SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 1: Executive Summary

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 1: Executive Summary

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 graciously agreed to be interviewed. The authors would also like to thank Susan Hines for helping 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

Evolution and Revolution	1
Summary of the Cyber Playbook Project	2
Findings on Adversaries	3
Wargames	5
The Playbook	8
Attack Response	12
Call to Revolution	14
About the Authors	15

Authors' Note About the Series

This report is part of a series on the future of cyber warfare. This part of the series covers the topline points of each section of the larger project, highlights key takeaways from the comparative studies, distills lessons drawn from the wargames, and brings together insights from the series as a whole. It also summarizes the new cyber playbook and proposes guiding questions that policymakers can use to shape responses to future cyberattacks.

Parts 2, 3, and 4 of this series examine how Russia, China, and Iran, respectively, fight in the cyber domain, and Part 5 examines U.S. cyber practices. 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.

Evolution and Revolution

The United States has been losing a war it did not know it was fighting, and it has been losing for the last 20 years. To reverse this trend line and make full use of its strengths, the United States needs to evolve its thinking and its policies about offense to fully integrate cyber tools as a larger part of national security. In certain areas, it must think past evolution—to revolution. It must revolutionize the concept of proportional response, recognizing that cyberattacks are hostile acts, not just part of the cost of doing business. Second, it must revolutionize defense, shifting focus and resources to build true resilience. Finally, it should revolutionize the structures that support cyber operations. It is time to create a cadre of soldiers built for cyber conflict, and their home should be a new Cyber Force standing alongside the other service branches. This combination of evolution and revolution must add up to a coherent strategy, where cyber is seamlessly integrated as part of foreign policy and policymakers are not scared to use it. This project describes the way forward.

Summary of the Cyber Playbook Project

This project provides a playbook for how the United States can fight smarter and win in the cyber domain. The research consisted of in-depth investigations of the cyber capabilities of Russia, China, and Iran, as well as the United States. Russia and China have fully integrated cyber tools into their larger foreign policy tool kits. Iran is a growing cyber powerhouse, learning from Russia's and China's approaches. All three have demonstrated both a strong defense and a willingness to use offensive tools aggressively. There is a clear strategic gap for the United States: Its adversaries are near-peers in offensive cyber tools but have far more willingness to use these tools for political ends and have a much stronger domestic defense.

To understand how U.S. policymakers think about cyberattacks, researchers conducted a series of wargames, which demonstrated the urgency of this project. Cyber strategy as a part of warfighting is still a foggy concept in the minds of policymakers, even several decades into the modern digital age. Clearing this fog before the next round—or rounds—of cyber conflict will be essential to a U.S. victory.

Finally, the project provides actionable steps to enact a cyber playbook that will posture the United States for success. This playbook builds on previous flagship projects like the Cyberspace Solarium Commission (CSC), and it proposes concrete measures to evolve some policies and revolutionize others.

This chapter covers the topline points in each section of the larger report. It highlights key takeaways from the comparative studies, examines lessons drawn from the wargames, and brings together insights from the series. It explains six key areas of action, which are part of a new cyber playbook, and identifies critical questions policymakers can ask in the future to guide their response to a cyberattack.

Findings on Adversaries

Russia Poses a Continuing Threat, China Pulls Even, and Iran Adopts an Aggressive Stance

CSIS researchers focused on Russia, China, and Iran because they pose the greatest near-term threat to the United States in every domain, including cyber. Further, each has demonstrated a willingness to use cyberattacks to further a foreign policy goal.

- Moscow constantly uses what it calls information confrontation (*informatsionnoe protivoborstvo*, or IPb), encompassing both cyber tools and information operations, as an important instrument of policy, even during putative peacetime. It considers itself constantly in an information war with the West. Furthermore, the war in Ukraine may give a false sense of security about the threat Russian cyberattacks pose. Unlike Ukraine, the United States lacks resilient systems. Meanwhile, Moscow is learning from its experiences in Ukraine and advancing its cyber capabilities with emerging technologies.
- For Beijing, war and peace are not separate endeavors, but a spectrum. China has been operating at a low level of warfare continuously, using cyber-forward hybrid tactics for decades. While Russia has historically been at the forefront of the cyber domain, starting from the dawn of the internet, China has caught up and is now the top threat to the United States in the cyber ecosystem. Beijing's combination of immense resources and aggressive persistence have made it prodigious in espionage and formidable in operational preparation of the environment (OPE).
- Iran has emerged as an aggressive cyber actor, willing to poke the United States in vulnerable spots with attacks on critical infrastructure. While less advanced than Russia or China, the ongoing conflict with Israel and the United States has prompted Tehran to accelerate its

cyber prowess. Tehran has already targeted U.S. civilian critical infrastructure and is likely to continue pursuing destructive cyber activities.

Evaluating the gap between these adversaries and the United States revealed that Washington would probably lose a purely cyber-versus-cyber fight. Each of them has demonstrated advanced capability and willingness to use that capability against the United States. Each has also built exceptionally strong defenses, largely due to their paranoia about domestic unrest, but these walls are dual-use, capable of defending against domestic usurpers just as much as from foreign powers. Meanwhile, the United States has repeatedly deprioritized defense, resulting in a massive, lightly defended attack surface. The United States is exposed and, as a result, has been unwilling to risk an escalating tit for tat in the cyber domain. This gap means Russia, China, and Iran can largely choose the level of conflict in the cyber domain, leaving the United States constantly plugging holes in the ship's hull and bailing out, rather than sailing on. The wargames, explained in the next section, found that these dynamics will severely hamper an effective U.S. policy response to a massive cyberattack.

Wargames

The Fog of Cyber War Prevails

CSIS researchers ran a series of three wargames to test how foreign policy practitioners' implicit assumptions and views would play out in an extreme circumstance: a cyberattack inside the United States that causes deaths and injuries. The games showed that foreign policy practitioners have no common underpinning for thinking about a cyber conflict, nor do they have a coherent view on what counts as an act of war or as a proportional response. (See Part 6: Testing U.S. Policy Responses to Destructive Cyberattacks with Wargames for the full readout of the game.)

This exchange illustrates the confusion:

> Player 1: So, what qualifies as a tit for tat in the cyber realm?
>
> Player 2: 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.

One can imagine this discussion taking place in the Situation Room during a crisis. Confusion reigns in such a situation, and that confusion is only exacerbated by the uncertainty about what cyberattacks really signify. This could cost the U.S. precious hours.

Each scenario was fictional when written—all were created prior to the public acknowledgement of the Volt Typhoon attacks and before the Iranian attack on water facilities running Israeli software. But they drew on the same themes, just expanded to true crisis levels. There was one game each for Russia, China, and Iran:

- 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. This scenario was meant to represent a **low death count, very low-confidence attribution, and a fight against a 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 "many deaths." This scenario was meant to represent a **medium-severity death count, low-confidence attribution, and a fight against a near-peer competitor.**
- Finally, in the Iran scenario, renewed regional fighting was the context for a cyberattack on the Hoover Dam, which resulted in a full breach, ensuing flooding, and thousands of deaths. This scenario was meant to represent **a high death count, high-confidence attribution, but not a near-peer competitor.**

The higher the casualty count, the more likely participants were to recommend an aggressive response. In the Iran scenario, which had thousands of deaths and almost certain attribution, participants favored swift, kinetic retaliation. That level of response was easier, of course, because the adversary is militarily weaker than the United States. In contrast, participants showed far greater hesitation to escalate to kinetic response when confronting near-peer adversaries like Russia and China. In those scenarios, there were fewer deaths and those deaths were indirect, leading participants to debate whether Moscow and Beijing intended to cause casualties or disruption. The muddier the scenario, the muddier the thinking of the players, which is reflective of likely real-world scenarios.

At the end of each game, researchers asked participants to individually answer the question: Are we at war? The goal was to examine when policymakers would consider a cyberattack severe enough to count as hostilities. Responses varied:

- In the high-casualty Iran scenario, all but one participant said yes (89 percent of participants).
- In the China scenario, 82 percent of participants said yes (nine in total), while 18 percent said no (two participants). The yes votes took into account the combination of the Chinese quarantine of Taiwan, a disruption to U.S. military communications, and the cyberattack.
- 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; the "no" group was worried about misattribution and about escalation to a nuclear conflict.

Participants hotly debated how to respond to the aggression in each scenario. They said cyber tools felt inadequate as a response for several reasons: The expected consequences were not harsh enough to qualify as a complete response; the tools they wanted were unlikely to be quickly available; and the message sent would be too weak. The overall takeaway from the games was that cyber is still poorly understood and that policymakers need a new playbook to grapple with this form of warfare. A summary of that playbook follows in the next section.

The Playbook

How to Win a Cyber War

Creating the conditions for the United States to succeed in a cyber war will require evolution and revolution. It starts with a new mindset that breaks free of complacency and silos. Next, the U.S. approach to offense must evolve, and policymakers should issue a bold new statement of policy. Critically, it requires a revolution in defense and new structures to bolster U.S. capabilities. Each interlocking piece will make Washington's position stronger across the spectrum of conflict. (For the full text of the playbook, see Part 7: How the United States Can Win.)

Evolution: A New Mindset

The United States is fundamentally complacent about cyber. The prevailing mindset is as follows: The threat of catastrophic attack is theoretical, defense is probably good enough, and cyber is something for technical experts to worry about, not foreign policy generalists to use. This complacency cedes ground to adversaries and hamstrings both offense and defense. A new mindset is necessary, where cyber is an integrated part of the larger foreign policy picture. Policymakers need to remove the handcuffs of fear caused by a weak defense, empower U.S. actors to use their imagination on offense, and think about cyber access as a source of leverage.

Evolution: Empowered Offense

Policymakers must build a strong, flexible, and empowered offense. One mental model is an octopus: a creature that has a central brain organizing the effort, but also a mini-brain in each tentacle that allows it to adapt quickly to the environment. It can crawl effectively over a reef,

letting each tentacle be opportunistic in finding food while ensuring all tentacles continue to move the creature in a clear direction. An octopus model for offensive cyber operations might include strategic guidance from the National Security Council (NSC), serving as the central brain; interagency cyber campaign planning; a forward-leaning approach to exploration and opportunism; and delegation of responsibility to the National Security Agency (NSA), the Central Intelligence Agency (CIA), and U.S. Cyber Command (USCYBERCOM) or its successor for execution of low- and moderate-risk missions. The new idea here is a more integrated whole with clear centralized guidance.

Revolution: Redefined Proportionality

Policymakers must revolutionize outdated conceptions of proportionality for the cyber domain. The old model of retaliating against cyberattacks largely with cyberattacks is outmoded and a guaranteed losing strategy for the United States. Washington has been rightfully unwilling to use cyber where it might be most impactful but also most malicious—against critical infrastructure in attacks sure to hurt civilian populations. Further, Washington does not endorse harassment of businesses by cyber criminals or massive IP theft. This self-restraint is right and comports with democratic values, but in order to effectively defend the United States against aggressors, Washington needs alternative mechanisms for signaling and appropriate retaliation. Otherwise, adversaries will consistently win on the escalation ladder.

Any single cyberattack is unlikely to cause enough damage to merit a strong economic or even kinetic response. For example, the United States should not respond to a ransomware demand with a cruise missile. However, pinpricks add up to an intolerable chorus of pain for U.S. businesses and government entities, and allowing these attacks to continue with little to no response destroys any semblance of deterrence. As a result, the United States needs to shift its thinking on proportionality to consider the entire pattern of behavior and draw on a wider tool kit, such as a combination of sanctions, regional diplomacy, cyber retaliation, and—in extreme circumstances—kinetic action. The section on page 12 called “Attack Response” lays out seven questions that can help guide policymakers to an appropriate response to a cyberattack.

Revolution: New Statement of Policy

This shift must be accompanied by explicit signaling of the change. The United States must publicly warn that it will no longer be walked all over in the cyber domain and that attacks will be met with far harsher responses. Adversaries will test that new stated resolve, and Washington should be loaded with retaliatory options to signal seriousness.

Revolution: Demanding a Strong Defense

Critical to this new approach is revolutionizing how the United States prioritizes defense so that it is treated as a no-fail mission. If the United States leaves itself open to easy attacks, Washington will find itself retaliating far too often, and every retaliation both exhausts the U.S. tool kit and has

potentially risky results. Instead, creating effective defense and improving societal resilience means harsh retaliation will be reserved for only rare, effective, extraordinary attacks.

Secure-by-design efforts of recent years are a step in the right direction. For too long, software makers have gotten away with a publish-first, patch-later approach, which prioritizes getting a product to the market rather than insisting on thorough testing and security. Further, Congress should look at incentives for entities to learn to safely fail and quickly recover, creating resilience in the face of an ongoing epidemic of ransomware attacks. Societal resilience is harder to incentivize but is equally important. Schools should teach good cyber hygiene early, including using multi-factor authentication on school devices. Further, Congress should create a pipeline of cyber talent who begin their careers working in state, local, tribal, and territorial governments. Such a program could repay student loans for recent graduates who work in school districts and other vulnerable state and local-level offices, experience that would also help them apply and hone their recently acquired cyber skills.

Revolution: New Structures

Three bold steps that create improved structures would bolster the United States' ability to fight in the cyber domain. First, Congress should eliminate the so-called dual-hat, where the same person is director of NSA and commander of USCYBERCOM. Creating a balance between military and intelligence activities has been a continuing irritant, and having one boss at the head of two missions is likely cheating both. Strong, visionary leadership is needed to appropriately integrate cyber activity into modern national security efforts, and each organization should have a capable leader advocating for its interests as part of that larger whole. It is time for an amicable divorce, to allow each element to grow and engage in this fight.

Second, the United States should create a Cyber Force alongside the Army, Navy, Air Force, Marines, Coast Guard, and Space Force, allowing the United States to build a force fit for purpose. It would provide a pathway to advancement for ambitious cyber warriors, and it would allow recruitment standards that are significantly different from those required by other services. The emphasis should be on creating a robust reserve cadre, as industry will surely lure away many of these troops. However, a new Cyber Force should embrace that exodus, letting its reserve cadre hone its skills with the best inside and outside government and creating strong, enduring linkages between the U.S. military and industry leaders.

Third, there needs to be greater accountability for U.S. government cyber defense. Departments and agencies have repeatedly postponed or canceled major IT upgrades that would have created a far more secure government, using the rationale that the threat was theoretical and that limited resources should go to core mission functions. Department heads should be held accountable for low cybersecurity scores, including with removal in extreme situations. CISA should also send an intervention team to take over cyber defense efforts at departments and agencies that fail two cybersecurity audits in a row.

With these new policies and frameworks in place, decisionmakers will be far better prepared for a crisis. The next section lays out seven questions that leaders can use to further hone their thinking when such a crisis occurs.

Attack Response

Seven Questions for Decisionmakers

CSIS's wargames showed that policymakers did not know how to assess the severity or impact of a cyberattack as a precursor to choosing a proportional response. That wheel spinning would be disastrous in the middle of a disruptive cyberattack, when leaders will need to triage information and rapidly decide on the best course of action. This set of seven questions will help them parse the known and unknown aspects of a situation, as well as its implications, and suggest a set of responses:

1. **How much damage is there**? Was there loss of information, property damage, or risk to health and life? Were there casualties?
2. **Are there more attacks coming?** Is the attack an opening salvo in a string of attacks, or is it an isolated incident?
3. **Do Americans need reassurance?** Did the attack cause panic or fear about the safety of critical infrastructure?
4. **How certain is the attribution?** Is it highly likely authorities know the actor, even if the evidence is not ironclad? What evidence would the United States need to feel confident about the identity of the actor, and is that evidence likely forthcoming?
5. **How has the perpetrator's behavior evolved over time?** Has the actor been increasingly aggressive? Is the act significantly more aggressive than previous attacks?

6. **Did the intent of the attack match the outcome of the attack?** Cyber tools can cause unintended consequences: Was this attack meant to cause casualties or disruption? Was it meant as theft or to disable a key part of state functioning?
7. **What was the target?** Is the victim industry, non-profits, or government? Is this a concerted attack on a particular sector over time? Does there seem to be a larger pattern striking at a key function? Somewhere on the spectrum between a ransomware attack on a small business and a malicious cyberattack that causes physical damage to a large defense contractor, the U.S. government will find the point at which an event is an attack on national interests. While that tipping point is hard to define, policymakers should explicitly consider it and the precedent they are setting with their response.

The answers to each of these seven questions should inform the severity of the U.S. response to an attack. A chart in Part 7: How the United States Can Win goes into further detail about parsing these questions and potential policy responses.

Call to Revolution

Fixing Cyber Policy Is Urgent

U.S. adversaries have had 20 years largely unopposed to hone their offensive cyber skills and test the United States' will to respond to a series of increasingly aggressive attacks. Washington must recognize the significant gap between cyber activity conducted by Russia, China, and Iran and the United States' defense.

The United States is behind, but that can change quickly. Catching up must begin with a concerted effort to build resilience at home, using new incentives and penalties for shirking security responsibilities. Then, Washington must make a bold new statement of policy, demonstrating the intent to silence the continuing drumbeat of cyberattacks. But stated intent is hollow without a demonstration of will; the United States should be ready to prove it will no longer tolerate cyberattacks as the cost of doing business. That demonstration should herald a new era of readjusted norms, moving back toward protection of civilian populations, intolerance for harassment and disruptions, and consequences for continuous attacks. Policymakers have a new playbook to upend—and win—the cyber game.

About the Authors

Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program and vice president 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.

COVER PHOTO LEENA MARTE/CSIS; MOCKO/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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