The Most Radical Reinterpretation of Armed Conflict Since Clausewitz*, New York: Free Press, March 31, 1991.

Verseck, Keno, "Is the Czech Republic Moving Closer to China and Russia?" *Deutsche Welle*, January 31, 2018. As of July 31, 2018: https://www.dw.com/en/is-the-czech-republic-moving-closer-to-china-and-russia/a-42392040

Victor, Daniel, "Why You Shouldn't Trust 'Polls' Conducted Online," *New York Times*, September 28, 2016.

Viray, Lourdes Patricia, "Chinese Applying New Tactic in Pag-asa Sandbars, Says Alejano," *Philstar News*, October 4, 2017.

Visegrad Group, "About the Visegrad Group," webpage, undated. As of February 4, 2019: http://www.visegradgroup.eu/about/about-the-visegrad-group

"Voeux à la Presse: Macron Annonce une Loi Contre les 'Fake News,'" Radio France Internationale, January 4, 2018.

Wang Wen and Chen Xiaochen, "Who Supports China in the South China Sea and Why," *The Diplomat*, July 27, 2016.

"Warsaw's Łazienkowski Bridge up in Flames," Radio Poland, February 14, 2015.

Weinbaum, Cortney, "Covert Influence Is the New Money Laundering," *TechCrunch*, November 5, 2017.

White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017.

Whitlock, Craig, "Pentagon: China Tried to Block U.S. Military Jet in Dangerous Mid-Air Intercept," *Washington Post*, August 22, 2014.

"With Israeli Missiles, Philippine Navy Takes Step Toward Modernization," *Times of Israel*, May 11, 2018.

Wuthnow, Joel, "Did China Use Water as a Weapon During Doklam Standoff?" *War on the Rocks*, October 4, 2017.

Yung, Christopher, and Patrick McNulty, *China's Tailored Coercion and Its Rivals' Actions and Responses: What the Numbers Tell Us*, Washington, D.C.: Center for a New American Security, January 2015.

Zhao Lei, "Island-Maker' Dredger Will Top Asia Rankings," *China Daily*, June 15, 2018.

Zhou, Laura, "Chinese Island-Building Firm Wins Contract with South China Sea Rival Claimant, the Philippines," *South China Morning Post*, October 27, 2017.

Zhu, Charlie, "China Tests Troubled Waters with $1 Billion Rig for South China Sea," Reuters, June 20, 2012.

The United States is entering a period of intensifying strategic competition with several rivals, most notably Russia and China. U.S. officials expect this competition to be played out primarily below the threshold of armed conflict, in what is sometimes termed the gray zone between peace and war. In this report, the authors examine how the United States might respond to Russian and Chinese efforts to seek strategic advantage through coercive actions in the gray zone, including military, diplomatic, informational, and economic tactics. The United States is ill prepared and poorly organized to compete in this space, yet the authors' findings suggest that the United States can begin to treat the ongoing gray zone competition as an opportunity more than a risk. Moreover, leaders in Europe and Asia view Russian and Chinese gray zone aggression as a meaningful threat and are receptive to U.S. assistance in mitigating it. In this report, the authors use insights from their extensive field research in affected countries, as well as general research into the literature on the gray zone phenomenon, to sketch out the elements of a strategic response to the gray zone challenge and develop a menu of response options for U.S. officials to consider.

NATIONAL DEFENSE RESEARCH INSTITUTE

www.rand.org

$34.00

ISBN-10 1-9774-0309-3
ISBN-13 978-1-9774-0309-4

53400

9 781977 403094

RR-2942-OSD