The United States and its allies increasingly face challenges from state actors seeking to erode and undermine a system that has expanded peace and prosperity for 70 years. These efforts, variously described as hybrid warfare, irregular warfare, asymmetric warfare, or political warfare (and in this brief, gray zone challenges) are “attempts to achieve one’s security objectives without resort to direct and sizeable use of force.” Drawing on a range of existing research, CSIS convened a half-day conference to identify lessons from previous Western experience with gray zone challenges that can help guide the United States, its allies, and its partners in their current efforts. The result of the conference led the study team to three lessons:

THE ISSUE

- Identify competitors’ gray zone tactics quickly, respond boldly, and think ahead to the adversary’s “next move” and corresponding Western strategies.
- Consider responses across the full range of tools, within and beyond the government. Relying on the military tool is too slow and often creates unnecessary crisis points.
- Operate in concert with allies and partners to amplify effectiveness, bolster deterrence, and increase resilience of one’s

WHAT IS THE GRAY ZONE AND WHAT IS THE THREAT WITHIN IT?

In May 2018, CSIS convened a half-day conference to broaden public dialogue on the growing challenge to U.S. interests stemming from gray zone actors, defined as powers engaging in “attempts to achieve one’s security objectives without resort to direct and sizable use of force.”

CSIS convened two groups of experts to discuss examples from recent history of what has worked, what has not, and steps that the United States and other liberal democracies could take to better respond to future gray zone actions by competitor states. The discussion built on a large existing body of work, including The Kremlin Playbook, Countering Coercion in Maritime Asia, Recalibrating U.S. Strategy Toward Russia, Deterring Iran after the Nuclear Deal, and Meeting the China Challenge.

In addition to yielding specific prescriptions for how the United States and its allies should respond to current and future gray zone challenges, four key issues emerged. First, the discussion highlighted the need to identify gray zone actions quickly and respond boldly to minimize their effects. Second, gray zone responses will be strongest when they create an aligned and unified response from like-minded countries. Third, panelists highlighted the importance of standing by Western norms and the rule of law when confronting gray zone challengers. Speakers
warned that the strategic messaging value of operating inconsistently with our principles would be self-defeating. Finally, the panelists emphasized the importance of operating in concert with allies and partners to amplify the effectiveness, bolster the deterrence, and increase the resilience of one’s own country when confronting current and future gray zone challenges.

The panelists discussed these overarching themes, while providing insights into the adversaries’ approaches, the West’s successful counters, and assessments of where (and how) to do better. The remainder of this brief summarizes that discussion.

WHAT TOOLS ARE COMPETITORS USING?

The main tools employed by malign actors operating in the gray zone include:

- **Military, paramilitary, or other state-controlled forces.** This tool is exercised most regularly by Russia and China, and less often by Iran, and includes forces directly responsible to the coercing state’s government.

- **Proxy forces.** Iran’s efforts to exert political influence through militarized intimidation or through control of territory are notable. Russia’s “little green men” and China’s “little blue men” offer other examples.

- **Information warfare.** Russia, and China in lesser ways, has regularly used information warfare techniques to sow doubt, dissent, and disinformation in foreign countries through social media and other outlets in addition to traditional efforts to bolster their own narrative through propaganda. Iran has also used information warfare to, for example, build a narrative that the United States created ISIS.

- **Corruption of politicians:** Evidence suggests China and Russia have active efforts under way to directly influence political candidates or sitting politicians in a number of countries. Iran’s financial support of Hamas is also a source of potential corruption in that political process.

- **Economic tools.** Examples of economic instruments being used to achieve political or other ends include Russia’s targeted withholding of energy supplies to nearby countries at critical moments, and China’s investment in infrastructure projects in third world countries that have no apparent economic return.

- **Shaping civil society.** China has utilized its Confucius Institutes and economic leverage in universities to limit anti-Chinese sentiment and grow support. Russia has invested substantially in the funding of sympathetic nongovernmental organizations such as the Russkii Mir or Russian World Foundation and through extensive use of the Russian Orthodox Church.

TECHNIQUES TO COMPETE SUCCESSFULLY

Conference speakers highlighted factors important to countering gray zone competitors.

- **Transparency.** Panelists noted that drawing attention to coercion as it happens is an effective way to increase the cost of initiating, and reduce the likelihood of repeating, coercive tactics. Examples of effective transparency have included the publication of the Mandiant Report on China’s cyber activities; the U.S. indictment of PLA officers for cybercrimes; the social-media investigations exposing regular Russian forces deployed in Ukraine without uniforms; exposing the use of fictitious or illicitly hacked materials as the Macron campaign did when such tactics were employed against them; and, exposing and investigating state-directed corruption with links to malign political influence.

- **Deterrence.** Successful deterrence of gray zone actions has often involved senior-level officials threatening
specific consequences for taking specifically identified actions. For example, France and Germany are credited as having made explicit statements to Russia about the actions they would take should there be Russian interference in their respective countries’ general elections. These deterrent actions appear to have worked. Similar efforts aimed at preventing armed aggression as well as less direct challenges are likely to be important for successfully competing in the future.

- **Preparation and preemption.** Preparing one’s public for the potential challenges it could face, and encouraging it to proactively prepare, is important. An informed public that is aware of the tactics of malign influence reduces the potential impact of such efforts, as was the case during the French presidential election. Lithuania has taken concrete steps to ensure a resilient society, including by publishing “How to Act in Extreme Situations or Instances of War,” a manual of how to survive and continue to fight back in the event of an invasion. Sweden has revisited its Total Defense concept, which places strong emphasis on civilian defense. Both countries have returned to conscription. Few other countries have made similar efforts to prepare their publics for the types of challenges that must be navigated, whether invasion, disinformation, economic coercion, or other gray zone tactics.

- **Integrated action.** Panelists Hanna Smith, director of strategic planning and responses at the European Centre of Excellence for Countering Hybrid Threats, and Linda Robinson, senior policy researcher at RAND, noted that Finland and Estonia have sought to develop whole-of-society approaches that include creating integrated decisionmaking processes during crises (e.g., close coordination between the Ministries of Interior and Defense and the creation of the Estonian Defense League), and continual efforts to strengthen national identity. In addition to domestic-focused activities, Michael Tatham, deputy ambassador of the United Kingdom to the United States, argued that unity of action with allies and partners is essential. He described that within NATO, Article V represents the commitment by all members to consider an armed attack against one as an attack against all. The coordination between NATO and the EU to enhance military mobilization also encourages unity of effort. Consistent signaling of this type can also deter or limit the effects of gray zone competition.

- **Early, bold, action.** Malign actors choose gray zone tactics specifically to limit their own risk while exploring permissive boundaries. Response actions that exceed the initiator’s expectations will likely be effective in reversing or diminishing the perceived value of a gray zone tactic. According to Kelly Magsamen, vice president for national security at the Center for American Progress, the Obama administration employed this approach successfully when then-President Obama conveyed directly to President Xi Jinping of China the United States’ opposition to potential PRC island-building activities at Scarborough Shoal and combined it with a strong show of U.S. military force. Michael Tatham noted the collective response to Russia’s poisoning of Sergei Skripal, resulting in the expulsion of over 100 Russian diplomats from more than 20 countries. He said the response to Russia’s poisoning likely exceeded what Russia had anticipated, which deterred it from engaging in a similar action in the future.

- **Clear, specific, consistent messaging.** Kelly Magsamen also noted the importance of “clear, specific, consistent” messaging. The U.S. president and other senior cabinet
members regularly stated the United States position that the U.S.-Japan mutual defense treaty applies to the Senkaku Islands and that attempts to change the status of the islands by force would trigger U.S. military support for Japan. This is believed to be a strong contributor to China’s relatively moderate approach to the Senkaku Islands compared to the South China Sea.

WHEN HAVE WE COME UP SHORT?
Despite remaining the world’s largest economy, leading diplomatic power, and most effective military, the United States has underperformed in gray zone competitions. Panelists described several episodes where the United States or other Western countries have come up short and recommended ways to address some of those shortcomings.

SHORTCOMING 1: DISINFORMATION
The United States failed to deter or respond rapidly to Russia’s disinformation campaign throughout the 2016 U.S. presidential election. Jamie Fly, senior fellow and director of the Future of Geopolitics and Asia Programs at the German Marshall Fund of the United States and Linda Robinson noted that Russian disinformation is focused on driving wedges in American society, especially by drawing on contentious domestic issues to exacerbate social rifts. The ubiquity of social media in the United States makes disinformation a low-cost option to sow, or expand, division. Further maximizing the divisive potential of disinformation, Russia has targeted all sides in political debates.

RESPONSE 1:
To address disinformation, panelists offered three specific approaches. Hanna Smith noted the benefits of countering disinformation with positive, truthful narratives. She indicated this is often more effective than trying to “debunk” false stories, which can unintentionally further promulgate disinformation. Daniel Kimmage, acting coordinator of the Global Engagement Center at the U.S. Department of State, highlighted the importance of groups across the spectrum of government, civil society, academia, and allied governments working collaboratively to displace disinformation with accurate information. Michael Tatham offered the example of the United Kingdom’s experience countering disinformation with a regulatory system that allows the public to request reviews of media platforms’ content for accessibility, deliberately misleading content, or harmfulness.

SHORTCOMING 2: RAPID PLANNING AND RESPONSE
Since 2007, countries have seen numerous cases of gray zone action, including Russia’s invasion of Georgia and annexation of Crimea, cyber-attacks against Baltic states, China’s island building in the South China Sea, and Iran’s expanded support for proxy forces throughout the Middle East. Despite these indicators, Western countries have largely failed to engage in planning efforts to identify when or how they should respond to similar tactics in the future. Even in countries that have some of the most well-developed plans and response mechanisms, the plans are often triggered by an invasion or other clear crisis. For example, Finland and Estonia’s plans, as described by Hanna Smith, are largely responses to invasion, whether from uniformed military or others. When competitive strategies are deliberately crafted to avoid crossing such crisis-triggers, even prepared states may find it difficult to identify a point at which a broader or more robust response is necessary.

RESPONSE 2:
Finland and Estonia have already completed the most important step: preparation. They have developed a plan for what to do when faced with an adversary actively seeking
to attack them. Other countries should be examining recent gray zone tactics and developing ways to counter similar such actions in the future. Michael Singh, Lane-Swig senior fellow and managing director at the Washington Institute for Near East Policy, suggested that current gray zone competition requires actors to also start “looking ahead to the next threat” to understand what tools are needed now and what tools will be needed as threats evolve.

**SHORTCOMING 3: INSUFFICIENT USE OF CURRENTLY AVAILABLE TOOLS**

Although experts debate the degree to which the West has adequately flexed its military muscle to deter and respond to gray zone challenges, there is a general consensus that the United States has under-utilized and under-invested in a range of potentially powerful non-military tools both within and beyond government. Linda Robinson pointed out that non-military tools can often be deployed earlier than military forces in a slowly escalating situation, saying that “by the time the military is involved, the game is almost over.” Kelly Magsamen noted that nongovernmental actors can play a useful role in gray zone response. She cited the degree of environmental destruction caused by China’s artificial island building campaign as an issue that could galvanize helpful pressure from Western environmental organizations. In a related example, individuals and nongovernmental organizations were on the front lines of identifying Russian forces invading Ukraine. These private actors matched the social media accounts of the invading forces with known Russian military personnel—apparently with minimal engagement from Western governments. These efforts helped to belie Russia’s claim that the forces were Ukrainian rather than Russian.

**RESPONSE 3:**

There are ways to expand the tools used by the United States and like-minded countries to counter gray zone coercion. One approach that was repeatedly referenced is to more deliberately leverage the potential for transparency to shape public and leader opinions, and ultimately to deter or change undesirable approaches. For example, public knowledge of China’s investments in countries as part of its “One Belt, One Road” initiative, and how those terms may impact the receiving country would be a good near-term step, according to Kelly Magsamen. Another approach that Michael Tatham offered can expand the skill set within the government is represented by efforts in the United Kingdom to leverage flexible hiring authorities for its reserve forces to deliberately seek out diverse skills and bring them into the governmental process. This authority allows the United Kingdom to more rapidly incorporate specialized skills and perspectives from the private sector that may not otherwise be available in the government.

**QUESTIONS FOR FURTHER EXPLORATION**

The panel discussions surfaced several questions that will merit additional consideration by the United States, its allies, and its partners to respond effectively to future gray zone challenges from authoritarian states and nonstate actors. One key question is whether gray zone activity is warfare or something else. While such a discussion may seem semantic, how the challenge is framed will likely influence how publics and governments consider responding to it and which actors are given the resources and responsibility to counter future gray zone threats. Managing escalation dynamics will be critical.

Second, how can the United States, its allies, and partners integrate the tools available—and those that may yet be developed—to better deter gray zone competition in the first place? A campaign planning approach (such as those used by the U.S. military) may be a helpful construct for framing the key challenge and dynamic employment of tools needed.
A related question within the United States is how to develop integrated responses to gray zone challenges in ways consistent with divided statutory authority. For example, the agencies best positioned to understand the nature and scope of the gray zone challenge—the State Department and most of the intelligence community—lack the legal authority to engage in domestic activities that may be needed to counter foreign gray zone efforts. The agencies that have the appropriate legal authority to operate within the United States—such as the Department of Homeland Security (DHS), the FBI, and other law enforcement agencies—currently lack a significant mandate, and attendant resources, to operate effectively to counter gray zone threats at home. Without a dramatic (and tragic) attack against the United States, how far will Congress or the executive branch be willing to alter current structures to respond to the growing gray zone challenge?

Finally, how can the United States bolster civil society, private-sector engagement, and citizen education to identify and address some aspects of gray zone competition? The federated nature of the American political system, and its tradition of limited government, can be both an aid and a hindrance for fostering civic engagement initiatives.

CONCLUSION

U.S. leadership in an era of gray zone competition will require more than the largest economy or strongest military. National security begins at home and the United States must reinvigorate confidence in its institutions, its leaders, and its policy approaches. The United States can choose to strengthen and reinforce alliance structures, multilateral institutions, and democratic processes that have bolstered American economic prosperity and enhanced its security for 70 years or it can choose to degrade them. To compete more successfully, the United States must rapidly identify gray zone challenges and develop unified policy responses with allies and partners. These goals are achievable but will require the United States to restructure and reinvigorate its interagency structures, better prepare its citizens for gray zone competition, and ensure a whole-of-society approach. Maintaining an ongoing and comprehensive dialogue with allies and partners related to gray zone adaptation and best practices would also be extremely beneficial. Without these steps, the United States, its allies, and partners will likely continue to repeat avoidable mistakes and allow competitors to erode the integrity of Western financial, political, and security institutions. The result would be diminished American and allied power and sovereignty.

John Schaus is a fellow in the International Security Program at the Center for Strategic and International Studies (CSIS), where he focuses on defense industry and Asia security challenges. Michael Matlaga is a research assistant with the International Security Program at CSIS, where he focuses on NATO and European defense policy. Kathleen H. Hicks is senior vice president, Henry A. Kissinger Chair, and director of the International Security Program at CSIS. Heather A. Conley is senior vice president for Europe, Eurasia, and the Arctic and director of the Europe Program at CSIS. Jeffrey Rathke is a senior fellow and deputy director of the Europe Program at CSIS.

2. Ibid.

