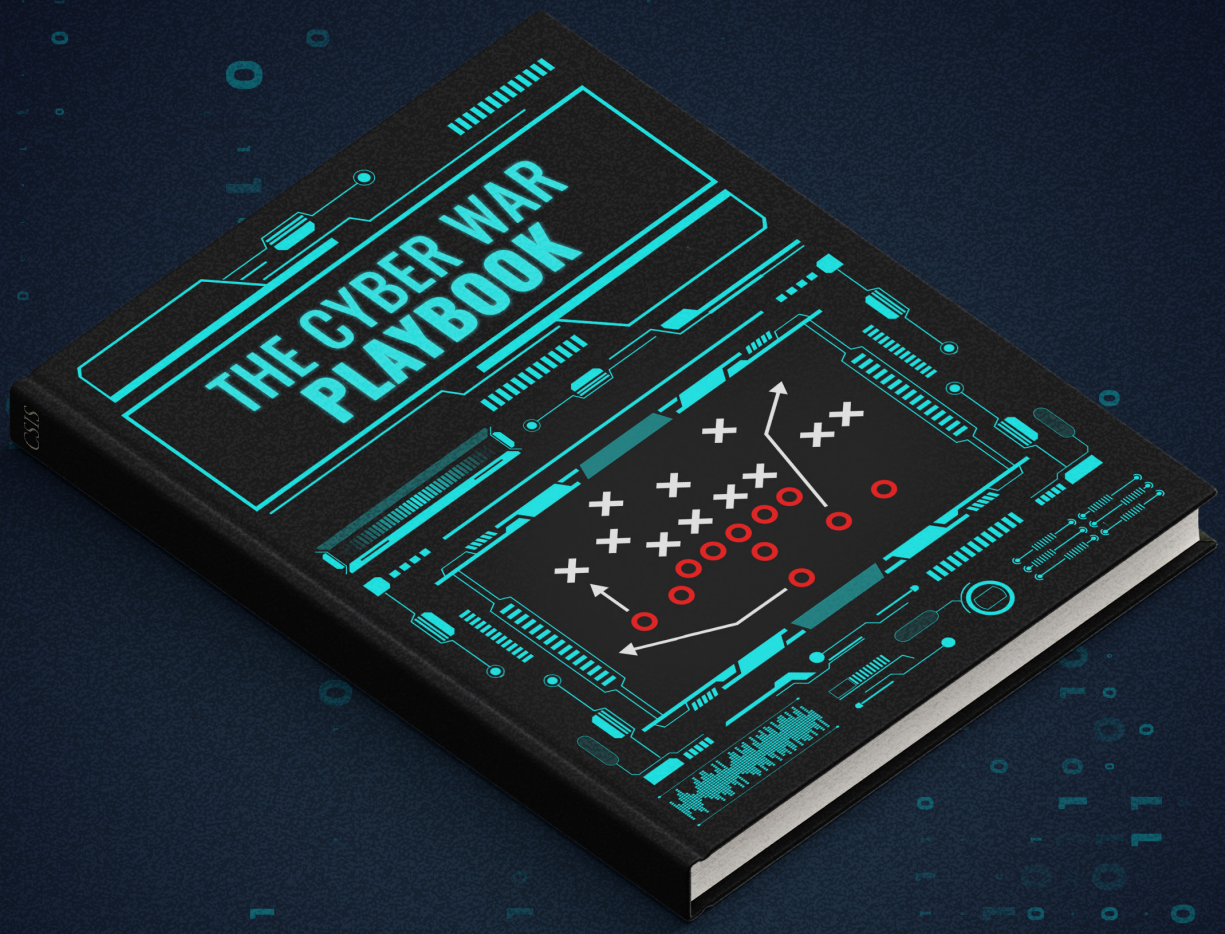
SEPTEMBER 2025

A Playbook for Winning the Cyber War

Part 7: How the United States Can Win



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 7: How the United States Can Win

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 Krista Auchenbach and Nikita Shah for providing valuable feedback, 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

Authors' Note About the Series

This report is part of a series on the future of cyber warfare. This part of the series offers a new playbook and set of recommendations for U.S. policymakers to help the United States fight and win in the cyber domain. The playbook is organized into several key components: a new mindset, an evolved approach to offense, a redefinition of proportionality in the cyber domain, a bold statement of policy, stronger defense, and new structures to bolster U.S. capabilities.

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. 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, this part (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 Playbook

The 2009 "Cyberspace Policy Review" started with fine words: that the nation is at a cross-roads, that the status quo is no longer acceptable, that the national dialogue must begin today, that the United States cannot succeed in isolation, that the United States cannot abrogate its role, that the country needs objectives for its next-generation infrastructure, and that the White House must lead the way forward. All in all, this business of developing cyberspace strategies appears to have been dreary work, recycling clichés for over a dozen years—the consequence of not being able to decide that cybersecurity is not a government problem but not being willing to do much about it either.

—Martin Libicki, Cyberspace in Peace and War[1]

China and Russia figured out how to bring down a superpower more than a decade ago. Rather than attack the superpower's strengths, they operate where it is complacent, forgetful, and weak. During the 20-year Global War on Terrorism, the United States built a military that was expert at counterterrorism, but it neglected the other elements of statecraft. It assumed the rules-based global economy would endure. While the United States focused on counterterrorism, Russia rose as a cyber superpower, conducting some of the earliest and most disruptive cyberattacks. China took the opening to slowly, nearly imperceptibly expand its influence over the economic and information space while also building military power. A lynchpin of China's strategy was aggressive activity in the cyber domain. Iran has also emerged as a hostile actor in this domain, devoting considerable resources to bolster its capability while demonstrating a brazen willingness to attack civilian critical infrastructure.

As Russia blazed a trail in this domain, China followed, with the former excelling in information operations and the latter engaging in an epic campaign of intellectual property theft. These U.S. adversaries changed the chessboard while the United States was not looking. Washington responded belatedly, slowly, and incorrectly. It originally interpreted Russia's hacking activity as normal espionage or low-level harassment. Chinese intellectual property theft started as annoying, became expensive, and then became an existential threat to many businesses. Washington was the proverbial frog in the pot, not noticing the increasing heat as both adversaries went after government networks. Worse, the United States was slow to increase its defenses against this creeping threat.

The mental framework of U.S. foreign policy scholars and practitioners facilitated this drift into complacency. The prevailing view has been that cyber activity is in a silo; it is for technology experts, not policymakers. Even if the cyber domain is an element of warfare, it is different from other war-fighting methods—safer, slower, less useful, and less consequential. Cyberattacks are viewed less like weapons and more like crimes or natural disasters. One leading scholar, Martin Libicki, compared cyberattacks to rain, saying that whereas wars must be won, rain must simply be "endured."[2] Similarly, some have argued that the cyber domain is a relatively safe arena for great powers to compete, given the low likelihood that a cyberattack will cause physical harm to a population, particularly compared to kinetic and nuclear conflict.[3] Some have argued that action in the cyber domain is inherently de-escalatory because cyberattacks are usually met with a cyber response and that cycle is slow and deliberate.[4] Consequences are annoying or disruptive but unlikely to cause death and destruction.

The problem with analogizing cyberattacks to rain or a natural disaster, or considering it a safe zone for competition, is that such thinking is dangerous and outdated. The first danger is that the analogy undersells the threat. Some rainstorms merely flood the basement; others are hurricanes. In the fall of 2024, a Category 4 hurricane hit Florida. That was nothing new—Floridians understand the danger and know how to prepare and rebuild. But Hurricane Helene did something few storms have done in recorded history: It went directly north, tearing through Appalachia. The storm killed more than 230 people and caused many millions in property damage, fully destroying several towns. Perhaps many rainstorms can simply be endured, but a hurricane that does not act as expected can leave millions reeling from the damage.

The second danger is that the analogy removes agency. Natural disasters have no actor; there is no one to blame. Further, a hurricane cannot be deterred. Neither can a tornado be convinced to turn around. Hurricanes do not decide to strengthen because they can get away with it; they do not decide that because their attacks are working, they should push harder. But cyberattackers—particularly state actors—make these decisions every day.

Since 2016, when Libicki likened cyber threats to rain in his book *Cybersecurity in Peace and War*, Moscow has used cyber tools to undermine Western democracies with attacks on elections;[5] cyberattacks have proven increasingly disruptive to the global economy as an epidemic of ransomware attacks—conducted by criminal groups sheltered by powers like Russia—has wreaked havoc; and another book came out with a much more sensational title: *This Is How They Tell Me*

the World Ends, by Nicole Perlroth. Cyber actors in China, Iran, and Russia have used cyber tools to undermine democratic institutions, support their military objectives in Ukraine, and infiltrate critical infrastructure, potentially aiming to handicap U.S. deployment to a conflict in the Pacific. Cyber criminals have drained billions of dollars from economies through ransom payments and outright theft—losses that have never been fully quantified.[6] Cyber threats are far beyond rain.

A new cyber doctrine should be a bold policy statement for a pivotal moment in history.

A new era of cyber power needs a new way of thinking and new actions to back it up. Much like the Monroe and Truman Doctrines, a new cyber doctrine should be a bold policy statement for a pivotal moment in history. This new doctrine should include the following elements: First, shore up defense and prioritize resilience. Second, break down cyber silos, and stop thinking of cyber tools as different or separate from the spectrum of conflict. Finally, create a coherent strategy where cyber policy is seamlessly integrated into foreign policy and policymakers are not scared to use it. Elements of such policy have appeared in previous statements, but actions have not followed through.

How do U.S. policymakers get from here to there? They must adopt a theory of deterrence in the cyber domain, expand the definition of a "proportional" response to a cyberattack, and create new government structures to reinforce this change. The time to settle these questions is now, before the United States and its allies find themselves in the midst of a crisis. (For a complete exploration of confusion in a crisis, see Part 6: Testing U.S. Policy Responses to Destructive Cyberattacks with Wargames.)

The section that follows is a summary of the top recommendations. The subsequent section examines each recommendation in depth and provides actionable guidance for policymakers to advance security. The third section outlines the questions policymakers should consider when selecting how to respond to a cyberattack. Finally, the last section demonstrates how policymakers should use the new playbook.

Summary of Recommendations

The United States urgently needs to integrate cyber into its larger foreign policy tool kit, deciding how cyber activity fits in with larger foreign policy actions, including deterrence, proportional response, and international norms. To do so, Washington should pursue the following actions:

1. **Create six new frameworks for a new era:**
    i. **Reframe offensive operations—think like an octopus.** Offensive cyber tools, at their best, are flexible, inventive, and opportunistic, akin to how an octopus hunts in the wild. Cyber offense must combine long-term planned campaigns and instant opportunism—like an octopus's central brain and tentacles.

ii. **Redefine proportionality and escalation to include the big picture.** Policymakers' view of proportionality must expand beyond the most recent incident and consider the aggregate costs of a pattern of attacks, the long-term economic and security consequences of those attacks, and the message sent by inaction. A new policy, which could be called "cyber first-cyber optional," must begin with explicit principles that the United States is redefining proportionality in the cyber domain, bolstering defense, and putting adversaries on notice that in the future the United States will retaliate for the overall pattern of behavior, not any one attack in isolation, and will use all tools at its disposal.

iii. **Lay the groundwork for deterrence.** Defining international norms of behavior will establish a clear baseline to facilitate future action, making it a worthwhile exercise, even if many states are likely to ignore them. Further, demonstrated will is critical to deterrence. A strong U.S. and allied response to the first cyberattack after an explicit policy goes into place will help set a new tone.

iv. **Get comfortable with being uncomfortable about the level of attribution.** There may be moments when it is necessary, even prudent, to act before definitive attribution. Establishing consequences for malign actors is a worthwhile goal, and the benefits of sending a strong message of response could outweigh the relatively small risks of misattribution. Make a plan to act in the face of uncertainty.

v. **Reimagine the cyber warriors.** Cyber war is largely fought on private networks with combatants who do not wear uniforms. The cyber domain needs its own service—a Cyber Force that can be built for purpose. It should tilt heavily toward reserve service, and its physical requirements should be utterly different from those of the Marines, for example. Further, the United States must view private sector partners as real partners. It should put in place protections for cyber operators who act in conjunction with the U.S. government, as so many from the private sector did in Ukraine.

vi. **Focus on defense as a no-fail mission.** A stronger cyber defense at home is a worthy goal in itself, but it is also the key to an unleashed U.S. offense. As long as policymakers worry that the home front is vulnerable to adversary attacks, they will hesitate to retaliate. To flip the script, the United States must make its adversaries believe that a cyberattack, particularly on U.S. critical infrastructure, will do minimal long-term damage to the United States and that retaliation, in whatever form, will be swift and painful. To create that stronger defense, the Cybersecurity and Infrastructure Security Agency (CISA) needs leverage beyond its convening and cajoling efforts. Departments and agencies must be held accountable for their investments—or lack thereof—in cyber defense.

2. **Establish a methodology for decisionmaking in a crisis**. Policymakers faced with the challenge of responding to a large cyberattack should start by answering seven questions. These questions will illuminate aggravating circumstances and suggest a set of responses that establish escalation dominance and create deterrence. (See page 19 for the list and see page 22 for a chart laying out potential response options.)

3. **Run the playbook.** Be bold. Match creative policy responses to the pain points of the particular attacker. Demonstrate that the United States will view a cyberattack that causes damage as just as serious as a kinetic attack. Plan for success on offense, confident in the strength of defense.

Six New Frameworks for a New Era

The term "theory" is much derided in policymaking circles. Practitioners are presented with urgent, crisis situations and must respond without considering which international relations theory underpins their decisions. The time to develop a worldview is before a crisis hits. This section does just that—exploring new concepts in cyber warfare and establishing a coherent theoretical underpinning so policymakers have a solid foundation for decisionmaking.

The suggested framework is evolutionary rather than revolutionary. Many of these ideas have been tried piecemeal; the newness comes in the coherence and overall approach—a shift away from the last-minute sprinkling of cyber ideas on top of an existing policy and toward an integrated approach that unites existing efforts. It includes new ways to think about offensive operations, proportionality and escalation, deterrence, standards of attribution, who qualifies as a combatant in cyber war, and defense and resilience. Each of these new frameworks points to actions: a new set of policies that will bolster U.S. capabilities in that area. This section describes each new framework, followed by recommended actions to make the new frameworks not just theory, but a regular part of practice.

1. Offensive Operations: Think Like the Octopus

The United States has treated offensive cyber operations as an exquisite, limited tool kit for narrow use in controlled circumstances. But warfare is evolving, as is conflict in the cyber domain. Adversaries use offensive cyber for a wider range of purposes than Washington and are less risk averse, thus outstripping the United States in agility and opportunism. While the United States should not abrogate its values and match adversaries who use cyber against civilian populations and

conduct rampant intellectual property theft, Washington must play to its strengths and rethink how it uses offensive capabilities to keep up with agile adversaries.

Offensive cyber tools, at their best, are flexible, inventive, and opportunistic, akin to how an octopus hunts in the wild. An octopus camouflages itself perfectly, uses its tentacles to explore nooks and crannies, and squeezes into impossibly small corners to wait for its prey. It solves problems, learns, and strikes decisively. Further, each tentacle acts independently but also as part of a whole. The central nervous system guides the effort, but a brain in each tentacle manages the search.

An octopus model for offensive cyber operations might include strategic guidance from the National Security Council (NSC); interagency campaign planning; a forward-leaning approach to exploration and opportunism; and delegated 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. For example, the goal might be to disrupt the supply chains for Russian arms. To achieve this, the interagency might aggressively lean into cyber tools as part of a comprehensive government approach that should also include sanctions, diplomatic engagement with regional partners, and attempts to secure weapons precursors through legal intervention. For the cyber piece, the national security advisor would issue guidance asking cyber elements to find vulnerabilities within the Russian arms procurement ecosystem—with the goal of identifying key nodes in those chains, from arms imports from North Korea to parts from China to the factories and plants that produce weapons in Russia—and order operational elements to preposition to disrupt those networks. The stakes are high, but the risk is low, as none of those actors would be shocked if such an effort were discovered.

Thus, U.S. cyber actors can crawl across the reef, searching for vulnerabilities and entry points. Central coordination continues to be essential to ensure that multiple tentacles are not exploring the same barren holes or, worse, attempting to grab the same morsel of food and thus tangling and failing. The campaign plan is the planned path of the octopus, seeking to cover an entire section of the reef without doubling back and retreading the same empty ground.

This framing is an evolution, not a revolution, from today's offensive model. Today, the U.S. government has plenty of cyber coordinating councils and brief references to cyber policy in strategic guidance, but these pieces do not operate as a strategic whole. Cyber policy plays a late, minor supporting role to the main characters in foreign policy. The needed evolution, then, depends on two actions: (1) sliding risk tolerance far higher, freeing operators to do more as the opportunity arises, and (2) shifting planning far to the left on the timeline, incorporating cyber tools in the early-stage policy planning process.

RECOMMENDED ACTIONS FOR OFFENSIVE OPERATIONS

- **Adjust risk tolerance**. A shift toward a higher risk tolerance for rapid action is essential for a more flexible, aggressive approach**. Cyber offense must combine long-term planned campaigns and instant opportunism**, as explored in the other chapters in this series. A large campaign is essential to create a coherent long-term approach, but within that

campaign, operators must be prepared to seize upon a vulnerability in the rare moment it appears. USCYBERCOM proved with Operation Glowing Symphony (see Part 4: Evaluating U.S. Cyber Strategy) that vetting an immediate opportunity through a staid bureaucracy that does not understand how cyber works is a recipe for losing the moment. Luckily, the United States, Australia, and other allies were operating against the Islamic State of Iraq and Syria (ISIS), a relatively unsophisticated cyber adversary, and could test out new structures for coordination and deconfliction at their own pace. A better model would be to flip the risk calculus: The default answer to a proposed operation should be "yes," and a naysayer must prove it is too risky instead of asking the operators to prove the operation is safe.

The default answer to a proposed cyber operation should be yes, and a naysayer must prove it is too risky instead of asking the operators to prove the operation is safe.

- **Collaborate early.** Cyber, in its relative newness, often gets relegated to a last-minute add-on to an operational plan instead of playing an integrated role in a larger campaign. This approach can allow cyber activity to contribute somewhat, but only on the margins. Instead, **planners should incorporate cyber operators into early-stage planning, particularly for contingency planning against a peer competitor. If developed early enough, cyber tools can distract and weaken an adversary, serving as a force multiplier for military and diplomatic action.** Any operation plan must consider the role of cyber tools in step one. Being ready to capitalize on lucky opportunities takes months of research, planning, and prepositioning. If cyber tools are to be available in moments of acute need, operators need lead time to plan.
- **Adjust planning.** Military planners should release the presumption that cyber mission planning is just like other planning. As one cyber operator put it, "Rigidly following the Joint Publication 5-0 sequence in planning cyber operations is often problematic. Far too often, the resulting cyber plans and orders have represented a triumph of doctrine over reality."[7] Policymakers should unleash cyber operators to plan and engage. Similarly, the military must train for cyber conflict. **Warfighters need to get comfortable with using cyber alongside other tools and acknowledge that some capabilities may disappear due to a cyberattack from adversaries.** Wargames to train fighters should include both offensive and defensive cyber campaigns. A key feature should be the loss of GPS and secure communications, and some games may also include cyberattacks on critical infrastructure in the homeland, designed to distract the United States from the larger fight.

2. Redefining Proportionality and Escalation

As an established global superpower, the United States' default approach to a foreign policy crisis is to stop escalation and return to the status quo. In the cyber domain, that approach has resulted in

a frog-in-the-pot conundrum. Adversaries have slowly and consistently pushed at U.S. boundaries, never committing an act severe enough to provoke a punishing response. Instead, the proportional response generally is far less damaging to the aggressor than the attack is to the United States. For example, mass intellectual property theft from U.S. businesses has led to legal indictments of Chinese nationals, but the intellectual property is still lost, as are millions of dollars in research and development. Sure, those operators can no longer travel to the United States to vacation at Disney World, but that punishment is minor compared to the victim's shuttered business.

Over time, each attack has slowly raised the tolerance threshold, creating a permissive environment for subsequent attacks. Cyberattacks were viewed first as an annoyance, then as a greater annoyance, then as an expensive annoyance, and most recently as an annoyance that has resulted in adversaries having persistent access to U.S. critical infrastructure that could be used to distract and delay the United States in the case of war.[8] But none of these offenses alone has prompted a response serious enough to restore a modicum of deterrence.

Policymakers have collectively de facto decided that a proportional response to any one hack would be too insignificant—or, conversely, too unpalatable—to undertake. For example, the United States is unlikely to steal the data of millions of Chinese citizens to retaliate for the Anthem data breach. Not only is it against U.S. values, but it also would be a relatively worthless response given the lack of privacy in the Chinese system. The U.S. government is similarly unlikely to request that a bunch of cyber criminals operating on U.S. territory harass Russian businesses in a tit for tat. But the effects of these attacks are cumulative: Years of unfettered aggression from Russian cyber criminals with at least the tacit approval of the state constitute, in aggregate, a huge problem.

Actors suffer no real consequences, cyber experts preach stronger defense with limited results, and the frog boils.

This dynamic calls for a rethinking of the concept of proportionality in the cyber domain. Policymakers' view of proportionality must take into account the aggregate costs, long-term consequences, and message sent by doing nothing. The United States needs to abandon the idea that it should only respond in the cyber domain. Instead, Washington should embrace a strategy of deterrence by punishment and be willing to take action in and outside the cyber domain.

The United States has a wide variety of tools to shape a foreign actor's risk calculus, but policymakers have hesitated to use them against cyber aggression. Criminal charges are often pursued, despite their fecklessness. Economic sanctions against individual actors or, in rare cases, hacking groups send a message but have little impact. Policymakers have balked at the logical next step: holding a state responsible for attacks conducted from its territory. As a result, actors suffer no real consequences, cyber experts preach stronger defense but produce limited results, and the frog boils. This dynamic must change. Enough is enough.

Some may claim a more aggressive retaliatory posture will be escalatory. What, then, is the alternative? A strategy of avoiding escalation has led the United States to the position of a doormat, with cyberattacks escalating in seriousness and impact, largely unopposed. Not responding has already led to escalation, though the escalation is one-sided.

RECOMMENDED ACTIONS TO REDEFINE PROPORTIONALITY AND ESCALATION

- **Create a new definition of proportionality. This new definition, which could be called "cyber first–cyber optional," must begin with explicit principles.** The United States should explicitly state that all tools of statecraft are available for retaliation at any time. Cyberattacks may be met with cyberattacks but also with naming-and-shaming efforts, arrests, hefty economic sanctions, and exposure of corrupt government practices to a domestic audience inside a nation's firewall. Further, military action is on the table: If a cyber actor targets civilians or imperils civilian life, a military response should be a clear option.
- **Signal the change.** This shift to a far more aggressive retaliatory posture must be accompanied by explicit signaling of the change**. The United States must warn that it will not be walked over any longer in the cyber domain and that attacks will be met with far-harsher responses.** Adversaries will test that new stated resolve, and Washington must be ready to retaliate and signal seriousness.
- **Target China's "five poisons."** In response to China's violations of U.S. cyberspace, the United States could target the country's "five poisons"—a term used by the Chinese Ministry of Public Security (MPS) to describe what it perceives as the greatest threats to China's internal security and sovereignty.[9] These include democracy advocates, Taiwan, Tibetans, Uyghurs, and Falun Gong—a domestic spiritual movement that the Chinese government perceives as a threat.[10] **This new framework of proportionality would allow for volleys such as the United States releasing detailed satellite photos of Uyghur prison camps in response to Beijing penetrating power grids in California.**[11] More attacks would result in a public welcoming of Uyghur leaders and other Chinese dissidents to the State Department. The U.S. government could also designate Chinese diplomats personae non gratae, ask the surgeon general to make a speech at the United Nations about terrible food safety in China, or ask the secretary of health and human services to give a speech about rising cancer rates due to atrocious environmental quality in China. The United States could threaten to build an international coalition to reopen the investigation into the origins of Covid-19 and demand access to the Wuhan Institute of Virology. All these actions would hit Chinese pain points the way Chinese cyberattacks hit U.S. pain points. U.S. policymakers just need to think outside of the box.

Statement of Policy: A New Doctrine for a New Domain

To communicate these new rules to adversaries, the United States should create a statement of policy that clearly lays out a cyber doctrine. Much as the Monroe Doctrine defined U.S. interests in the Western Hemisphere and the Truman Doctrine defined U.S. support for anyone against the Soviet Union, a cyber doctrine would declare U.S. policy in this modern battlefield. The statement of policy should be bold and clear, and it should contain the following points:

- The United States, as of today, is redefining proportionality in the cyber domain. The country is bolstering defense, and part of that strong defense is a message to any who would attack the United States using cyber tools: In the future, the United States will judge attacks based on the damage done and the overall pattern of behavior, not any one attack in isolation.
- Further, the United States will be far more aggressive in responding to attacks that imperil critical infrastructure or core economic and national security interests.
- Any attack that threatens the health and safety of civilians will be met with severe consequences. Attacks that cause casualties will be met with force.
- An attack on U.S. Department of Defense (DOD) systems causing an interruption to operations will be viewed as a hostile act and may be considered an act of war.
- The United States may also choose to retaliate for attacks on U.S.-based businesses, whether the attacker is a criminal group or state actor, using the full scope of state power.
- Espionage efforts will be found and exposed, and the United States will feel free to retaliate.
- Adversaries who have assumed they can act with impunity in the cyber domain should be on notice. The cyber domain is no longer a new arena where bad actors can experiment with limited consequences. The world economy and the health and well-being of its people depend on the reliable functioning of this domain. The United States is prepared to defend it.

3. Deterrence Across Domains: Bringing Cyber into Existing Structures of Deterrence

While deterrence is well established as a fundamental principle of hard-power foreign policy, the consensus is that deterrence in the cyber domain is impossible. That conclusion stems from a rigid view of proportionality: The United States will always lose in a retaliation game that allows only cyber for cyber. The consequences the United States is willing to impose in this narrow domain are

unlikely to raise costs on an adversary enough to deter by punishment, and U.S. defenses are far too weak to deter by denial.

RECOMMENDED ACTIONS TO ESTABLISH DETERRENCE ACROSS DOMAINS

- **Define norms, even if they will be ignored**. The United States should pursue an international agreement that clearly declares that human casualties from cyberattacks must be treated as if they were casualties from a direct kinetic attack. Further, actions resulting in a loss of data are clearly less severe than actions resulting in loss of life; actions that result in property damage could fall on either side of data loss, depending on the data. These norms of behavior should be clearly stated, even if the United States assumes adversaries will still conduct cyberattacks, because they establish a clear baseline to facilitate future action. A coalition of states should sign an "enough is enough" pact, vowing to treat cyberattacks not as weather events or petty crimes but as threats to economic stability and international peace.
- **Demonstrate will.** Demonstrated will is critical to deterrence. A threat is hollow if the adversary has little confidence the threat will materialize. Previous "red lines" that turned out to be nonexistent have hampered U.S. credibility, perhaps disastrously.[12] **A demonstration of will in the form of a strong response to the first cyberattack after an explicit policy goes into place will help set a new tone.** The new definition of proportionality, described above, will be a critical element of successfully establishing deterrence.

4. Attribution: Get Comfortable with Being Uncomfortable

Cyberattacks are usually designed to be deniable, or at least to obfuscate their origin. By nature, the cyber domain is shadowy and deniable. Criminal actors provide cover for state activity, and infrastructure is relatively fluid and disposable. A rented internet protocol (IP) address is far less traceable than a cruise missile.

In tension with that ambiguity, the U.S. Intelligence Community (IC) takes its responsibility to be accurate deeply seriously. Backing up assessments with strong evidence is a core principle of the IC and how it operates. As a result, the IC has been extremely reluctant to lean far forward on attributing cyberattacks. That reluctance puts policymakers in a position where private cybersecurity organizations have attributed an attack in public statements but the IC, under its methodology, is not certain enough to make a high-confidence assessment.[13] Further, the IC may never be certain; it cannot necessarily promise that more information will be forthcoming in a week, or two, or ten.

No one likes making consequential decisions with incomplete information, but it is necessary in the cyber domain. If a principals committee decides wrongly, the result could range from heightened tensions to open conflict. But the consequences of deciding nothing could be equally impactful over the long term. Policymakers' inaction has already led to economic losses, diminished public trust in information and government, and a critical infrastructure system that is highly vulnerable.

Thus, there may be moments when it is necessary, even prudent, to act before definitive attribution. Establishing consequences for malign actors is a worthwhile goal, and the benefits of sending a strong message of response could outweigh the risks of misattribution. Policymakers can borrow a concept from Amazon here: There are one-way doors and two-way doors. Once you walk through a one-way door, you cannot go back. But a two-way door allows a reversal. Weak attribution but a necessity to act suggests finding the policy equivalent of a two-way door, or a course of action that sends a strong message but has reversible consequences. That could include, for example, sanctions, public censure, travel bans, or asset seizures.

Sometime, perhaps soon, policymakers will be faced with the need to act without high confidence. CSIS wargames conducted for this study created this conundrum for players. Facts pointed to a particular cyber actor but left some room for uncertainty, leading participants to hotly debate whether they knew enough to retaliate against an actor. The ensuing confusion hampered a policy response. (For more on the wargames, see Part 6: Testing U.S. Policy Responses to Destructive Cyberattacks with Wargames.)

RECOMMENDED ACTIONS ON ATTRIBUTION

- **Understand the complexities of attribution.** Policymakers must revisit what counts as enough certainty to act in the cyber domain. **The IC should not necessarily change its methodology for attribution, but policymakers need to understand it, including its rigor.** In particular, policymakers should understand what the IC's standards are for low-, moderate-, and high-confidence assessments and understand the difference between the methodology for such an assessment in the cyber domain versus any other area. Put differently, a cabinet secretary accustomed to reading IC assessments about leadership dynamics in Iran should not assume that the standards of certainty are identical for a political assessment and for attribution of a cyberattack.

Policymakers need to stop viewing a fig leaf as a stop sign.

- **Plan action in the face of uncertainty.** Policymakers need to stop viewing a fig leaf as a stop sign. Instead, **the United States needs to create a set of policy options for responding to nonlethal attacks that causes pain and shows resolve but is largely reversible in the low-probability scenario that the United States wrongly attributes an attack.** This is a challenging needle to thread, and the range of options will fall largely in the economic realm. Frozen assets, travel bans, and hefty fines come to mind. But if a cyberattack is lethal, as modeled in the CSIS wargames for this project, policymakers cannot wait for additional information before responding, lest the United States lose any credibility for protecting itself. Policymakers will need to get comfortable with the discomfort of uncertainty.

5. Reimagine the Warriors

Cyber war has a new cast of warriors. They likely do not have high-and-tight flattops or excellent marksmanship; they are far more likely to choose energy drinks over protein shakes. They are also not necessarily government employees, or if they are, it might be for one weekend a month and two weeks a year, when they come in for reserve duty.

Cyber war is largely fought on private networks with combatants who do not wear uniforms, and the U.S. government needs to adjust to that reality. The hand-to-hand fighting of the past is now done through keyboards, and the glory comes through a paycheck from Microsoft, Google, Mandiant, CrowdStrike, Palo Alto Networks, or any number of companies that employ a small cyber army to secure their networks. These companies are global, with de facto intelligence-gathering capabilities to match. While there is plenty of precedent for the U.S. military to rely on contractors for military support, like providing base security or life support services, fully incorporating private individuals as equal partners—or even more advanced ones—is a mindset shift.[14] The U.S. government should work to fold in this talent and make reserve military service fit with a profitable private sector career.

Further, cyber capabilities are far from the top priority for each service, meaning each is paying short shrift to cyber training. Rather than consolidate cyber talent into a single service, cyber officers may spend up to 18 months studying operations and strategy in, say, land operations but less than six weeks studying cyber operations.[15] This is how a soldier might pursue a side hobby, not how one establishes a core competency.

RECOMMENDED ACTIONS TO REIMAGINE THE WARRIORS

- **Create a Cyber Force. The cyber domain needs its own service—a Cyber Force that can be fit for purpose and constructed to incorporate this new brand of warrior.** It should tilt heavily toward reserve service, and its physical requirements should be utterly different from those of the Marines, for example. This force should be responsible for creating a steady flow of cyber talent through active-duty servicemembers and, in particular, assembling a strong reserve cadre. This talent should staff USCYBERCOM and fill other joint needs. The force would provide a pathway to advancement for ambitious cyber warriors with leadership capability, and it would allow recruitment standards that are significantly different from those required by other services. Experts in the field could organize training, and the emphasis could be on retention through a reserve service, as industry will surely lure away many of these troops.
- **Eliminate the dual hat**. The head of NSA is also the commander of USCYBERCOM. Making one person the heads of both organizations was originally meant to create efficiencies and establish a single arbiter of any conflicts arising between the two, be it in turf or operational priorities.[16] When USCYBERCOM was new and small and drawing many of its capabilities from the NSA's infrastructure, the dual hat made sense. However, creating a balance between military and intelligence activities has been a continuing irritant. It is time for an amicable divorce, to allow each element to grow and engage in this fight. **Having one boss at the**

head of both 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. (See Appendix I for more.)

- **Embrace a real role for the private sector**. The United States must view private sector partners as real partners. **It should put in place protections for cyber operators who act in conjunction with the U.S. government,** as so many from the private sector did in Ukraine. Further, it should coordinate closely with companies that can serve as nongovernmental assets for international allies, almost as a letter of marque would allow private citizens to engage in conflict on the high seas.[17] Finally, the United States must sit side by side with corporate partners on defense of the U.S. homeland in the cyber domain, as discussed in the next section.

6. The No-Fail Mission: Defense

Champion Formula 1 (F1) racer Mario Andretti famously explained that the brakes on an F1 car are not there to slow the car down but to allow it to go faster.[18] Similarly, a stronger cyber defense at home is the key to an unleashed U.S. offense. As long as policymakers worry that the home front is vulnerable to adversary attacks, they will hesitate to retaliate.

Imagine that Moscow or one of its cyber minions infiltrates an oil pipeline, as in the Colonial Pipeline incident of 2021, and the United States retaliates by conducting a noisy, meant-to-be-discovered penetration into Rosneft, the huge quasi-Russian-owned oil company. While the attack does no damage, it sends a clear message that the United States could retaliate by temporarily crippling Rosneft. Russia might do something far outside the bounds of expected proportionality and respond by shutting down power grids in Dallas, Los Angeles, and Philadelphia. In such a case, the United States would be highly unlikely to retaliate with a similar move for two reasons: First, from a moral standpoint, that kind of attack harms civilians more than governments. Second, the risk that Russia will again retaliate by picking 5 or 10 more grids to shut down would be front of mind for policymakers. Russia dominates this escalation ladder as U.S. defenses falter.

In contrast to China's great firewall, Iran's National Information Network, and Russia's intensive censorship and defense regime, the United States has a decentralized approach to cyber defense. Every U.S. entity is largely responsible for its own defense and recovery, be it a mom-and-pop grocery store, a multinational firm, or a local power plant. Even at the federal level, most agencies must supply their own cybersecurity services. As long as these entities believe they are not a target for adversaries, they have incentives to prioritize other activities, like lowering prices for customers or providing additional services. It is only when the threat becomes real that entities prioritize defense and resilience. As a result, the United States has a highly vulnerable patchwork of defense haves and have-nots.

The Biden administration began an important shift, putting the onus on software developers to make new products secure by design.[19] Much as cars are expected to meet safety requirements and

food must meet safety standards, so too should software be built safely. Products should not be rushed to market with the expectation that companies can deliver now and patch later. One stark example came early in the Covid-19 pandemic, when hackers started Zoom-bombing—dropping into Zoom calls uninvited and leaving pornography or hate speech behind.[20] Zoom welcomed crowd-sourced reporting and rushed solutions, but better advance testing that considered the actions of adversaries and mischief-makers might have averted the problem.

Software producers must assume malintent by some actors and test thoroughly. But even if the results of those tests are solid, producers should still game out the worst-case scenario. Failures will happen. Both software producers and consumers should focus on resilience—in particular, creating a rapid recovery plan. Ukraine has demonstrated that it is necessary to assume defenses will fail and focus on resilience. Russian hackers have been persistently aggressive against multiple tiers of Ukrainian infrastructure, from power to media to satellite communications to command and control. Yet Ukraine has largely bounced back with little downtime, thanks to a decade or more of working toward resilience and the efforts of Ukrainian and private sector cyber fighters. Systems failed, but they came right back, with little impactful interruption.

RECOMMENDED ACTIONS TO BOLSTER DEFENSE

- **Give the Cybersecurity and Infrastructure Security Agency (CISA) more robust power.** On the defensive front, CISA needs leverage beyond its convening and cajoling efforts. Departments and agencies must be held accountable for their investments—or lack thereof—in cyber defense. CISA has been successful in large part because the agency has been seen as helpful and nonthreatening. But mere encouragement only goes so far: Some government and private sector entities are blissfully—or more likely willfully—ignorant that they are targets and that a cyberattack could affect far more than their bottom line**. In extreme cases, CISA should have the capability to send an intervention team to take over cyber defense efforts at departments and agencies that fail two cybersecurity audits in a row.** The intervention team would have the authority to make purchasing decisions, hire and fire personnel, renew or end contracts, and make all other decisions relevant to managing cybersecurity efforts.
- **Demand faster progress inside the federal government.** 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 limited resources should go to core mission functions. However, the threat is not theoretical, and no mission will be accomplished if organizations are laid bare to attack. **Department heads should be held accountable for low cybersecurity scores, including with removal in extreme situations. But earlier measures should include leadership bonuses for strong scores and, conversely, a requirement that the heads of the lowest-scoring agencies brief the president and Congress on how they are addressing an agency's shortfalls.**
- **Strengthen Secure by Design.** The U.S. government has made the Secure by Design program largely voluntary, but defense is too urgent and important to maintain that approach**. The U.S. government should announce that Secure by Design is mandatory**

and that, after a grace period of two years, software products must display a security label similar to the red-yellow-green traffic light system the United Kingdom uses to describe the health risks of food products. In the two-year grace period, the U.S. government should create grading standards and a system of inspectors. At the end of five years, if software does not include the label, the producer is liable for security flaws. Naysayers will contend that a new inspection regime is expensive and bureaucratically fraught. For comparison's sake, the entire food safety budget of the Food and Drug Administration (FDA) for FY 2024 was $133 million, which included food chain continuity efforts and cosmetics safety.[21] The National Transportation Safety Board, with 400 employees, had a budget of $145 million.[22] The Cyber Safety Review Board, by contrast, has five employees, 20 standing members, and an operating budget of $2.8 million.[23]

- **Learn to create fail-safes.** CISA should create online resources that give small, medium, and large entities a set of tabletop exercises to drill failure. These exercises would prompt entities to identify their top three most critical functions, show how different types of information technology (IT) collapses would affect those functions, and provide instructions to drill a recovery plan. Collapses might include a ransomware attack that locks data, disconnection from the internet, or a hostile actor with administrative privileges**. The resources could include a flexible framework that serves as a starting point for entities to anticipate failure and could include where to turn for more help within CISA or at a Federal Bureau of Investigation field office.**
- **Develop Uber for cyber.** Part of the friction preventing smaller entities from setting up effective defense is the feeling of entering a maze of indistinguishable promises and incomprehensible sales pitches from cybersecurity companies. To make the ecosystem more navigable, **CISA could create an Uber-style compatibility service, where companies fill out a questionnaire about their setup and exposure and CISA's app recommends which security processes should be the highest priority.** Smart cyber companies will learn to reflect those recommendations clearly and simply on their websites and can submit bids on the app for contracts, much as Uber drivers post their availability and the services they are willing to offer.
- **Introduce multifactor authentication (MFA) in middle school.** Many school systems gave Chromebooks to every student after the Covid-19 pandemic began**.**[24] **The U.S. government could partner with Google to establish an MFA training program through which the students using Chromebooks would use MFA once a week to log on to their accounts.** The email sending the code could include a cybersecurity tip. This approach would train children to expect MFA and more broadly strengthen cybersecurity awareness across society.
- **Reach older Americans through morning shows**. CISA could ask CNN, Fox News, and network morning shows like *The Today Show* to feature a CISA cyber tip of the week. AARP already sends cyber mailings to educate older Americans; it could sponsor or cohost the segment.[25]

- **Develop a Cyber for America program.** Just as Teach for America brings college graduates and professionals into classrooms for two years, a Cyber for America program could repay student loans for those recently certified in cybersecurity in exchange for two years of supporting school districts, local critical infrastructure like water systems, or local governments.
- **Enhance National Guard resources**. In many states, the National Guard is a powerhouse of cyber talent, but other states are still building their capacity. These resources can bridge the gap between the federal and local levels, not only sharing threat information but also providing on-the-ground expertise and assistance. As some units, like the Maryland National Guard's 169th Cyber Protection Team, are replete with cyber talent, states should set up partnerships or exchanges.[26] For example, Maryland and Vermont could team up, with the former providing cyber training and the latter providing cold-weather expeditionary training. California and Alabama could swap cyber training for explosives training.

***

These programs will help bolster domestic cybersecurity over the medium term, but the threat is present today. The following sections, which assume the United States' resilience posture remains largely as it is today, will help policymakers think through the risks and retaliation options for a cyberattack, starting with a series of questions to establish the seriousness of an attack.

Decisionmaking in a Crisis

Questions, Answers, and Uncertainty

Policymakers faced with the challenge of responding to a large cyberattack should start by answering seven questions. These will illuminate aggravating circumstances and suggest a set of responses that establish escalation dominance and create deterrence.

1. **How much damage is there?**
   Was there loss of information, property damage, or risk to health and life, or were there casualties? What was the scope of the loss? For highly aggressive attacks, what was the threat to health or life? Was it localized or widespread? Was it foreseeable? In other words, should the adversary have known a successful attack would likely hurt people?
2. **Are there more attacks coming?**
   Is the attack an opening salvo in a string of attacks, or is it an isolated incident? While the latter allows for time and calibration, the former suggests leaning far forward on both the severity of the response and the speed of the reaction, which may also suggest operating with less than total confidence on attribution.
3. **Do Americans need reassurance?**
   Some attacks are more widespread and more public than others. If the attack causes fear–for example, Americans begin to doubt the safety of U.S. critical infrastructure or election security–that suggests need for a stronger, faster response, combined with robust and consistent public communication about the risk.
4. **How certain is the attribution?**
   Obvious attribution makes quick, definitive action easier. But as discussed above, action

without definitive attribution may become necessary, even wise. 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, or at least the sponsor of the behavior? Is that evidence likely forthcoming, and if not, how can authorities act before they have it?

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? Why? Accelerating aggression is a clear sign that the actors in question believe they can push the boundaries with impunity. No more frogs in pots—a tough response will say enough is enough. If the actor is new or the attack consists of espionage following a series of prepositioning hacks for operational preparation of the environment (OPE), a lesser response is acceptable.[27]
6. **Did the intent of the attack match the outcome of the attack?**
   Cyber tools can cause unintended consequences. An exploit meant to cause limited damage to an unoccupied building could accidentally kill a worker. There are already examples of ransomware attacks on hospitals that likely harmed people, including a lawsuit about an infant who died after suffering brain damage at a hospital dealing with a ransomware attack.[28] Conversely, an attack designed to be destructive can fail. Policymakers should retaliate in alignment with the intent, where possible to discern.
7. **What was the target?**
   Whereas an adversary attack on a government target requires a relatively straightforward calculus, attacks on business targets are more complicated. While the United States views the public and private sectors as separate, adversaries do not; business interests and state interests in Russia, China, and Iran are closely intertwined.

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. But that tipping point is hard to define. Some factors that could provoke U.S. government involvement might include repeated, costly attacks from one origin point, especially over time and increasing in severity; attacks causing massive economic loss, on the scale of hundreds of millions of dollars; or a disruptive or destructive attack on a company that provides critical infrastructure, defense, or intelligence infrastructure.

The answers to each of these seven questions should inform the severity of the U.S. response to an attack. For sample answers to hypothetical attacks, see Table 1 on page 22.

Options

Running the Playbook

Table 1 uses real-world examples to illustrate the seven questions and how the answers to them might suggest a more aggressive or less aggressive response to a cyberattack. An attack that returns mostly "yes" answers points to the need for a stronger response; one that returns all "yes" answers points to a strong, speedy retaliation, even in the face of uncertainty.

Table 1: The Cyber Playbook

Damage	More Coming?	Public Reassurance Needed?	Confident Attribution?	Pattern of Behavior?	Intent Matches Outcome?	Intended Target	Suggested Response
Espionage (e.g., Chinese hack of U.S. Treasury Department in 2023)	✓	✗	✓	✓	✓	Government	• Continue spy vs. spy espionage operations. • Strengthen defenses and make a public statement highlighting that the intrusion was discovered and disrupted. • Share indications of compromise widely.
Disruption to infra-structure (e.g., Colonial Pipeline)*	✓	✓	✗	✓	✓	Infrastructure	• Take legal action against suspected criminal network. • Deploy economic sanctions against state hosting criminal group. • Use offensive cyber to recover any ransom payments. • Deploy offensive cyber information operations against host government.
Disruption to government operations or services (e.g., Iranian attack on Albania)	✓	✓	✓	✓	✓	Government	• Call on allies to pool resources for rebuilding and for a cyber counterattack. • Enact alliance-wide sanctions on the aggressor. • Leverage information operations to embarrass government actors who ordered the attack. • Use offensive cyber to blow a hole in censorship firewall.
Property damage against businesses (e.g., Sands casino attack)	?	✓	✓	✓	✓	Business	If the attack was conducted by a criminal group, default to criminal prosecution and push for extradition. A military response is necessary if property damage is extensive, particularly if attacks targeted U.S. government or critical infrastructure.
National-level economic harm (akin to "Blue Screen of Death" Day, but intentional)	?	✓	✓	✓	✓	Infrastructure	• Enact devastating sanctions against a state actor, with allies if possible. • Disrupt shipping and supply chains via interdictions or kinetic operations.
Death of citizens	?	✓	✓**	?	✓	People	Respond with military/kinetic action.

* This attack was a huge disruption, but it was an attack on billing, not on the actual operations of the pipeline. The attacker likely didn't anticipate shutting down gas to the entire east coast. This is a key example of the intent of the attack not matching the result of the attack, oddly through no fault of the attacker.

** Patterns of previous attacks, but first instance of a casualty.

Seven Pieces, One Message

This report is the culmination of this seven-part series that examines how Russia, China, Iran, and the United States stack up in a fight in the cyber domain. These seven pieces add up to a clarion call for action: U.S. policymakers must urgently shore up national defense, establish an explicit cyber policy, and redefine core concepts like proportionality in order to win in this new era of warfare.

In brief, the project found the following:

- Russia's war against Ukraine may give a false sense of security about the risks of a cyber conflict between Moscow and the United States. Unlike Ukraine, the United States has not prioritized developing resilient systems, nor does it have the years of practice defending against Russian cyberattacks. Meanwhile, Moscow is learning from its cyber campaigns in Ukraine and has made clear its ambition to enhance its cyber capabilities using advanced technologies like artificial intelligence.
- While Russia initially led in cyber operations, China has caught up and is now the top threat to the United States. Beijing's vast resources and aggressive persistence have made it highly effective at espionage and formidable in OPE. Most concerningly, Chinese threat actor Volt Typhoon has targeted critical infrastructure, almost certainly prepositioning itself to disrupt U.S. systems and delay the U.S. military's ability to mobilize in the event of a kinetic conflict between the United States and China.

- Iran is a rising, aggressive cyber actor. Though less advanced than Russia or China, Tehran has shown a brazen willingness to target civilian critical infrastructure and is likely to pursue further destructive cyber operations. It should not be underestimated.
- The United States is among the world's most capable offensive cyber actors, but it is also self-restrained due to its strong moral and legal constraints on cyber offense and weak domestic defenses. As it stands, the United States is ill-prepared for a devastating cyberattack.

For this project, CSIS also conducted a series of wargames to evaluate how U.S. policymakers might respond to a deadly cyberattack on the homeland. Each game illustrated the likely disastrous confusion that would follow such an attack, as policymakers debate basic ideas like what qualifies as an act of war. In the midst of a crisis is not the time to grapple with new concepts; therefore, policymakers must incorporate an understanding of cyber warfare into their calculations now, before a major attack occurs.

This report gives policymakers a new way to think about how cyber operations fit into the spectrum of war, peace, and irregular warfare. It provides a cyber playbook that offers a set of ready policy options, including innovative tactics and a framework for a comprehensive response to the continual onslaught of attacks. The recommendations in this report will help policymakers create a web of deterrence that elucidates clear consequences but preserves flexibility in response.

The status quo has led to a situation in which the U.S. government is besieged, Americans' data has been pillaged, and businesses are left to fend off hostile foreign states. A dramatic change is needed in the cyber domain. It is past time that the United States becomes the fierce defender of the cyber domain it needs to be and the fierce competitor it should become.

Appendix I

The Dual Hat

The debate over the dual hat may be divided into three main parts: the potentially diverging goals of the two united groups, the tension between military and intelligence authorities, and the growing centrality of cyber warfare in conflicts of the present and future.

First, the goals of intelligence gatherers and operators at some point diverge. Intelligence agencies are meant to collect information to provide insight to policymakers. On one hand, the realm of computer network operations requires stealth, persistence, and no disruption to the adversary's operations. A military operation, on the other hand, is more likely aimed at creating effects, from a momentary disruption to physical destruction. A precursor to those effects is OPE, which is meant to create the conditions for these effects at a moment's notice.

OPE can look quite similar to intelligence—it also requires stealth and persistence, lest the vulnerability be discovered and patched before the effects occur. As a result, the same vulnerabilities can be highly valuable for both espionage and OPE. Leadership must decide which entity controls each vulnerability and access to the networks. They must also determine when the scales tip from listening and watching to causing an effect. The dual-hatted leader is useful for having one clear arbiter of these disputes, possibly preventing services from tripping over each other while pursuing the same target, as in the tangled octopus analogy. However, forcing one leader to choose gives short shrift to the neglected mission, and if one side is frequently the loser, trust and effectiveness are shaken. It may be better for the national security advisor, rather than the agency head, to be the ultimate arbiter between the spying and operational goals.

Second, this division between military and intelligence derives from the authorities under which each element operates. Intelligence authorities, known as Title 50 capabilities, include espionage. Military entities operate under Title 10.[29] This split is in some ways artificial, as the secretary of defense has sub-entities that operate under both titles. Nevertheless, Congress uses the split to chart oversight responsibilities, and clarity about authorities is one way national security law provides a check on both military and intelligence activities.[30] Muddled authorities open the possibility for abuse and simultaneously make oversight harder, which is far from ideal when an agency is operating largely in the shadows out of necessity.

Finally, when USCYBERCOM was created in 2012, cyber was largely a tool for espionage or psychological effects. While those two functions are still central to the mission, the ability of cyber activity to cause real-world damage and to feature in a war plan has become clear. Russia's battle plan for Ukraine and China's attempts to cause disruptions in the United States through the Volt Typhoon attacks starkly demonstrate how U.S. adversaries are looking at potential actions in the cyber domain. Luckily, Volt Typhoon's capabilities have not yet been deployed to great effect. Further, the Ukrainian defense has, for the most part, bested the Russian offense. However, the United States is far from Ukrainian standards of defense and resilience. Washington's complacency could cost the United States dearly. There is no room for structural weakness when this domain is growing so rapidly in importance to both the United States and its adversaries.

Appendix II

The Debate Over a Cyber Force

Congress and DOD have debated the merits of creating a separate Cyber Force, similar to the Space Force, which was created in 2019.[31] The considerations surrounding this debate are complex, but the crux of the issue is whether USCYBERCOM, as currently situated, along with each service's Cyber Force, is enough to effectively fight adversaries in the cyber domain, particularly when those adversaries have made cyber operations central to their war-fighting strategies. Long-time cyber operators point out that too little has been invested in cyber professionals under the current structure, particularly among mid-career military personnel who do operational planning. John Cobb, an Air Force offensive cyber officer, writes, "These problems often prevent or distort the alignment of tactics and strategy, leaving Cyber Command and its Cyber Mission Force incapable of achieving strategic goals."[32]

Each service is responsible for force generation, including recruitment and training. Combatant commands are responsible for force employment, or applying those troops to a mission. USCYBERCOM's model is to pull from each service's cyber forces and unite them for action in the cyber domain. Further, operational planning is split across five service headquarters rather than located in one joint headquarters. According to Cobb, this approach "makes planning parochial based on the quirks of service cultures and limits the joint force's ability to learn from successful and unsuccessful approaches to planning and operations."[33]

This model, while successfully cultivated under then-USCYBERCOM Commander General Paul Nakasone, has significant constraints on how much it can grow and develop. USCYBERCOM depends on each service to recruit and train an effective cadre of cyber professionals at a time when

each service is facing severe recruitment challenges. Not only are they competing with industry, which pays far more than military service, they are also competing with each other for the best talent. Finally, the skill set required for a cyber warrior is vastly different from that of an infantry soldier, surface warfare officer, or pilot. Services tend to recruit troops for those missions first.

Counterarguments include the bureaucratic headache, the cost of setting up a force, and the claim that each service will require its own cyber cadre, even if a Cyber Force exists, causing duplication. The first two claims are correct. But if not now, when will the United States incur these costs? Further, duplication has not stopped the Navy from having planes, even though the United States has an Air Force, or the Marines from having land vehicles, even though the United States has an Army. It is more likely that creating a Cyber Force will allow each service to focus on a smaller core mission and do it better. The services can secure their own systems, networks, and weaponry against attack and leave the offensive capabilities and big-picture defensive capabilities to a cadre of cyber professionals who joined the service to fight within their skill set. (See the section "Organization of Capabilities" in Part 5: Evaluating U.S. Cyber Strategy)

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, 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 Johns Hopkins University.

Aosheng Pusztaszeri is a research assistant with the Intelligence, National Security, and Technology (INT) Program at CSIS, where he supports research on the intersection of emerging technologies, national security, and intelligence. 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.

Endnotes

1 Martin Libicki, *Cyberspace in Peace and War* (Annapolis: Naval Institute Press, 2016), 73–74.

2 Ibid., 81.

3 Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional and Nuclear Domains: Moving beyond Effects-based Logics," *Journal of Cybersecurity* 5, no. 1 (2019): 5, https://doi.org/10.1093/cybsec/tyz007; Erica D. Lonergan and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace* (Oxford, UK: Oxford University Press, 2023), 6; and Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (Fall 2019): 11–39, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-3/Borghard.pdf.

4 Lonergan and Lonergan, *Escalation Dynamics in Cyberspace*.

5 Examples include Russian intervention in a 2016 Dutch referendum on an EU-Ukraine trade deal, the 2017 French presidential election, and the U.S. presidential elections of 2016, 2020, and 2024. Erik Brattberg and Tim Maurer, "Five European Experiences with Russian Election Interference," in *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (Washington, DC: Carnegie Endowment for International Peace, 2018), 5–28, https://carnegieendowment.org/research/2018/05/russian-election-interference-europes-counter-to-fake-news-and-cyber-attacks?lang=en. In early April 2025, Poland's government asserted that Russian and/or Belorussian actors had likely attempted to interfere with upcoming elections. The goal was "either to gain access to data or generate content using the compromised computers. Polish authorities described the cyberattack as 'quite dangerous.'" Daryna Antoniuk, "Poland's Prime Minister Says Cyberattack Targeted His Party as Election Nears," The Record, April 3, 2025, https://therecord.media/poland-prime-minister-cyber-targeted.

6 "Cybercrime," U.S. Department of State, https://www.state.gov/cybercrime.

7 John Cobb, "Cyber Campaign Plans and Other Fairy Tales," War on the Rocks, December 20, 2024, https://warontherocks.com/2024/12/cyber-campaign-plans-and-other-fairy-tales/.

8 Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: ODNI, February 2024), https://www.intelligence.senate.gov/sites/default/files/hearings/unclassified_2024_ata_report_0. pdf; and AJ Vicens, "Feds: Chinese Hacking Operations Have Been in Critical Infrastructure Networks for Five Years," CyberScoop, February 7, 2024, https://cyberscoop.com/feds-chinese-hacking-operations-havebeen-in-critical-infrastructure-networks-for-five-years/.

9 Coline Chavane and TDR team, *A Three-Beat Waltz: The Ecosystem Behind Chinese State-Sponsored Cyber Threats* (Rennes, France: Sekoia.io, November 2024), https://blog.sekoia.io/a-three-beats-waltz-the-ecosystem-behind-chinese-state-sponsored-cyber-threats/.

10 Ibid.

11 "Who Are the Uyghurs and Why Is China Being Accused of Genocide?," BBC News, May 24, 2022, https://www.bbc.com/news/world-asia-china-22278037.

12 Council on Foreign Relations, "Red Line in Syria: 2013 (Mini Simulation)," Council on Foreign Relations, accessed April 16, 2025, https://education.cfr.org/teach/mini-simulation/red-line-syria-2013.

13 Cybersecurity firms may have a financial incentive to do the opposite of the IC and lean forward on attribution. Being the first to attribute can grab headlines and perhaps market share. Well-established firms are less likely to risk their reputation on an inflated attribution statement.

14 One model is contractors operating surveillance drones for the U.S. government. They are an integral part of the effort but are not allowed to perform "inherently governmental functions."

15 Eugenia Lostri, Erica D. Lonergan, and Jen Patja, "Lawfare Daily: The Case for a U.S. Cyber Force," Lawfare, April 22, 2024, https://www.lawfaremedia.org/article/lawfare-daily-the-case-for-a-u.s.-cyber-force; and Cobb, "Cyber Campaign Plans."

16 Andrew Schoka, "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat," War on the Rocks, April 3, 2019, https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.

17 For more, see CSIS's No Front Lines project.

18 Duncan Milne, "The Brakes Aren't There to Slow Us Down – What Can Legal and Compliance Programs Learn from the Fastest Sports Teams on the Planet?," The Compliance and Ethics Blog, January 31, 2022, https://complianceandethics.org/the-brakes-arent-there-to-slow-us-down/.

19 Joseph R. Biden Jr., "Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity," The White House, January 16, 2025, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/.

20 Khristopher J. Brooks, "Zoom Says It Will Fix Security Holes That Video Hackers Have Exploited," CBS News, April 3, 2020, https://www.cbsnews.com/news/zoom-video-conferencing-feature-freeze-security-flaws/.

21 U.S. Food and Drug Administration (FDA), *FY 2024 FDA Budget Summary* (Washington, DC: FDA, n.d.), 1, https://www.fda.gov/media/166050/download.

22 National Transportation Safety Board, "NTSB Statement on the President's Fiscal Year 2024 Budget," press release, March 14, 2023, https://www.ntsb.gov/news/press-releases/Pages/NR20230314.aspx.

23 "DHS creates Cyber Safety Review Board to review significant cybersecurity incidents," CSO Online, February 4, 2022, https://www.csoonline.com/article/572001/dhs-announces-the-creation-of-the-cyber-safety-review-board.html; and U.S. Department of Homeland Security, *Cyber Safety Review Board Charter* (Washington, DC: DHS, September 2021), 5, https://www.cisa.gov/sites/default/files/2023-04/cyber_safety_review_board_charter_508_compliant_8.pdf.

24 Benjamin Herold, "Schools Handed Out Millions of Digital Devices Under COVID-19. Now, Thousands Are Missing," *Education Week*, July 23, 2020, https://www.edweek.org/technology/schools-handed-out-millions-of-digital-devices-under-covid-19-now-thousands-are-missing/2020/07.

25 Helena M. Mentis and Nora McDonald, "Older Americans Are Given the Wrong Idea About Online Safety – Here's How to Help Them Help Themselves," *UMBC Magazine*, March 24, 2022, https://umbc.edu/stories/older-americans-are-given-the-wrong-idea-about-online-safety-heres-how-to-help-them-help-themselves/.

26 Sarah McClanahan, "169th Cyber Protection Team Is Capable and Ready," National Guard News, November 7, 2019, https://www.nationalguard.mil/News/Article-View/Article/2009731/169th-cyber-protection-team-is-capable-and-ready/; and Benjamin Hughes, "Maryland Air National Guard Begins Divesting A-10s," National Guard News, March 27, 2025, https://www.nationalguard.mil/News/Article-View/Article/4136645/maryland-air-national-guard-begins-divesting-a-10s/.

27 According to Title 10 of the U.S. Code, Operational Preparation of the Environment (OPE) refers to "the conduct of activities in likely or potential operational areas to set conditions for mission execution." *United States Code*, Title 10, § 127f (2023)(Expenditure of funds for clandestine activities that support operational preparation of the environment and non-conventional assisted recovery capabilities). See https://www.law.cornell.edu/uscode/text/10/127f#j.

28 Kevin Collier, "Baby Died Because of Ransomware Attack on Hospital, Suit Says," NBC News, September 30, 2021, https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465.

29 *United States Code*, Title 10, § 113 (2023); and United States Code, Title 50 (War and National Defense), (2023).

30 Michael E. DeVine, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Definitions*, CRS Report R45175 (Washington, DC: Congressional Research Service, November 2022), https://crsreports.congress.gov/product/pdf/R/R45175.

31 Erica Lonergan and Mark Montgomery, *United States Cyber Force: A Defense Imperative* (Washington, DC: FDD Press, March 2024), https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf.

32 Cobb, "Cyber Campaign Plans."

33 Ibid.

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**