SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 6: Testing U.S. Policy Responses to Destructive Cyberattacks with Wargames

Emily Harding Julia Dickson Aosheng Pusztaszeri

A Report of the CSIS Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 6: Testing U.S. Policy Responses to Destructive Cyberattacks with Wargames

AUTHORS
Emily Harding
Julia Dickson
Aosheng Pusztaszeri

A Report of the CSIS Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values–nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

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

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

Acknowledgments

The authors would like to extend their gratitude to those who agreed to participate in the wargame. The authors would also like to thank Dr. Benjamin Jensen, Jose Macias, Yasir Atalan, and Divya Ramjee from the CSIS Futures Lab for helping design and analyze the games, Rex Booth and George Corbari for graciously providing feedback, Susan Hines for assisting with the project contract, and the CSIS iDeas Lab for offering their design expertise.

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

Contents

Authors' Note About the Series

This report is part of a series on the future of cyber warfare. This part of the series examines a set of wargames designed to test U.S. policymakers' responses to three large, deadly cyberattacks on the U.S. homeland, including how they approach attribution, domestic defense and recovery efforts, proportionality of a U.S. response, and if these attacks constitute an act of war.

Part 1 of this series offers a broad introduction to the report, covers key takeaways from the comparative studies and wargames, and summarizes the authors' recommendations. Parts 2, 3, and 4 examine how Russia, China, and Iran, respectively, fight in the cyber domain, and Part 5 examines U.S. cyber practices. This part, Part 6, tests how U.S. policymakers view cyber operations as part of the spectrum of war, peace, and irregular warfare, illuminated by a set of wargames. Finally, Part 7 fully explains the new playbook that will close the gap between how the United States and its adversaries fight and succeed in the cyber domain.

The Wargames

CSIS developed three wargames to test how U.S. policymakers would respond to a large, deadly cyberattack on the U.S. homeland. In the past, U.S. responses have treated most cyberattacks as natural disasters or criminal acts, but researchers for this project wanted to understand whether associated deaths would prompt policymakers to pursue stronger, even kinetic, response options. Further, researchers anticipated that policymakers would struggle to assimilate a massive cyberattack into their existing mental constructs for national security, in particular how to define a “proportional” response and how to conceive of deterrence.

To evaluate these questions, researchers brought together senior experts from the U.S. government, industry, academia, and the think tank community, assigning each participant a position as a cabinet-level leader in a mock Principals Committee meeting, such as the secretary of state or the secretary of defense. The participants then received a scenario in which a U.S. adversary (Russia, China, or Iran) hit the U.S. homeland with a massive cyberattack.

Each scenario was different and had a cyberattack with a unique level of destruction, a different international context, and a different level of certainty in attribution (for full scenarios, see Appendix 1):

- **Low death count, very low-confidence attribution, near-peer competitor:** In the Russia scenario, Moscow renewed its offensive against Ukraine after a two-year ceasefire. At the same time, there was a massive cyberattack on the U.S. electrical grid, leaving millions without heat in the middle of winter, among other complications. A few deaths were indirectly tied to the blackout. Further, rumors spread on social media that “big oil” caused the blackout; other threads claimed “green activists” hacked the grid as a protest. Private cybersecurity firms publicly pointed to Russia, but the U.S. Intelligence Community (IC) could not yet make an assessment.

- **Medium death count, low-confidence attribution, near-peer competitor:** In the China scenario, Beijing ordered a quarantine of Taiwan, then disrupted U.S. military communications. As the United States attempted to mobilize to help Taiwan, a cyberattack on a water plant in Chicago poisoned thousands of people and led to deaths. Attribution had low confidence, but the IC assessed that China intended to distract the United States from its likely impending invasion of Taiwan.
- **High death count, high-confidence attribution, not a near-peer competitor:** In the Iran scenario, renewed regional fighting was the context for a cyberattack on the Hoover Dam, which resulted in a full breach and thousands of deaths. The IC declared with high confidence that Iran’s Islamic Revolutionary Guard Corps (IRGC) was the perpetrator.

At the end of each game, researchers asked participants, “Are we at war?” The answers were mixed and illuminated how policymakers grapple with this relatively new form of warfare.

This was a limited set of games, and the scenarios were complex. The CSIS research team would like to run more games to gather better data, isolating each of the variables (death count, attribution, and the competitor’s capability) to test how each affects policy responses. Researchers anticipate that a high casualty count will be necessary for participants to choose a strong military response, but also that the threat of quick escalation with a near-peer competitor will temper that action more than it would against a competitor seen as less capable, such as Iran.

Overarching Themes for All Three Wargames

Faced with simultaneous domestic and foreign crises, participants grappled with the complex scenarios and debated how to parse and prioritize. They agreed that domestic recovery must be the priority, although in the China scenario in particular, the participants were eager to pass that responsibility off to domestic agencies.

Participants disagreed on whether a sharp foreign retaliation was necessary to reassure the U.S. public. One participant summed it up as follows: "I think [our responses] need to be visual though. You do anything cyber? Covert? Nobody's gonna know about it. A physical visual–that's how the American people are."[1]

Defining forceful action was also difficult, as participants struggled to define a proportional response. One participant, thinking out loud, illustrated this problem perfectly: "I do think that it is important that we develop a vehicle, or some means that is a direct response to this, is proportional, but yet causes real pain to the Kremlin, and essentially responds in order to deescalate."

Uniformly, the overarching goal of the participants in each exercise was to walk a narrow path: help people at home and retaliate enough to deter the aggressor from further action, but precisely calibrate the response to avoid full-scale war. The severe complicating factor was attribution–in the China and Russia scenarios, participants were held back from quick retribution by a lack of

[1] The war games were recorded, and researchers used an auto-transcription service. As a result, some of the conversation was muddled. When reporting quotations in this piece, researchers quote where possible and paraphrase where necessary to accommodate for the imperfect recording and keep the text readable.

certainty about who perpetrated the attack. One participant aptly noted: “We want to impose costs but not escalate, and we are not sure who to impose costs against.” As another participant highlighted, “The dilemma is that we need to stall for time . . . [while] looking for attribution. So, we need to sort of hurry up and wait. We need to stall for time, yet take forceful action.”

The next sections of this report will explore in detail several themes–attribution; domestic response and recovery; proportionality and escalation; cyber, economic, and kinetic responses; and deterrence–that emerged across scenarios and that policymakers in real-life crises must address. The report then explores the one question that was at the core of each debate: Are we at war?

Attribution

Uncertainty about the attacker’s identity severely hampered rapid-response options. Greater uncertainty about whether the perpetrator was a government actor led to slower, more tentative responses. This confusion is why actors engage in the cyber domain–to keep opponents off-balance in their reaction.

Attribution was most uncertain in the Russia game. In the scenario, one private security firm assessed with high confidence that the Russian government was responsible, but another disagreed, claiming that it was a hacktivist group. The National Security Agency (NSA) had not yet determined the source of the attack.

Due to the attack’s severity, some participants were willing to publicly call out Russia and begin retaliatory actions without 100 percent confidence that Russia was behind the attack. One participant said, “I don’t think it’s possible to wait before [publicly] attributing it to Russia. . . . We should be willing to jump the gun.” Others, however, preferred to wait to respond until the attribution was definitive: “Attribution is key here. . . . There’s not a lot we can do in counterresponse today.” Participants debated how long they could wait for definite attribution before they needed to act. They expressed concern that waiting too long would send the wrong signal and fail to deter Moscow from taking further action. However, without 100 percent confidence that the Kremlin was responsible, participants highlighted that it might be difficult to get international buy-in for a high-order response: “How do we go to our allies with this and justify retaliating with force?”

In the China scenario, attribution also came up, but the associated move against Taiwan and U.S. military mobilization seemed to tamp down questions over who was responsible. One participant said: “I want to hear more from our intelligence community. The attack may or may not be of Chinese origin. I think it’s critical that we acknowledge what we don’t know and preserve decision space and not overreact until we are certain what we’re dealing with. . . . I think it’s premature to respond.”

Confusion over attribution also led to extensive discussions about how to strategically communicate the attack. In the Russia and China scenarios, policymakers debated what to say about who was responsible and how they would be held accountable. They were also uniformly frustrated that they did not have better information to share. Participants expressed the need to communicate stability and strength.

Does Intent Matter?

Somewhat unexpectedly, participants did not ask questions about the intent of the attacker. When the game runners asked about intent, the majority of participants in all three scenarios agreed that intent did not matter, particularly in response to the high-casualty Iran scenario. One participant in that scenario said, “We have to deal with results, so I care less about their intent. I care about changing their risk calculus.”

The following exchange in the China game showed that participants were willing to hold the adversary accountable when it should have known what the results would be:

> Director of the NSA: Again, we’re not quite sure. Maybe they just wanted to get a whole bunch of people really sick, right? So, was there an intent to murder U.S. citizens? I’m not sure we’re at war.
>
> Chief of Staff: They know that when you inject lye and sodium hydroxide into drinking water, people are going to die. So, there was an intent, a knowledge. I think we can impute a sort of an awareness that this was going to happen with fatal consequences. So, I view that as an act of war, especially taken in conjunction with what’s happening in Taiwan.

Domestic Defense and Recovery

In each scenario, a foreign actor hit U.S. critical infrastructure with a devastating cyberattack to distract the United States from a hostile act against a neighbor. If the casualty count was low, that tactic worked somewhat, as participants spent at least some time grappling with the domestic picture and not responding to the foreign crisis. Furthermore, they were concerned about recovery and messaging at home in ways they would not have been had the cyberattack not occurred. In the China game, for instance, one participant recommended that the United States focus on “resiliency and restoration” to prevent future attacks on critical infrastructure: “Let’s amplify messaging and get threat intelligence out through the Sector Risk Management Agencies down to the field.” Still, the response to the apparent impending Taiwan invasion dominated the game. In the transcript, “Chicago” appears 11 times, while “Taiwan” appears 50 times.

In the Russia scenario, several participants raised the political costs of the event, including the fallout from a lack of retribution, the wrong retribution, or scrutiny over weaknesses in domestic defense. One participant expressed concern that if the damage had resulted from a known or long-standing vulnerability, the blame would fall squarely on the administration. Another pointed out just how difficult it would be to explain the following course of action to the public:

> So, the idea you guys want to sell to the American people, some of whom are freezing cold and in the hospital with no acute response, is that we're going to now reengage in Ukraine, which is already incredibly unpopular, and we're going to patch their systems? And by the way, we're going to have CIA [Central Intelligence Agency] and the NSA come in to nongovernment infrastructure?

While it is difficult to communicate tone in a transcript, the skepticism and sarcasm were palpable. The main point for these participants was that security lapses in domestic systems were enormous vulnerabilities for both practical and political purposes, and that most "proportional" responses to an attack were likely to be woefully unsatisfactory in the eyes of the American public.

The Iran scenario clearly had massive domestic impact, to the extent that one participant questioned whether military forces were needed for the relief effort. This scenario was also the one to backfire on the adversary–rather than be distracted and focused on the home front, policymakers moved to immediately and aggressively attack.

Proportionality and Escalation

Director of the NSA: So, what qualifies as a tit-for-tat in the cyber realm?

Secretary of Energy: I don't know. We don't have the specifics on what was done to us. So, I would try to do something proportional once we're able to identify what the proportional response is.

—Exchange between two participants in the Russia wargame

The above exchange encapsulates the debates across all three wargames regarding what constitutes a proportional response. Participants discussed whether a cyber response would be "enough," including what level of cyber response would be sufficient to send a strong message to the adversary, and whether a hidden U.S. hand would be satisfactory for the American public. Furthermore, when participants felt the situation merited a stronger response than cyber could provide, there were additional debates about what kinds of responses could dangerously escalate or prompt a full military conflict.

The question of proportionality was particularly thorny when the attack caused deaths only indirectly. This exchange from the Russia wargame illustrates the challenge:

> Secretary of the Treasury: I think what you're gonna sell to the American public before you start World War III is violence, right? That's the difference between this and a real act of war. Like lethality, like loss of life.
>
> Chief of Staff: But there was loss of life.
>
> Secretary of the Treasury: Yeah, indirect whatever but that's why they . . .

> Director of the Central Intelligence Agency: Let me push back on that just a little bit though. There are acts of war that do not cause lethal consequences, like a blockade.
>
> Chief of Staff: Yeah, and also everyone in this room who's a cyber expert has said that responding to cyber with cyber is useless.
>
> Department of Homeland Security: It's just like it's . . . not a proportionality. It's just another end.
>
> U.S. Mission to the United Nations: We're not going to [unintelligible] unless we're in active conflict.

Even though the scenario indicated that the cyberattack had led to deaths, participants were unsure how to interpret those deaths and where they fit into a "normal" estimation of war footing. Researchers assume that if a Russian, Chinese, or Iranian bomb killed a dozen people in downtown Chicago, policymakers would clearly view it as an act of war. However, a cyberattack causing critical infrastructure failure, which then resulted in deaths, altered perceptions of proportionality.

There were also discussions about the adversary's proportionality calculus. A participant in the Russia scenario attempted to gauge Moscow's intent by assessing the potential impact of a U.S. response: "The Russians would do this. Not for the purpose of starting a war. They don't want to start a war. They want an option, an aggressive option, that is short of World War III, and that's exactly why they use this."

In other words, the participant believed Russia was sending a nuanced signal with this cyberattack– that Moscow wanted to distract and harass the United States but did not view the move as a precursor to war. Thus, Moscow would likely see a kinetic U.S. response as a dramatic escalation.

Following that debate, a discussion ensued about whether Russian intent mattered when formulating a response: "Right, but then if we don't respond to it as an act of war, then we're just letting them run the table. . . . [W]e're letting them have that. They win if we allow them to say, 'Oh, well, it's not a real act of war because you didn't bomb somebody. It's not kinetic, so it's not real.'"

Debate over intent and escalation is hardly unique to cyber conflict. However, there is a common lexicon and somewhat understood "rules of the road" in conventional warfare. These rules are still being established in the cyber domain, making it more likely for there to be a mismatch between the message intended and the message received. This can be true on the front end and the back end. In other words, the initial attacker may intend to harass but not provoke. The victim may seek to respond with what it views as a proportional action, signaling a reluctance to escalate, but the attacker might perceive that response as either excessive or insufficient, interpreting it as a push toward full-scale war or a sign of weakness, respectively. This project seeks to address such miscommunications before they occur, especially given the high stakes involved.

Cyber Responses

All three groups discussed responding to their scenario's cyberattack with some version of a cyber response. Proposed options included, on the extreme end:

> We have to be careful in how we address this, but this is not a time for restraint. Every infrastructure target and cyber target that we have in Iran [and] with its proxies, I think we should execute. We should do this in a planned and deliberate way, but we need to cripple them in their digital infrastructure and in their physical infrastructure where we can.

Participants saw a strong cyber response as justified given the high casualty count, and they paired this robust cyber response with kinetic action. In the games with lower casualty counts against near-peer competitors, participants were far more focused on identifying a proportional cyber response that would send a clear message of U.S. preference to avoid escalation.

In the China game, for example, there was an explicit tit-for-tat calculation. The following quotations illustrate that portion of the discussion:

- "We need to hit them hard, in the cyber world, and nothing more. No more, no less."
- "So, we'll fight in the cyber world and will hurt you. And there will be deaths because you've murdered our citizens and we're going to murder yours."
- "Are we actually talking about a response on Chinese critical infrastructure in the Chinese homeland?"

The latter point reflected concerns about escalation—that China might not view an attack on its homeland as proportional or justified and would immediately escalate to direct military conflict. Some participants argued that China had done exactly the same to the United States, while others questioned whether targeting Chinese civilians was something the U.S. government would be willing to do from a moral standpoint.

In the Russia game, participants were generally frustrated, believing that cyber options against Russian infrastructure would be pointless, even if the United States were willing to conduct them:

> A response in kind may not actually affect the Russians in the same way that [it] affects us. Their heating systems and critical infrastructure does not work as reliably as ours and so, therefore, their practices and their sort of resilience factors are better because they have less stable infrastructure than we do. They're used to things being offline.

The Russia game also raised a broader point about the ready availability of cyber responses: these tools are difficult to create and are not "sitting on a shelf" ready to deploy in most cases. The cyber experts in each room, playing roles such as director of the NSA/U.S. Cyber Command (USCYBERCOM) or director of the CIA, had bad news like this to deliver:

> There's not a lot that we can do at this point directly in Russian infrastructure. We are not prepared to execute sort of a counter response today. Those options can be worked, but they will take some time for replacement and execution, probably on the order of weeks.

> I [get] enormous amounts of questions like, "Can't you just have something on the shelf?" I'm like, okay, but the 50 guys that I have doing finished intelligence collection, I will take them off and [they will] be "off-the-shelf" dudes. Is that really what you want? Yeah, the answer was always no.

Other participants were generally frustrated by these answers, as expressed by this participant: "I'm sort of disheartened that we don't we have all these tools. There's all this money going to CYBERCOM and zero [cyber response options are immediately available]."

For many participants, this quotation reflected the crux of the discussion: "Cyber is not an effective response in most situations." All groups agreed that the United States needed to retaliate in the cyber domain *at a minimum*. But they also agreed that those cyber responses were unlikely to satisfy the need for proportional response or create deterrence against future attacks. This calculation was most apparent in the Iran game, which had a very high casualty count. One participant said, "Our response should include cyber actions, but not be limited to them. Iran committed an act of war, and our response should reflect their actions."

Economic Responses

In these games, punitive economic steps were a side note, not a central feature. This likely stems from the estimated consequences of measures like sanctions. Iran and Russia are already subject to quite comprehensive sanctions regimes, and additional sanctions are likely to have little effect. With China, there was talk of using the United States' considerable economic leverage but also a recognition that those sanctions would bite hard inside the United States itself.

In the China wargame transcript, the term "economic" appears 26 times, compared to once in Iran's and eight times in Russia's. Participants expressed sentiments such as "the [Chinese] regime responds to economic pressure" and "I personally think the best way to hold their feet to the fire is economic." However, written responses did not indicate that participants would pursue higher-order economic responses following a Chinese attack compared to a Russian or Iranian one. In the written responses, only one-quarter of the participants mentioned taking any economic action against China. Some participants, for instance, advocated for "sanctions of [China]-connected companies" and for using "international coalitions' economic power," but many responses emphasized other actions aimed at damaging Chinese military capabilities and protecting Taiwan.

Against Russia, participants recognized that economic measures were largely spent, with sanctions for the 2022 Ukraine invasion still in effect. One participant suggested exposing additional Russian government corruption, and another advocated completely cutting Russia off from the international financial system: "If it is Russia, I would make them a pariah. And I would pull them off the global stage. Just pull them off the books, the global stage. So, delist them off SWIFT. Take them out and scramble the internet routing, right? So, they are an island in and of themselves, and to get in and out virtually or physically becomes impossible."

Similarly, participants considered economic measures against Iran to be largely ineffective. They were far more focused on kinetic responses, such as sinking the entire Iranian navy.

When Things Go Kinetic

In the Iranian cyberattack scenario, which caused thousands of U.S. deaths, policymakers immediately advocated for a strong, kinetic response. During the discussion, participants used the word "kinetic" 20 times, compared with only twice in the Russia game and 6 times in the China game. Participants expressed sentiments like "nothing less than a kinetic strike will do" and "working to restore deterrence will necessitate kinetic strikes." Similarly, the written responses tended toward military campaigns and the use of force, with participants suggesting the following:

- new Authorization for the Use of Military Force (AUMF) (replace the 2001 AUMF), targeting all cyber facilities and critical infrastructure, the IRGC, and nuclear facilities
- military strikes on Iran
- retaliatory cyber action coupled with kinetic action against cyber capability
- overt military response

Participants in the Iran game also discussed the possibility of regime change. One recommendation stated that the U.S. response should focus on "regime change, [including] IRGC senior leadership and those around the supreme leader." Conversely, others highlighted that "regime survival is their number one goal," so perhaps sending the message that regime change is not the goal would cause Tehran to "stand down" and limit escalation.

In the China and Russia games, participants did not advocate for similar actions. China and Russia would be near-peer competitors militarily, with hefty nuclear arsenals, so there were several references to trying to avoid World War III. In addition, in the Russia scenario, attribution was unclear at the time of the mock Principals Committee meeting, which considerably dampened enthusiasm for military action. Instead, participants explored low-kinetic options such as targeting the Russian state-funded mercenaries of the Wagner Group in Africa, moving a carrier group into the region, or sending additional troops into Poland. Still, there was pushback:

> I will maintain my opposition to both kind of potentially invoking the threat of war and then moving military assets in the region as being potentially escalatory to the point of miscalculation, and I think one of the objectives we have is to actually avoid actual war with Russia. If we're just signaling with moving military assets into the region, that doesn't quite make sense; I think it's not worth the potential risk.

In the China scenario, Beijing had already begun a quarantine of Taiwan and looked poised for an invasion. Participants mobilized to respond, meaning that military action was already in play. One participant advocated for harassing the Chinese People's Liberation Army Navy (PLAN) ships responsible for maintaining the quarantine, while another said, "We have to assume that kinetic action has begun, and we should begin to flow forces."

In each scenario, someone raised the option of invoking Article 5 of NATO's founding treaty, which states that an attack on one ally is considered an attack on the entire alliance, and that all members will take whatever actions they deem necessary to assist the attacked ally. This led to a debate about whether the cyberattack would qualify. One participant wondered if "the consensus at this meeting is [that] NATO wants to say that any cyberattack against critical infrastructure is considered an act of war?"

Two factors likely account for the variance across games regarding the willingness to use the U.S. military. First, the casualty count played a large role: the high death toll in the Iran game was seen as shocking and requiring a bold response, whereas the death toll was in the "tens" in the China game and a handful in the Russia game. The latter two sets of casualties were also indirect results of the cyberattack, so participants did not feel as much public urgency to retaliate with force. The second factor was the potential for retaliation: the participants were confident that the United States would succeed in extensive military action against Iranian assets, whereas the risk of great power conflict leading to a global war was top of mind in the Russia and China scenarios.

Deterrence

> *U.S. Mission to the United Nations: This has to be the last cyber war. If we fight Cyber War 1, we need to make sure there can't be a Cyber War 2.*
>
> *—Participant in the China wargame*

Participants discussed deterrence extensively, but there was no consensus on how to restore it or whether deterrence is possible in the cyber realm. They debated demonstrations of will meant to deter further actions, such as moving military assets or invoking Article 5. These were intended to show that a severe cyberattack would be met with more than just a cyber response, at least threatening kinetic action. Furthermore, participants indicated a desire for an international framework for cyber warfare: "We're going to come out of this war with treaties and regulations for a post-cyber war world to make sure that we treat electrons no different than any kind of weapon and that this never happens again."

The sentiment in the room reflected skepticism that deterrence was possible, but also a need to try to establish a red line around civilian casualties. In the Russia game, one participant said, "So why don't they do this again in two years? Why don't the Chinese do it [in] three years? [If] we don't set a cost for them executing this, what stops them from doing it in the future?" In the China game, there was a clear sense that previous inaction by the United States had done nothing to establish deterrence: "I would make the argument that we've seen this before, and we did nothing. I think this plays to our weakness where every time we take what we think is a round one punch, it's actually round seven."

The Core Question: Are We at War?

At the end of each game, researchers posed a question: Given the scenario, are we at war?[2] This question aimed to address one of the core propositions for this project—whether policymakers have a clear view on how a cyberattack, even a deadly one, fits into existing national security frameworks.

In the Iran game, 89 percent of participants (all but one) answered that yes, given the massive cyberattack causing thousands of deaths, we were at war with Iran. The China and Russia scenarios were less clear. For China, 82 percent said yes, and 18 percent said no (nine participants and two participants, respectively), but these findings are complicated by elements of the game involving impending conflict over Taiwan. Participants did not seem to think that the Chinese quarantine of Taiwan, the disruption of U.S. military communications, or the cyberattack that poisoned Americans were enough individually to qualify as being "at war." However, the combination of the three tipped the participants to a wartime footing.

The Russia scenario was far more complicated: 60 percent of participants said yes, the United States was at war with Russia, while 40 percent said no (six and four participants, respectively). The "yes" group seemed willing to accept a low-confidence assessment that Russia was responsible for the

[2] The researchers specifically framed this question as "at war" rather than a declaration of war to allow for legal flexibility. Instead of getting participants bogged down in discussions of legal authorities and AUMFs, the question was more along the lines of whether these adversaries had brought war to the United States. It was intended to convey the idea, paraphrased, that "you may not be interested in cyber war, but cyber war is interested in you."

cyberattack on critical infrastructure, particularly in light of its renewed hostility against Ukraine. The "no" group was far more cautious, still questioning the attribution and Russia's intent in conducting the attack. This group was also concerned about rapid escalation to a full-scale conflict between the great powers.

Implications

Confusion and Uncertainty

Having only run three games, the CSIS research team is hesitant to overgeneralize or draw sweeping conclusions without more data. That said, each game—despite differing fact patterns and aggressors—illustrated the likely, disastrous confusion in the event of a major cyberattack on the U.S. homeland. In the midst of a crisis, policymakers should not be grappling with basic questions like whether this counts as an act of war or what level of attribution is sufficient to justify action. Moreover, they need to understand how their allies view these same questions in order to confidently call on NATO, Pacific region partners, and other allies for assistance.

Confusion is common in moments of crisis. Immediately following shocking, unprecedented attacks such as Pearl Harbor or 9/11, policymakers were also in turmoil about how to respond. Yet, those attacks had more clarity than a cyberattack likely would. In both cases, the actor was clear, and the need for an immediate wartime footing was obvious. A kinetic response was a given, not a question. But cyber is different: in each of the games, the person playing the chief of staff grew increasingly frustrated at the lack of good options to present to the president—none seemed to strike the right balance between communicating strength, creating deterrence, and fitting within the amorphous U.S. definition of "proportional." Cyber conflict is still new, and these games demonstrated how important it is for policymakers to assimilate ideas about cyber warfare into their calculations well before one occurs.

Next Steps

Time and resources only allowed for three games, so while the results are informative, they did not enable researchers to isolate key variables. Researchers were able to draw conclusions from the challenges participants highlighted in the discussions, but a follow-up exercise involving 30 to 40 games would allow them to test a range of variables that emerged as important to policymaker decisions:

- casualties or no casualties
- near-peer adversary or a militarily weaker adversary
- clear attribution to a state actor or to a state-affiliated actor versus unclear attribution
- the extent to which cyber experts are involved in the policymaking decision

Casualty Count: In the Iran game, a high casualty count led to immediate kinetic action, but the highest casualty count also occurred against the least capable adversary, which muddies the results. In the two games against near-peer adversaries (Russia and China), the casualty count was lower and participants were far less eager to reach for military tools. The research team would like to disaggregate these two variables with several test games.[3]

[3] Researchers acknowledge the flaws in this game setup. However, they prioritized a realistic story for each actor with this exercise. A future round of games would be more effective at isolating key variables.

Near-Peer Adversary: To test whether participants would be more or less likely to resort to cyber tools rather than kinetic tools in response to an attack, researchers would like to hold the power level of the adversary constant.

Attribution to a State Actor: To test how much clear attribution matters in a response, researchers would hold other variables constant and vary the level of certainty the IC has about the perpetrator of the attack. For example, participants in the Russia game debated how clear the attribution was to Moscow, which influenced the strength of their response against the likely perpetrator. Some participants wanted to leave space for backing down if it became clear that the actor was actually a criminal group.

Cyber Expertise: The siloed approach to foreign policy, where the U.S. government tends to treat cyber as a separate arena from other foreign policy tools, is one of the issues CSIS researchers sought to highlight in this report. Testing the effect of having cyber expertise present—or absent—in the discussion would be a crucial finding for policymakers seeking to respond to a crisis. Cyber experts participated at varying levels in each of the games in this round. Rerunning a scenario with and without cyber experts present would provide an empirical way to test whether the respondents are more or less likely to understand the severity of the attack and respond with cyber or non-cyber tools.

Researchers also propose running this exercise with Five Eyes partners and NATO allies. The Five Eyes—an intelligence alliance comprising the United States, the United Kingdom, Canada, Australia, and New Zealand—will be the first line of alliances in the event of a contingency. NATO allies will need to determine whether to answer an Article 5 call from a victim of a massive cyberattack. While it is official NATO policy that a cyberattack would qualify for an Article 5 response, the threshold for an attack to qualify has not been clearly tested or explained. The game could clearly demarcate those red lines.

About the Authors

Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program and deputy director of the Defense and Security Department at CSIS. As the head of the INT Program, she provides thought leadership on the most critical issues facing intelligence professionals and on the future of intelligence work. She also serves as vice president of the Defense and Security Department, where she is responsible for leading a team of world-renowned scholars providing policy solutions that shape national security. Drawing on her decades of experience in national security, Emily has established herself as an expert on how technology is revolutionizing national security work. Harding has served in a series of high-profile national security positions at critical moments. While serving as deputy staff director on the Senate Select Committee on Intelligence, she led the committee's investigation into Russian interference in the 2016 elections, which was lauded for its bipartisanship. At CIA, she led analysts and analytic programs through moments of crisis, including shepherding the Iraq Group during the attempted Islamic State takeover. During a tour at the National Security Council, she served as director for Iran. After leaving the White House, her team ran the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for briefing the incoming administration. Harding is an adjunct lecturer at the Johns Hopkins School of Advanced International Studies. Her analysis has appeared in the Wall Street Journal, BBC, NPR, Bloomberg, and other outlets. Harding holds a master's degree from Harvard University's Kennedy School of Government and a bachelor's degree from the University of Virginia.

Julia Dickson is a research associate with the Intelligence, National Security, and Technology (INT) Program at CSIS. Her research interests include cybersecurity and cybercrime and the role of technology in conflict. Prior to joining CSIS, she was awarded a Fulbright grant and spent a year teaching English in Osh, Kyrgyzstan. She was also previously a research assistant at the Wilson Center, an intern for the Conventional Defense Program at the Stimson Center, and a communications and outreach intern at the International Crisis Group. She holds a BA in international studies with a minor in French from the Johns Hopkins University.

Aosheng Pusztaszeri is a research assistant with the Intelligence, National Security, and Technology (INT) Program at CSIS, where he focuses on emerging technologies and their implications for national security. Prior to joining CSIS, Aosheng interned in the U.S. Senate and the U.S. House of Representatives and worked as an undergraduate research assistant in Cornell University's Department of Government. He holds a BA in government and history from Cornell University.

Appendix 1

The Scenarios

Russia

Participants received a scenario about a cyberattack in which an attacker–likely, though not certainly, Russia–disrupted the U.S. electric grid, causing blackouts that lasted for days during the winter. Citizens were unable to heat their homes, and hospitals were only able to provide a limited number of services, resulting in a few deaths. The attack coincided with Russia renewing its war in Ukraine, suggesting that Moscow sought to distract the United States. Read the full scenario below.

It is February 24, 2027. The conflict between Ukraine and Russia, which began with Russia's illegal invasion in 2022, ended in 2025 with a ceasefire and a stalemate. Russia continues to control vast portions of Ukrainian territory, including Crimea and parts of Donetsk, Kherson, Luhansk, Mykolaiv, and Zaporizhzhia Oblasts.

On the fifth anniversary of the invasion, protesters in the city of Kherson hold a rally with Ukrainian flags, chanting that the oblast is still Ukrainian and will never be Russian, no matter how long Russia illegally occupies the territory. The Russian military gave little warning before opening fire on the protesters. Thirty Ukrainians were killed, and a graphic video was immediately posted to social media, showing Russian soldiers desecrating the bodies. In response, forces from a local Ukrainian resistance movement killed 20 Russian troops over the next few days, prompting Moscow to deploy additional troops to Kherson, including a notorious spin-off of the Wagner Group. Moscow says its loyal friends in Ukraine will quell the "CIA-sponsored coup."

The U.S. president reaffirms support for Ukrainian sovereignty and calls on Russia to end its illegitimate control of Ukrainian territory. NATO and EU leaders express concern about the risk of renewed fighting between Ukraine and Russia as Russian troops are deployed throughout occupied Ukraine, especially near the current borders. The Ukrainian president orders a remobilization of the Ukrainian Armed Forces, but both he and Moscow know that the army is exhausted and depleted after four years of fighting. Moscow sees its chance for total victory and claims that a Ukrainian "provocation" against sovereign eastern Ukraine justifies a renewal of fighting.

Knowing the United States has pledged to provide support for Ukraine, Russia has plans to distract Washington with cyberattacks. Russian President Vladimir Putin makes a public statement that the "defense" of independent provinces in eastern Ukraine is Russia's right, and any outside interference is unacceptable. Shortly after, GRU operatives–members of Russia's foreign military intelligence agency–trigger the malware TUBE NIGHTMARE to temporarily disrupt industrial control systems, including power grids, factories, water utilities, and oil pipelines.

Russia successfully disrupts electric grids and causes blackouts in major cities across the United States. Power is out for days. Citizens are unable to use heating during the cold February days, and while hospitals are running on backup generators in a limited capacity, services are dramatically curtailed. Ambulance response times increase, hospitals become overcrowded, and many life-saving technologies are unavailable. Electric vehicles are unable to charge, and cell service continues on a limited basis. Rumors are spreading on X, the social media platform formerly known as Twitter, that the U.S. power grid has failed due to administration "green fuel subsidies." On left-leaning X forums, some are calling for violent protests against oil companies. On right-leaning forums, some are calling for violent protests against wind farms.

Policymakers meeting in the Situation Room (SITROOM) have the following facts:

- Russia is poised to renew its offensive against Kyiv, and Western powers are not well-positioned to stop it this time.
- A cyberattack has heavily disrupted life across the United States during the winter. While no one has died directly as a result of the attack, anecdotal reports suggest that the lack of electricity has led to casualties.
- Protests are brewing, and the Department of Homeland Security (DHS) has noticed that some opposing protests are scheduled for the same time and place–a classic Russian information operations tactic.
- DHS is working with private sector cybersecurity firms to uncover the source of the cyberattack. One firm assesses with high confidence that Russian government actors are responsible. Another disagrees and suggests the attack was likely carried out by a hacktivist group, possibly based in Romania. NSA is working its sources, but whoever

engaged in the attack ran it through U.S.-based information and communications technology, complicating NSA's legal authorities.

China

Participants received a scenario about a Chinese cyberattack on the James W. Jardine Water Purification Plant in Chicago, which supplies water to 64 percent of the city's residents. Access to the system allowed Chinese hackers to remotely increase levels of lye, used to control water acidity, poisoning thousands of people in the Chicago area and causing many deaths. The attack was intended to cause domestic strife and distract the United States as China launched a blockade against Taiwan.

The scenario for the China wargame had the most components—a Chinese de facto blockade of Taiwan, potentially as a precursor to a full-scale invasion; disruptions to U.S. military communications; and a cyberattack on a water purification plant in Chicago, assessed with low confidence to have been carried out by a China-based group. Policymakers in this multifaceted situation debated which issue was the most urgent. Read the full scenario below.

It is May 1, 2027. During a speech for International Workers' Day, Chinese President Xi Jinping announces that he can no longer tolerate "foreign meddling," which he claims has ignited misguided, pro-independence voices in Taiwan. He says he is ready to reunify China, by force if necessary, and protect it from "Western influence."

The Chinese government orders a quarantine of Taiwan. China claims it will inspect goods only to ensure no weapons are included, but it becomes clear in the first few days that the quarantine is a de facto blockade. The PLAN turns away ships carrying food, fuel, and components for manufacturing semiconductor chips. The blockade intercepts maritime and air traffic, cutting off Taiwan's vital imports, preventing Western reinforcement and resupply, and disrupting Taiwanese communications for operational and psychological purposes.

Policymakers in Washington anticipate that the quarantine is a precursor to reunification by force, either through economic pressure or a full-scale invasion. They begin scheduling meetings and discussing response options over e-mail and on the phone—conversations that China intercepts.

Prior to the start of the quarantine, Chinese government hackers had installed exploits at U.S. military bases in Japan, the Philippines, and Guam. They established a persistent presence for espionage and deployed malware designed to compromise communication infrastructure, disrupting any deployment or emergency response attempts. Additionally, China positioned explosives on undersea cables carrying U.S. military communications between U.S. bases and between U.S. and Asian bases.

As China intercepts U.S. plans to respond militarily to the quarantine, it decides to pull the trigger on disruptions to military communications in order to deter the United States from engaging. Roughly half of the communications network becomes nonfunctional, but backups to the backups–including flag officers using personal cell phones to communicate via secure messaging apps–keep enough communication flowing to organize a response. The U.S. government triggers contingency plans for rapid deployment to the region and goes on full alert, anticipating a Chinese invasion of Taiwan and potential strikes on U.S. assets in Japan, Guam, and the Philippines.

Taiwan's leaders make a public statement that the blockade is an act of war against a sovereign nation, and the People's Liberation Army (PLA)'s blockade turns kinetic. The PLA suppresses Taiwan's air defenses, and the PLA Air Force strikes communications facilities, including satellite ground stations, undersea cable landing sites, and communications satellites. It then targets mobile and backup communications equipment, and amphibious forces capture ports and seize airfields.

In parallel with the assault on Taiwan, China decides to take more dramatic action to distract the United States. The Chinese president authorizes cyberattacks against critical infrastructure in the United States, and the People's Liberation Army Cyberspace Force (CSF) activates malware deployed months earlier in preparation for such a contingency.

Aiming to create domestic strife and convince the U.S. president that focus needs to remain at home, Chinese government hackers target the James W. Jardine Water Purification Plant in Chicago, which supplies water to 64 percent of the city's residents. Spear phishing provided initial access, which Chinese operatives escalated to control of the supervisory control and data acquisition (SCADA) systems. On the command of Beijing, they use the exploit to dramatically increase the levels of lye (sodium hydroxide) in drinking water. Thousands of people in the Chicago area are poisoned by their water, and many lives are lost. Simultaneously, China plants conspiracy theories on TikTok, suggesting that a white supremacist group is trying to "cleanse" Chicago. TikTok shows the rapid spread of viral videos suggesting the incident was racially motivated. News media report on "rumors" that a white supremacist working at the plant sought to poison Black residents of Chicago. Local police begin to hear reports of looting and unorganized, violent protests.

Policymakers in Washington have the following facts:

- China has set a de facto blockade on Taiwan–an act of war.
- The United States can still communicate with assets in the Pacific using informal methods and satellite communications, but Washington knows Beijing can hold those at risk. There are significant concerns at the Pentagon about reliable secure communications.
- A mass casualty event is occurring in Chicago. No group has claimed responsibility, and rumors are spreading rapidly that it was an inside job by a white supremacist.

- Experts are conducting a forensic investigation of the system, but initial reports point to a hack of the SCADA systems from outside the country. The tactics, techniques, and procedures (TTPs) look like those of the CSF, but there is no hard evidence yet. NSA and USCYBERCOM assess with low confidence that the group is China-based.
- NSA reports new information that strongly suggests the Ministry of State Security, which functions as China's intelligence, security, and secret police agency, has access to encrypted phone communications between the national security advisor and the secretary of state.

Iran

Participants were presented with a scenario involving an Iranian cyberattack on the Hoover Dam. Iranian hackers remotely gained operational control of the floodgates, unleashing a flood of water that inundated downstream towns and cities. The crisis persisted in the aftermath of the attack, as residents were left with limited water resources and power outages, resulting in thousands of deaths.

Participants viewed Iran as a less capable adversary, prompting more severe responses across the board. They were generally unconcerned about the risk of escalation. Read the full scenario below.

It is November 3, 2027. After years of U.S.-brokered negotiations between Saudi Arabia and Israel, the two nations have finally reached an agreement to normalize relations and establish formal diplomatic ties.

Iranian Supreme Leader Ali Khamenei publicly denounces the normalization as a reactionary and regressive move, claiming the Saudis have abandoned the Palestinian cause, given Israel's ongoing occupation of the Gaza Strip. He calls on the "real" Islamic world to attack the House of Saud.

Two days after the normalization is announced, Houthi rebels fire dozens of loitering munitions at Saudi oil facilities, causing an estimated 15 percent of Saudi oil production to be temporarily offline. In response, Saudi Arabia launches a renewed campaign of air strikes against Houthi bases. The Houthis retaliate by launching missiles at Israel, U.S. facilities around the Persian Gulf, and targets in Abu Dhabi and Riyadh. The United States pledges full support to Saudi Arabia and issues a stern warning to Iran: any further Houthi strikes will lead to "strong retaliation," though specifics are not provided.

Iran's IRGC argues internally that Tehran should not wait, and Khamenei approves a cyberattack targeting the United States. Drawing on experience gained in the November 2023 attacks on U.S. water systems, the IRGC gains access to the Hoover Dam's SCADA system, taking operational control of the floodgates. They unleash a flood, engulfing downstream towns and cities as far away as Yuma, Arizona, and Needles, California, resulting in a significant loss of life.

In the following weeks, the crisis continues. Twenty-five million residents in cities that rely on Lake Mead for water, including Las Vegas and Scottsdale, face severely limited water resources. Agriculture in the region suffers immensely. Additionally, the area experiences a significant loss of electricity, as the Hoover Dam's hydroelectric power plant supplies electricity to roughly 1.3 million people. The short- and long-term effects of the cyberattack are devastating: thousands of people die, and the economy suffers severe consequences.

Policymakers meeting in the SITROOM have the following facts:

- A cyberattack on critical infrastructure has resulted in significant loss of life and dramatic economic consequences.
- The IC assesses with high confidence that the attacker was the IRGC, based on TTPs from previous attacks and signals intelligence intercepts of Iranian leaders discussing the operation.
- DHS is unsure whether the threat actor has access to or control over other critical infrastructure systems. It is working through Sector Risk Management Agencies to assess the situation.
- The Houthis continue firing at Saudi Arabia and Israel; Riyadh is launching a massive offensive against Houthi facilities in Yemen; and Israeli leaders are weighing both cyber and kinetic responses against Iran.

Appendix 2

The Charts by the Numbers

Before the games, the CSIS research team formulated the following two hypotheses:

1. In the event of deaths resulting from a cyberattack, policymakers will opt for a stronger, non-cyber-only response.
2. Policymakers will struggle to determine what constitutes a "proportional" response to a severe cyberattack that causes civilian deaths, particularly because the cause of those deaths is indirect.

To test these hypotheses statistically, researchers asked participants in the wargames to read the scenario and then fill out a worksheet identifying their preferred options. Participants selected one policy response in each category (Cyber, Diplomacy/Messaging, Espionage/Covert Action, etc.). Actions at the top of each column (e.g., one or two) represented low-magnitude responses, while those near the bottom (e.g., seven or eight) were higher-magnitude, often kinetic, responses. This task was completed before discussions began on how the group should respond, aiming to capture individual preferences before anyone was influenced by a persuasive group member. The chart served as a starting point for discussion, but participants were not bound to the listed policy options and could write in other responses at the bottom of the chart.

Table 1: Wargame Worksheet

	Cyber	Diplomacy/ Messaging	Espionage/ Covert Action	Economic/ Sanctions	Law Enforcement	Military
Response Magnitude (1 = low, 7 = high)	1. Espionage (ramp up efforts to access internal communication)	1. Private messaging to dissuade further action	1. Aggressive collection efforts on cyber forces	1. Travel sanctions against cyber actors	1. Repossess stolen assets (chase the bitcoin)	1. Messaging from USCYBERCOM about capabilities
	2. Operational preparation of the environment (OPE) (creating backdoors and implanting malware for potential use later)	2. Outreach to allies and partners to share information about the attack	2. Covert messaging campaign directed at cyber actors (e.g. targeted text messages to private cell phones)	2. Financial sanctions against cyber actors and/ or leadership	2. Pursue criminal indictments against cyber actors and leadership	2. Schedule exercises with regional allies
	3. Loud OPE (Design your OPE efforts to be found, by way of demonstration of capabilities)	3. Name and shame: Public messaging to call out the activity	3. Covert messaging campaign directed at adversary's domestic audience	3. Seize state assets	3. Civil lawsuits for damages	3. Move additional assets into theater
	4. Disruption (temporary shut downs of activity)	4. Directly threaten retaliation	4. Harassment campaign against their leadership	4. Sanctions on major financial institutions	4. International cooperation to seek arrests	4. Conduct in-theater exercises immediately
	5. Destruction (physical destruction of property, but no casualties; only economic consequences)	5. Call for international coalition against cyberattacks	5. Covert sabotage of government functions	5. Central Bank sanctions	5. Propose new legislation to Congress for stiffer penalties for cyberattacks	5. Harassment of military and civilian assets, ranging up to potential quarantine operations
	6. Destruction with physical damage, potentially including human casualties	6. United Nations Security Council (UNSC) resolution	6. Covert sabotage of critical infrastructure	6. Tariffs on attacker's goods		6. Targeted strike on cyber facilities
	7. Attack on critical infrastructure, likely causing death or extensive illness	7. Invoke Article 5 of the NATO treaty	7. Covert kinetic action in adversary's homeland	7. Economic blockade		7. Comprehensive military strike

Recommended Response

Target(s) & Goals:

Expected Outcome:

Hypothesis 1

In the event of deaths resulting from a cyberattack, policymakers will opt to pursue a higher-order, non-cyber-only response.

Further testing is needed to definitively prove or disprove this hypothesis, as this variable was not effectively isolated in the game design. Statistical analysis of the written results from this round of games showed little difference in participants' preferences for kinetic action against Iran, Russia, or China. Given the large number of lives lost in Iran's attack, if the first hypothesis were valid, researchers would expect to see a statistically significant difference in the non-cyber responses in the Iran game compared to the other two games.

After analyzing participant response magnitudes written in the chart on page 26, the only statistically significant finding was that Iran had a higher non-cyber magnitude than Russia. However, there was no meaningful difference between Iran and China, or Iran compared to both Russia and China. Therefore, researchers concluded from this set of games that Hypothesis 1 was not valid, meaning a higher death toll did not necessarily lead to a higher-order, non-cyber response in these games. Researchers would like to rerun the game, removing the Taiwan elements of the China scenario to better isolate the potential for military reactions to a severe cyberattack.

Interestingly, researchers found that Iran had a statistically significant higher cyber response magnitude than both Russia and China, meaning **participants in the Iran game opted for higher-magnitude cyber weapons compared to those in the other games**. The average cyber response magnitude for Iran was six: "Destruction with physical damage, potentially including human casualties." Multiple participants also selected option seven, involving attacks on critical infrastructure and causing death or widespread illness. The average cyber response magnitudes for Russia and China were four and 5.5, respectively. This may reflect Iran's more limited cyber capabilities or the significant loss of life in this scenario, prompting policymakers to use every tool in their tool kit.

Hypothesis 2

Policymakers will struggle to determine what constitutes a "proportional" response to a severe cyberattack resulting in many deaths.

If Hypothesis 2 were valid, researchers would expect to see noisier data and more observable variance between categories in the Iran game compared to the Russia or China games, as noisy data indicates that participants struggled to arrive at a response. Researchers found that Hypothesis 2 is valid, highlighting that **experts struggled to identify a proportional response to a cyberattack resulting in a high number of deaths.**

Other Findings

Policymakers were less likely to call for diplomatic responses to a destructive cyberattack perpetrated by Russia than by Iran or China. This may be a result of Russia's current diplomatic isolation, suggesting that Russia cannot be influenced by political messaging. In the Russia scenario, participants selected lower-magnitude options for diplomacy ("name and shame: public messaging to call out the activity") than in the Iran and China game ("call for international coalition against cyberattacks").

Participants selected a statistically significantly higher average magnitude for military response in the China game compared with Russia. In the China game, participants selected an average of approximately five ("harassment of military and civilian assets, ranging up to potential quarantine operations"), but only three for Russia ("move additional assets into theater"). Much of this difference is likely explainable by the context of the scenario, where Russia was reengaging against Ukraine, while China was making a new military move against Taiwan.

In the Iran scenario, participants selected a statistically significant higher-magnitude covert action/espionage than in the Russia or China games. The mean option selected for Iran was nearly seven, the highest option, calling for "covert kinetic action in their homeland," whereas the mean magnitude for Russia was almost four ("harassment campaign against their leadership") and five for China ("covert sabotage of government functions").

COVER PHOTO LEENA MARTE/CSIS; MOCKO/ADOBE STOCK
PHOTO CREDIT: THE WHITE HOUSE

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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