

# U.S. Cyber Policy: *Offense, Deterrence, & Strategic Competition*

Recalibrating Our Approach

POLICY BRIEF



```
elif operation == "MIRROR_Y":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = True  
    mirror_mod.use_z = False  
elif operation == "MIRROR_Z":  
    mirror_mod.use_x = False  
    mirror_mod.use_y = False  
    mirror_mod.use_z = True  
  
#selection at the end -add back the deselected mirror modifier object  
mirror_ob.select= 1  
modifier_ob.select=1  
bpy.context.scene.objects.active = modifier_ob  
print("Selected" + str(modifier_ob)) # modifier ob is the active ob  
    mirror_ob.select = 0  
None = bpy.context.selected_objects[0]  
bpy.data.objects[None.name].select = 0  
  
print(f"Please select exactly one object, the last one gets selected")  
  
#selection at the end -add back the deselected mirror modifier object  
mirror_ob.select= 1  
modifier_ob.select=1  
bpy.context.scene.objects.active = modifier_ob  
print("Selected" + str(modifier_ob)) # modifier ob is the active ob  
    mirror_ob.select = 0  
None = bpy.context.selected_objects[0]  
bpy.data.objects[None.name].select = 0  
  
print(f"Please select exactly one object, the last one gets selected")
```

# **Task Force** on National Security & Law Enforcement

## Co-Chairs

### **Thomas P. Bossert**

President and Co-Founder  
Trinity Cyber

Former Assistant to the President for  
Homeland Security

### **Frank J. Cilluffo**

Director, McCrary Institute for Cyber  
and Critical Infrastructure Security

### **Hon. Chris Inglis**

Former National Cyber Director

### **Gen. Kenneth F. McKenzie, Jr., U.S. Marine Corps (Ret.)**

Executive Director  
Global and National Security Institute

Executive Director  
Cyber Florida

## Task Force Director

Kyle Klein

## Members

George Barnes

Ben Bass

Dave Bowdich

Stephen Boyd

Cheri Caddy

Christopher Cleary

Mike D'Ambrosio

Victoria Dillon

Ernest Ferraresso

Preston Golson

Matt Hayden

Suzanne Heckenberg

Rob Joyce

Cynthia Kaiser

Brian Keeter

Steve Kelly

Matthew Kempf

Alison King

Dave Luber

Daniel Kroese

Mark Montgomery

Chris Porter

Nicholas Sellers

Joshua Stiefel



*This report is published in partnership with The Florida Center for Cybersecurity at the University of South Florida (Cyber Florida at USF), a state-funded organization advancing Florida's leadership in cybersecurity through education, workforce development, applied research, and public-private collaboration.*

# Contents

Foreword	05
Executive Summary	08
Introduction	11
Evolution of U.S. Cyber Policy	14
The Rise of U.S. Offensive Cyber Doctrine	22
The Future of Cyber Deterrence	27
Organizational & Policy Challenges Ahead	33
Conclusion	36

*While the Task Force reached broad areas of agreement, individual members should not be understood to endorse every finding or recommendation in this report.*



## EXPLORE MORE WITH THE **CYBER FOCUS** PODCAST

**Cyber Focus**, from the McCrory Institute, explores the people and ideas that shape and protect our digital world. **Each week our host, Frank Cilluffo, speaks with the leading voices in cybersecurity**, and brings to light what steps public and private organizations need to be taking to keep our country secure.



# 1

## Foreword

U.S. cyber policy has evolved incrementally, leaving legal and organizational frameworks misaligned with a domain defined by persistent competition and continuous engagement. This paper examines how challenges among authorities, institutions, and doctrine constrain strategic advantage and identifies where reform is increasingly necessary.

# Foreword

“...effective preeminent cyber dominance depends not only on technical proficiency, but on the **alignment of strategy, law, policy, and organizational design.**”



Cyberspace has become a central arena of strategic competition, though the policies and structures governing U.S. cyber operations remain of limited effectiveness in addressing the challenges of today. Even though U.S. policy has evolved over time, the evolution has been largely incremental and reactive, proving to be insufficient for the current cyber domain. While the United States retains significant technical capabilities, it continues to operate within legal and organizational frameworks that were not fully designed for continuous engagement, pre-positioned access, or competition below the threshold of armed conflict. This gap increasingly constrains strategic coherence and timely decision-making.

This paper examines the evolution of U.S. offensive cyber policy with a focus on the authorities, institutions, and doctrines that shape national cyber operations. It proceeds from the premise that effective preeminent cyber dominance depends not only on technical proficiency, but on the alignment of strategy, law, policy, and organizational design. Over the past two decades, U.S. cyber policy has developed incrementally, often in response to adversary behavior, rather than through deliberate strategy, leaving unresolved tensions between military and intelligence missions, such as those between Title 10 and Title 50 authorities, and enduring questions about force structure and institutional maturity.

As peer competitors integrate cyber operations into long-term strategic planning, the operational environment has shifted toward persistent access, pre-crisis positioning, and blended campaigns that combine espionage, coercion, and disruption. In such an environment, a strategy focused primarily on defense and resilience, and commercial solutions overly reliant on detective controls, while necessary, cannot induce changes in adversary behavior on its own. The United States cannot simply defend its way out of a problem defined by adversaries that enjoy initiative, sanctuary, and asymmetric advantages in cyberspace.

Credible, offensive cyber capability is, therefore, not about unchecked disruption or escalation. It is about restoring strategic balance by denying adversaries free access, imposing uncertainty into their operational and planning calculus, and reinforcing deterrence by demonstrating that persistent intrusions and pre-positioning on our lifeline sectors will carry consequences.

The purpose of this analysis is not to advocate unfettered cyber offense nor a purely defensive posture, but to clarify the tradeoffs embedded in current policy choices and to identify areas where reform is increasingly necessary. By assessing the development of offensive cyber doctrine, the dual-hat relationship between NSA and U.S. Cyber Command, and proposals such as a standalone Cyber Force, this paper aims to inform a more disciplined and forward-looking policy debate. Further, this piece is intended as a scene-setting, context-providing paper ahead of further work by the task force to offer more specific recommendations for improved cyber offensive policy and structural reform.

In a domain characterized by speed, ambiguity, and persistent engagement, inaction and incrementalism are themselves strategic choices. Cyberspace is no longer peripheral to national security. It is a foundational domain of competition that will shape deterrence, crisis stability, and alliance credibility in the years ahead. The choices made now regarding authorities, organization, and doctrine will determine whether the United States can sustain strategic advantage in a domain defined by persistent campaigns and enduring competition.

During the course of its work, the Task Force engaged with a wide range of current and former officials and leaders working at the forefront of cyber policy and national security, and is especially grateful for the expertise shared by Lt. Gen. Kevin B. Kennedy, U.S. Air Force (Ret.), Maj. Gen. Ryan P. Heritage, U.S. Marine Corps (Ret.), and Dr. Michael Sulmeyer.

**Thomas P. Bossert**

President and Co-Founder  
Trinity Cyber

Former Assistant to the President for Homeland Security

**Frank J. Cilluffo**

Director  
McCrary Institute for Cyber and Critical Infrastructure Security

**Hon. Chris Inglis**

Former National Cyber Director

**Gen. Kenneth F. McKenzie, Jr., U.S. Marine Corps (Ret.)**

Executive Director  
Global and National Security Institute,

Executive Director  
Cyber Florida



# 2 Executive Summary

U.S. cyber policy remains misaligned with a domain defined by persistent competition and continuous engagement, leaving the nation reactive rather than strategic.

# Executive *Summary*

Today, the United States faces a cyber threat landscape that is shifting faster than relevant policy frameworks intended to address it. The United States remains structurally and doctrinally misaligned for strategic competition in cyberspace, complicating pre-crisis decision-making and coordination across military, intelligence, and law enforcement authorities. Washington has struggled to define and implement a coherent approach to offensive cyber operations and cyber deterrence, particularly as adversaries expand their capabilities, embed disruptive access within critical infrastructure, and exploit legal inadequacies. Offensive cyber policy has evolved in a piecemeal fashion and would benefit from deliberate reform, particularly in the authorities and processes that govern pre-crisis operations. What began in the early 2000s as an intelligence-driven model centered on clandestine collection has evolved into a contested operational environment where cyber effects are now entwined with traditional military planning, strategic competition, and crisis signaling. The United States must now navigate this space using authorities that were not designed for the scale or tempo of today's threats, while relying on an organizational structure that reflects institutional strength, as well as operational and policy challenges.

Over the last decade, adversaries such as Russia, China, Iran, and North Korea have steadily expanded the scope and ambition of their cyber operations. China has demonstrated the clearest long-term strategic intent. Its campaigns against U.S. critical infrastructure, government agencies, and private-sector networks underscore Beijing's preference for persistent access that can be weaponized during a future geopolitical crisis.<sup>1</sup> Russia has also used cyber operations to support military campaigns, most notably in Ukraine, where destructive malware and grid attacks accompanied conventional assaults. These developments indicate that adversaries increasingly treat cyberspace as a battlespace that is continuously in play, one where access, disruption, and coercion are cultivated in advance rather than activated only at the moment of conflict.

Against this backdrop, the United States has undergone a notable shift in cyber operational policy. For years, offensive cyber activity was tightly controlled, often requiring extensive interagency deliberation and White House approval. This changed with National Security Presidential Memorandum 13 (NSPM-13) in 2018, which allows the President to delegate greater operational decision-making to specific organizations, most notably U.S. Cyber Command, and the concurrent codification in the National Defense Strategy of the concept of "defend forward," that is, the policy that the United States must seek to operate continuously in foreign networks to disrupt adversary campaigns before they reach U.S. targets. Although effective in some operational respects, NSPM-13 also reignited debates around oversight, intelligence equities, Title 10–Title 50 boundaries, and the strategic risks of persistent engagement.<sup>2</sup>

The dual-hat relationship between the NSA and U.S. Cyber Command remains a central element of

---


<sup>1</sup> "Typhoon in the Fifth Domain: China's Evolving Cyber Strategy," September 3, 2025, Cyfirma, accessed November 17, 2025, < <https://www.cyfirma.com/blogs/typhoon-in-the-fifth-domain-chinas-evolving-cyber-strategy/> >.

<sup>2</sup> Pomerleau, Mark, "Are DoD's Rules of Engagement in Cyber Space too Limited?" June 27, 2025, Defense Scoop, accessed November 17, 2025, < <https://defensescoop.com/2025/06/27/dod-cyberspace-rules-of-engagement-limitations/> >.



this policy environment. While it creates unparalleled synergy between intelligence collection and operational capability, it also introduces friction regarding mission prioritization, resource sufficiency, and the degree to which intelligence-driven stealth or military-driven effects should take priority. There also exist questions about organizational maturity, service-like authorities, force structure, and the future of integration with the Intelligence Community (IC).<sup>3</sup> In addition, there appears to be a growing misalignment of mission between the NSA, which is a national asset, and the Department of War (DoW), which has a narrower mission.

To address these challenges, the United States will need to strengthen its doctrinal, legal, and organizational foundations. This includes modernizing statutory authorities, clarifying interagency roles, improving resilience across critical infrastructure, creating agility in our forces, establishing clear roles and attendant relationships between private and public sector personnel, and refining deterrence frameworks that account for adversaries who blend espionage, coercion, and pre-positioning activity. Most importantly, U.S. cyber policy must shift from reactive, episodic action to a durable posture capable of operating effectively in an era of continuous foreign intrusion. The stakes are significant. As adversaries deepen their access into American networks, the United States must decide whether its cyber strategy will remain bound by outdated assumptions or evolve in ways that reflect the realities of twenty-first-century conflict.



"Most importantly, **U.S. cyber policy must shift from reactive, episodic action to a durable posture capable of operating effectively** in an era of continuous foreign intrusion. **The stakes are significant.**"

<sup>3</sup> Roza, David, "Does the U.S. Military Need a Cyber Force?" October 27, 2025, Task and Purpose, accessed November 15, 2025, < <https://taskand-purpose.com/tech-tactics/us-military-cyber-force/>>.



# 3

## Introduction

U.S. cyber dominance is challenged as adversaries adapt faster than the policies, authorities, and organizational structures governing American cyber operations.

# Introduction

In recent years, the United States has been forced to confront a rapidly evolving cyber environment shaped by accelerating foreign threats, expanding digital attack surfaces, and an increasing reliance on interconnected systems across both civilian and military domains, as well as both general-purpose information technology systems (IT) and functionally bespoke operational technology (OT). While the United States once dominated the cyber domain, due to unmatched intelligence capabilities and the early development of offensive cyber tools, its strategic advantage has waned as adversaries have grown more agile, capable, and assertive. The U.S. Government has struggled to align its organizational structures, legal authorities, and operational norms with the pace and nature of modern cyber conflict.

The emergence of U.S. Cyber Command in 2010 marked the first major attempt to consolidate military cyber capability under a unified structure. From the outset, Cyber Command was intertwined with the National Security Agency, sharing leadership under a dual-hat commander and drawing heavily on NSA's unparalleled signals intelligence (SIGINT) infrastructure, as well as personnel, tradecraft, execution of close collaboration on operational activities. This relationship provided immediate operational benefits, enabling rapid capability development and access to global collection systems. But it also raised structural questions that remain unresolved today, including how to balance intelligence equities with operational effects, how to manage divergent missions under one roof, or whether the dual-hat structure should be split. One perspective is that Cyber Command has not yet reached the maturity or stability required for such a transition, and that separation from NSA could degrade capability rather than strengthen it. Recent NDAA language directed the Department of Defense to conduct analysis related to this question, without mandating a specific organizational outcome, but the debate is far from settled.<sup>4</sup> The statutorily required analysis found “substantial benefits that present compelling evidence for retaining the existing structure,” according to 2023 testimony before the Senate Armed Services Panel by then-Director of the National Security Agency, Gen. Paul Nakasone.<sup>5</sup>

For much of the early 2000s and 2010s, offensive cyber operations were tightly controlled through Presidential Policy Directive-20 (PPD-20), which mandated extensive interagency coordination and White House approval. Critics argued that these processes were too slow and risk-averse to counter fast-moving threats. That assessment prompted the first Trump administration to replace PPD-20 with NSPM-13 in 2018, delegating greater operational authority to the Department of Defense and enabling Cyber Command to conduct foreign operations under Title 10 authorities with less direct White House oversight.<sup>6</sup> The adoption of “persistent engagement” and “defend forward” altered

---

<sup>4</sup> Demchak, Chris, “Five Reasons Not to Split Cyber Command from NSA Anytime Soon—If Ever,” March 5, 2021, War on the Rocks, accessed November 15, 2025, <https://warontherocks.com/2021/03/five-reasons-not-to-split-cyber-command-from-the-nsa-any-time-soon-if-ever/>.

<sup>5</sup> Matishak, Martin, “One Leader for Cyber Command, NSA, has ‘Substantial Benefits,’ Report Says,” March 7, 2023, The Record, accessed December 16, 2025, <<https://therecord.media/nakasone-cybercom-nsa-dual-hat-dunford-report>>.

<sup>6</sup> Borghard, Erica, “What Do the Trump Administration’s Changes to PPD-20 Mean for U.S. Offensive Cyber Operations,” September 10, 2018, Council on Foreign Relations, accessed November 15, 2025, <<https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations>>.



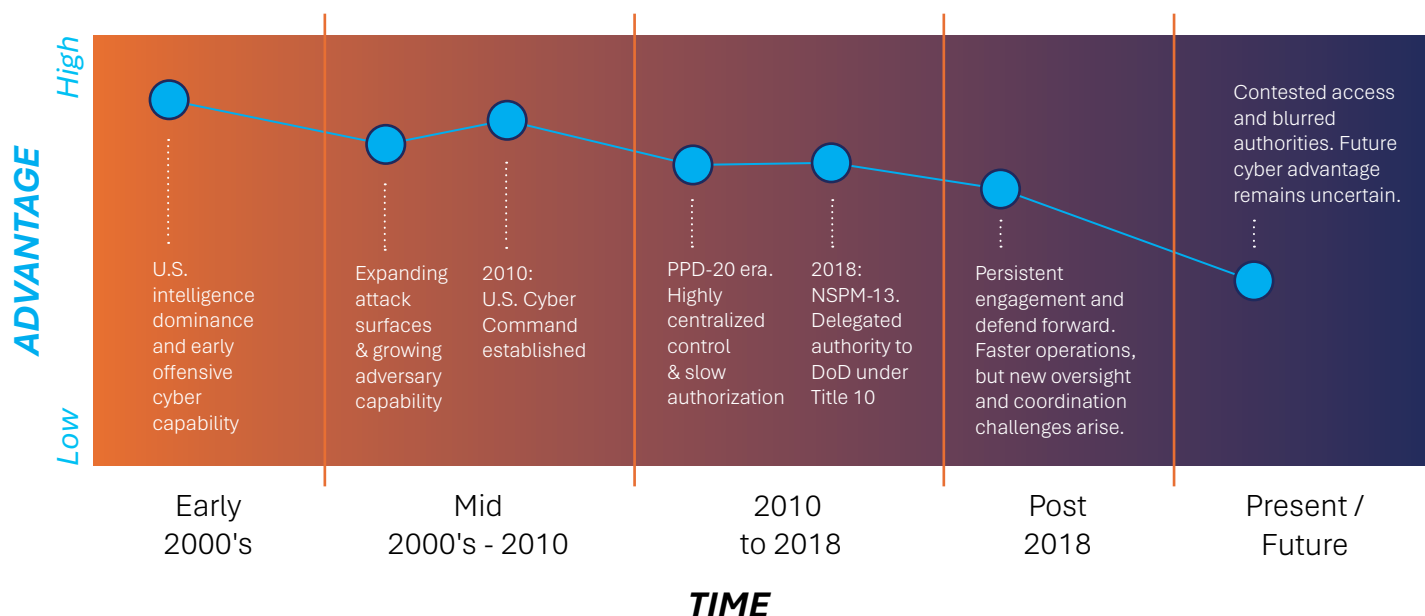
operational tempo relative to the PPD-20 approval regime, enabling more frequent pre-emptive activity but also introducing new coordination and oversight challenges.

Central to this discussion is the long-running debate over the boundary between Title 10 (military operations) and Title 50 (intelligence activities). Cyber operations often blur the line between these authorities in ways traditional national security law never anticipated. Intelligence agencies depend on long-term access for strategic insight, while military planners may prioritize disruption or effects that could compromise intelligence value. These tension points highlight the need for clearer policy frameworks that recognize cyber's unique characteristics and reconcile the competing demands of secrecy, speed, oversight, and operational impact.

Another dimension shaping U.S. cyber policy is the ongoing debate over whether the United States should establish an independent Cyber Force alongside the Army, Navy, Air Force, Marine Corps, Coast Guard, and Space Force. Proponents argue that cyberspace is now essential to modern conflict and requires its own service branch with dedicated career pipelines, acquisition authorities, and command structures.

As the United States confronts an era where adversaries increasingly view cyberspace as an active battlespace rather than a passive espionage environment, it must develop a strategy that accounts for the complexity of modern digital conflict. This requires sustained policy modernization, legal reform, and organizational adaptation. It also demands a realistic understanding of how the United States lost its early cyber advantage and what it will take to rebuild strategic leverage in an environment where access is contested, deterrence is uncertain, and adversaries are no longer deterred by traditional concepts of signaling or punishment. This paper outlines the evolution of U.S. offensive cyber policy, examines the organizational and statutory challenges that shape national cyber operations, and assesses the prospects for emerging reforms such as a standalone Cyber Force. Ultimately, the goal is to provide a clear-eyed analysis of how the United States can strengthen its posture in a domain that will increasingly shape the outcome of future geopolitical competition.

### ***U.S. Cyber Strategic Advantage Over Time***



# 4

## Evolution of ***U.S. Cyber Policy***

U.S. cyber policy has evolved into a contested operational domain, but remains constrained by legacy authorities and institutions that struggle to keep pace with modern cyber conflict.

# Evolution of *U.S. Cyber Policy*

The evolution of U.S. cyber policy reflects a prolonged effort to reconcile emerging digital threats with legacy legal authorities, command relationships, and institutional norms developed for earlier forms of conflict, particularly in authorities governing offense. In the 1990s, the United States viewed cyberspace primarily through the lens of espionage and information assurance. Early efforts such as Presidential Decision Directive on Critical Infrastructure Protection 63 (PDD-63) in 1998 framed cyber threats as risks to critical infrastructure and largely emphasized defensive resilience.<sup>7</sup> The United States' offensive advantage was not yet contested. Few adversaries had the capability to challenge American networks at scale, and the broader policy conversation remained firmly rooted in surveillance, not conflict.

A 1997 exercise, known as Eligible Receiver 97, including the National Security Agency (which acted as the red team), Central Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation, National Reconnaissance Office, Defense Information Systems Agency, Department of State, Department of Justice, as well as critical civilian infrastructure providers such as power and communication companies simulated cyberattacks on DoD and related U.S. critical infrastructure and directly resulted in a significant sense of urgency to address observed shortfalls in the defensibility of those systems and the lack of a credible U.S. deterrent.<sup>8</sup>

The Department of Defense<sup>9</sup> soon developed an operational approach to securing its information systems, creating in 1998 the Joint Task Force-Computer Network Defense (JTF-CND), which operated in conjunction with the Defense Information Systems Agency (DISA). JTF-CND evolved into Joint Task Force – Computer Network Operations (JTF-CNO) by the end of 1999, working under U.S. Space Command (USSPACECOM). When USSPACECOM was dissolved in October 2002, JTF-CNO joined USSTRATCOM.<sup>10</sup>

The Joint Chiefs of Staff in their 2004 National Military Strategy declared cyberspace a “domain” of conflict alongside the air, land, sea, and space domains, and noted DoD must maintain its ability to defend against and to engage enemy actors in this new domain. That same year, Secretary of Defense Donald Rumsfeld divided JTF-CNO into defensive and offensive components: Joint Task Force – Global Network Operations (JTF-GNO), responsible for defense; and Joint Functional Component Command – Network Warfare (JFCC-NW) for offensive cyberspace operations

---

<sup>7</sup> “Presidential Decision Directive 63 on Critical Infrastructure Protection: Sector Coordinators,” August 5, 1998, the National Telecommunications and Information Administration, accessed November 15, 2025, < <https://www.federalregister.gov/documents/1998/08/05/98-20865/presidential-decision-directive-63-on-critical-infrastructure-protection-sector-coordinators> >.

<sup>8</sup> “Our History,” U.S. Cyber Command, accessed December 13, 2025, < <https://www.cybercom.mil/About/History/> >.

<sup>9</sup> For the purposes of this paper, the term Department of Defense is used in reference to historical or statutory citations and the term Department of War is used when the reference is present day.

<sup>10</sup> Ibid.



planning.<sup>11</sup> Taken together, this began laying the groundwork for new iterations in cyber policy.

The post-9/11 era marked a turning point. As counterterrorism dominated national security priorities, the government expanded its use of intelligence-driven cyber operations to disrupt terrorist communications and financial networks. These activities highlighted the potential for cyber tools to serve operational purposes beyond traditional collection. However, offensive cyber operations during this period were tightly compartmented and rarely coordinated across agencies. A 2010 Government Accountability Office (GAO) report examining cyber warfare doctrine gaps within DoD observed that “hybrid warfare might be used informally to describe the ever-changing complexity and dynamics of the battlefield, but the department has not officially defined the term and has no plans to do so, claiming existing doctrine on traditional and irregular warfare is sufficient to describe the current and future operational environment.”<sup>12</sup>

In 2008, a malware-infected USB drive was inserted into a U.S. Army laptop in Afghanistan, leading to the infection of both classified and unclassified networks belonging to U.S. Central Command. In response, Operation Buckshot Yankee was launched to mitigate the attack and develop a way forward to address the cyber challenges the incursion underscored.<sup>13</sup> The creation of U.S. Cyber Command in 2010 represented a watershed moment. As the first unified military entity dedicated to cyberspace, Cyber Command was designed to centralize disparate service-level capabilities and build a coherent operational framework. But its establishment also underscored ongoing uncertainty about how cyber operations fit within the broader spectrum of military force. The command was initially subordinated to U.S. Strategic Command and relied almost entirely on the NSA for technical infrastructure, workforce, and operational reach. In practice, much early Cyber Command activity was essentially NSA-led, further blurring the line between military operations and intelligence collection and establishing a dubious presumption that NSA’s collection architecture (based primarily on targeting global commercial telecommunications systems) could simultaneously serve the needs of U.S. Cyber Command.

This period also coincided with significant foreign cyber aggression. Chinese cyber espionage surged throughout the 2010s, including the 2015 breach of the Office of Personnel Management (OPM) that compromised the personal records of more than 22 million Americans.<sup>14</sup> Russia’s 2014 and 2016 cyber operations against Ukraine demonstrated the use of cyber tools to shape military campaigns, while its information operations exposed Washington’s vulnerabilities to leaks of hacked materials.<sup>15</sup> Iran and North Korea conducted destructive attacks on U.S. companies, including the 2012 Shamoon attack on Saudi Aramco and the 2014 hack of Sony Pictures.<sup>16</sup>

---

<sup>11</sup> Ibid.

<sup>12</sup> Aitoro, Jill R., “Defense Lacks Doctrine to Guide it Through Cyberwarfare,” September 13, 2010, NextGov, accessed November 15, 2025, < <https://www.nextgov.com/digital-government/2010/09/defense-lacks-doctrine-to-guide-it-through-cyberwarfare/47575/> .

<sup>13</sup> Lyons, Jessica, “‘Four Horsemen of Cyber’ Look Back on 2008 DoD IT Breach that Led to US Cyber Command,” May 10, 2024, The Register, accessed December 8, 2025, < [https://www.theregister.com/2024/05/10/dod\\_usb\\_attack/](https://www.theregister.com/2024/05/10/dod_usb_attack/) .

<sup>14</sup> “22 Million Affected by OPM Hack, Officials Say,” July 9, 2015, ABC News, accessed November 15, 2025, < <https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731> > .

<sup>15</sup> Chinchardze, Ketevan, “From Georgia to Ukraine: Seventeen Years of Russian Cyber Capabilities at War,” July 30, 2025, Modern War Institute at West Point, accessed November 15, 2025, < <https://mwi.westpoint.edu/from-georgia-to-ukraine-seventeen-years-of-russian-cyber-capabilities-at-war/> .

<sup>16</sup> Lee, Timothy B. and Emily St. James, “The 2014 Sony Hacks, Explained,” June 3, 2015, Vox, accessed November 15, 2025, < <https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea> > .

Even after the creation of U.S. Cyber Command in 2010, US policy makers took a decidedly conservative approach to the employment of its capabilities with Secretary of Defense Chuck Hagel going so far in a 28 March 2014 speech to state that the U.S. "does not seek to 'militarize' cyberspace" and that the Department of Defense was building a modern Cyber Force to deter aggression and defend the nation from attacks, rather than becoming a primary offensive force.

These intrusions forced U.S. policymakers to confront the sobering reality that adversaries were no longer confined to espionage. They were preparing for strategic disruption, influence, and coercive leverage. In response, the Obama administration issued Presidential Policy Directive 20 (PPD-20) in 2012, establishing an interagency process for the approval of cyber operations that could have significant diplomatic or operational implications. While PPD-20 sought to impose order, critics argued that it imposed such procedural complexity that operations took months to approve.<sup>17</sup>

More importantly, subsequent to Secretary Hagel's 2014 declaration that the U.S. would exercise restraint in the employment of US Cyber Command, the actions of North Korea and Russia in the 2017 WannaCry and NotPetya attacks respectively gave notice to the U.S. that the policy of restraint could paradoxically encourage, if not feed, escalation by nation-states lacking a policy of restraint. The DoD's 2018 Defense Science Board Study "Cyber as a Strategic Capability" made note of this possibility and further stated that while the U.S. led the world in many domains, it lagged in cyber, with adversaries effectively using cyber for strategic effects, threatening infrastructure and prosperity. The report urged the U.S. to develop its own strategic cyber power, emphasizing integration with other national power instruments (diplomacy, economy) for deterrence and achieving strategic goals, recognizing cyber as crucial for modern warfare and national security. Key takeaways involved countering adversarial cyber operations, strengthening defenses for critical infrastructure, and treating cyber as a core, integrated military capability, not just a technical function.

By the late 2010s, these criticisms led to a policy shift. In 2018, the Trump administration rescinded PPD-20 and replaced it with National Security Presidential Memorandum 13 (NSPM-13), which allowed the President to grant greater authority to the Secretary of Defense and U.S. Cyber Command to conduct operations without requiring extensive White House approval. NSPM-13 (later amended during the Biden administration with NSPM-21) was further enabled by the declaration in the National Defense Authorization Act of 2019 that cyber operations conducted by the US military constituted "traditional military operation[s]," and was wholly aligned with the National Security Strategy and Cyber Command's emerging doctrine of "persistent engagement" and "defend forward," which held that the United States must counter adversary operations inside foreign networks before they reach U.S. systems.<sup>18</sup> For the first time, U.S. cyber policy embraced a posture of proactive, continuous operations. But this operational freedom also raised new questions: how to avoid escalation, how to preserve intelligence access, and how to manage operations that straddle Title 10 and Title 50 authorities.

In parallel with military authorities is the role of federal law enforcement, which consistently

---

<sup>17</sup> Bing, Chris, "Trump Administration May Throw Out the Approval Process for Cyber Warfare," May 2, 2018, CyberScoop, accessed November 17, 2025, < <https://cyberscoop.com/ppd-20-white-house-national-security-council-cyber-warfare-tactics/>>.

<sup>18</sup> U.S. Cyber Command Public Affairs Office, "Cyber 101: Defend Forward and Persistent Engagement," October 25, 2022, U.S. Cyber Command, accessed November 17, 2025, < <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/>>.

conducts operations that meaningfully shape the digital battlespace. The Department of Justice has increasingly used amended Rule 41 search and seizure authorities to access, disrupt, or remove malware from compromised systems inside the United States, as seen in botnet takedowns and cryptocurrency seizures tied to ransomware groups.<sup>19</sup> These court-approved operations function as a lawful form of disruption that imposes direct costs on foreign adversaries. Abroad, NSA can rely on authorities delegated by Executive Order 12333 and Title 50, whereas U.S. Cyber Command directly leverages Title 10 authorities to target hostile infrastructure, gather intelligence, or preempt malicious campaigns before they threaten U.S. networks. This offers U.S. Cyber Command a key benefit in the dual-hat arrangement of being able to leverage Title 10 authorities in the combatant commander role but also benefit from the Title 50 authorities, as delegated by the Director of the National Security Agency. In combination, these authorities have shifted disruption left of impact, in which law enforcement, intelligence agencies, and Cyber Command all participate in shaping the threat environment rather than responding after the fact.

Today, the United States continues to navigate this complex landscape. The accelerating tempo of adversary activity demonstrates that cyber policy can no longer be treated as a mere technical issue. It is a strategic domain central to national defense, and its evolution reflects the broader challenge of adapting twentieth-century institutions to the demands of twenty-first-century competition.

### ***The Four Tension Forces***



<sup>19</sup> Iftimie, Alex, "No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims," April 19, 2021, Lawfare, accessed December 9, 2025, < <https://www.lawfaremedia.org/article/no-server-left-behind-justice-departments-novel-law-enforcement-operation-protect-victims#:~:text=Over%20the%20years%2C%20the%20Justice,where%20a%20computer%20is%20located.>>



# The NSA – U.S. Cyber Command

## ***Dual-Hat Structure***

The dual-hat relationship between the NSA and U.S. Cyber Command is one of the most distinctive and debated organizational features of the U.S. cyber enterprise. From the moment Cyber Command was established, the Department of Defense recognized that building offensive and defensive cyber capability from scratch would take years. NSA, by contrast, possessed unmatched SIGINT infrastructure, analytic expertise, global access, and operational tradecraft. The solution was to place both organizations under a single leader, the Director of NSA, who would also serve as the Commander of Cyber Command.

This arrangement created immediate advantages. NSA's vast technical resources enabled Cyber Command to develop operational capabilities rapidly, and shared leadership ensured consistent alignment between intelligence collection and operational planning. In practice, early Cyber Command teams relied almost entirely on NSA infrastructure, including foreign accesses, hardware implants, analytic tools, and mission platforms.

Yet the dual-hat has always carried inherent tension, coinciding with the stated benefits. NSA is fundamentally an intelligence agency, operating under Title 50 authorities that require secrecy, long-term access, and protection of sources and methods. U.S. Cyber Command is a military entity governed by Title 10 authorities, which prioritize operational impact, effects, and mission execution. These missions can conflict. Intelligence agencies may wish to preserve an access for years to support global collection, while military planners may prefer to disrupt or degrade an adversary network during a crisis or campaign. Additionally, NSA has people with years and even decades of experience, whereas the bulk of the military personnel are rotating frequently.

The 2017 National Defense Authorization Act included provisions outlining the conditions under which the dual-hat could be severed, though successive administrations have refrained from making the change.<sup>20</sup> Subsequent NDAA's have further applied additional criteria required should a separation occur and have restricted the use of funding to prohibited limiting the authorities of Cyber Command.<sup>21</sup> Supporters of maintaining the dual-hat argue that the integration between NSA and Cyber Command is a national advantage, giving the United States a level of intelligence-operational synergy unmatched by adversaries. Critics counter that the arrangement creates structural conflict and risks giving one individual too much influence over both intelligence and military operations.

The debate has intensified as the United States considers the possibility of a future Cyber Force. In the event of a split of the dual-hat structure, there would exist a greater need for an independent Cyber Force. Yet even critics acknowledge that separating the two organizations prematurely could degrade capability and slow operational tempo. Until the United States resolves the future of its cyber

---

<sup>20</sup> Chesney, Robert, "Ending the 'Dual-Hat' Arrangement for NSA and Cyber Command?" December 20, 2020, Lawfare, < <https://www.lawfaremedia.org/article/ending-dual-hat-arrangement-nsa-and-cyber-command>>.

<sup>21</sup> "National Defense Authorization Act for Fiscal Year 2026," Section. 1508, House Armed Services Committee, accessed December 18, 2025, < [https://armedservices.house.gov/uploadedfiles/rcp\\_text\\_of\\_house\\_amendment\\_to\\_s.\\_1071.pdf](https://armedservices.house.gov/uploadedfiles/rcp_text_of_house_amendment_to_s._1071.pdf)>.

organizational structure, the dual-hat arrangement will remain both a strategic asset and a potential source of friction, not to mention a very real and relevant case study of the nature of intelligence secrecy and military action that lies at the heart of American cyber policy.

## ***Title 10 vs. Title 50: A Structural Tension at the Core of Cyber Policy***

Few issues illustrate the complexity of U.S. cyber policy more clearly than the persistent tension between Title 10 military authorities and Title 50 intelligence authorities. These statutes were never designed with cyberspace in mind, and their boundaries, once clear in traditional domains, blur significantly when applied to digital operations. As a result, U.S. agencies have been forced to interpret and apply legal frameworks that predate the internet to activities that defy conventional categorization.<sup>22</sup>

Title 10 governs the activities of the armed forces, providing the statutory basis for military operations, including offensive cyber operations conducted by U.S. Cyber Command. Title 50 governs intelligence activities, including clandestine collection and covert action. Traditionally, the distinction between the two domains hinged on visibility and intent. Military operations were overt and aimed at achieving physical or strategic effects, whereas intelligence activities were clandestine and aimed at acquiring information. Some of America's closest allies, the United Kingdom and Australia, have explicitly granted cyber offensive authorities to their primary cyber agencies—a potential policy solution worthy of consideration by the United States.

In cyberspace, these distinctions are far less intuitive. An operation to establish persistent access within an adversary network may look identical at the technical level, whether conducted for intelligence collection or preparatory military action. Moreover, the same exploit chain used to exfiltrate data could also enable disruptive effects if activated. The Intelligence Community prefers long-term persistence, stealth, and integrity of access. The military may require rapid disruption or temporary degradation to support a broader campaign. This divergence can place Title 10 and Title 50 missions in direct conflict.

The structural debate with the adoption of NSPM-13, which allowed the President to push significant and sustained offensive operational authority under Title 10 into the hands of Combatant Commanders. This shift gave Cyber Command flexibility but also increased the risk that Title 10 operations could inadvertently compromise intelligence programs, escalate tensions, or trigger diplomatic consequences. It also shifted attention away from difficult choices related to whether and how the U.S. should seek to achieve parity with our near peer adversaries who are using cyber means to achieve their broader steadily expanding strategic ambitions beyond traditional military objectives. The challenge is that U.S. law does not clearly define when a cyber operation transitions

---

<sup>22</sup> DeVine, Michael E., "Covert Actions and Clandestine Activities of the Intelligence Community: Selected Definitions," November 29, 2022, Congressional Research Service, access November 17, 2025, < <https://www.congress.gov/crs-product/R45175>>.

from intelligence activity to a military operation or vice versa. Nor does it provide consistent guidance for situations in which both authorities apply simultaneously. Concurrently, U.S. Cyber Command also conducts a number of intelligence-related activities in cyberspace.

In recent years, policymakers and scholars have called for statutory reform. Yet despite years of debate, Congress has not enacted major legislative updates. The result is a landscape where agencies must navigate blurred authorities on a case-by-case basis, often relying on internal processes, interagency negotiation, and executive-level guidance rather than clear statutory lines.

This ambiguity is not infinitely sustainable. As adversaries deepen access to U.S. critical infrastructure and the tempo of cyber operations increases, the United States must modernize its legal framework. Without responsive unambiguous authorities, Washington risks inefficiency, operational conflict, and, in a crisis, delayed response. More importantly, ambiguous authorities undermine deterrence, signaling uncertainty to adversaries at a moment when clarity and resolve are essential.

# Title 10

## Military Operations

Conducted by the Department of War as overt or covert military activities.

Prioritizes operational effects, disruption, and battlefield advantage.

Optimized for speed, tempo, and execution.

Accepts higher risk to long-term access in exchange for operational impact.

Doctrine flows from the laws of armed conflict and traditional military command structures.

# Title 50

## Intelligence Activities

Conducted by Intelligence Community for collection, analysis, and decision advantage.

Prioritizes long-term access, persistence, and secrecy.

Optimized for strategic understanding.

Avoids actions that could compromise sources, methods, or future access.

Doctrine flows from intelligence oversight regimes emphasizing control and deniability.

# 5

## The Rise of U.S. *Offensive Cyber Doctrine*

U.S. offensive cyber policy has shifted to a more proactive model of persistent engagement, yet remains constrained by policy, organizational, and escalation risks that limit its deterrent impact.



# The Rise of U.S. ***Offensive Cyber Doctrine***

The maturation of U.S. offensive cyber policy reflects a broader shift in how the United States conceptualizes power projection in the digital domain. For much of the early cyber era, U.S. operations were shaped by intelligence culture. That is, stealthy, compartmented, and risk averse. Offensive cyber tools were used sparingly, often only in situations where physical consequences were limited or where national leadership deemed effects essential. Stuxnet, discovered publicly in 2010 but deployed years earlier, demonstrated the potential for cyber capabilities to produce strategic, real-world effects. That revelation served both as proof of concept and as a catalyst for international competitors. States recognized that if the United States could weaponize code to sabotage Iranian centrifuges, others could pursue similar tools for coercion, disruption, or destruction.<sup>23</sup>

Following the Stuxnet exposure, adversaries intensified their investments in offensive cyber capabilities, while the United States found itself caught between expanding threats and internal hesitancy about deploying its own tools, and concerns that the U.S. might violate emerging global norms like the UN GGE norms of 2015 if it did so.<sup>24</sup> By the mid-2010s, cyber operations had become an integral component of Russian and Chinese military doctrine. Russia demonstrated the operational use of cyber during its annexation of Crimea and later throughout the conflict in Ukraine, employing wiper malware, grid-targeting campaigns, and information operations in tandem with conventional forces. China's long-term approach, meanwhile, has emphasized persistent access and infrastructure infiltration that can be used for coercive leverage or pre-crisis disruption. These developments prompted U.S. policymakers to reevaluate whether traditional intelligence-based frameworks could meet emerging threats.

In response, U.S. Cyber Command began articulating a vision that diverged sharply from earlier policy constraints. This vision, often referred to as "persistent engagement," held that cyber threats could not be countered solely through episodic operations or defensive fortification. Instead, the United States needed to operate continuously in the adversary's space, shaping behavior, imposing costs, and degrading malicious infrastructure before attacks reached U.S. networks. This doctrine required faster operational decision-making, greater autonomy for Cyber Command, and a shift from reactive operations to a posture of active contestation.

The pivotal moment came in 2018, when NSPM-13 allowed delegation of greater authority to DoD, bringing U.S. policy into alignment with Cyber Command's concept of operations. In the years since,

---

<sup>23</sup> Zetter, Kim, "Zetter Details how Stuxnet Marked a Turning Point in Cyber Warfare by Enabling Physical Sabotage through Code," July 23, 2025, Industrial Cyber, accessed November 17, 2025, <<https://industrialcyber.co/industrial-cyber-attacks/zetter-details-how-stuxnet-marked-a-turning-point-in-cyberwarfare-by-enabling-physical-sabotage-through-code/>>.

<sup>24</sup> "2015 UN GGE – Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security (A/70/174), July 2015, Digwatch, Geneva Internet Platform, accessed December 13, 2025, <<https://dig.watch/resource/un-gge-report-2015-a70174>>.

Cyber Command has conducted a broad array of missions, from disrupting Russian troll farms during the 2018 midterm elections to targeting Iranian cyber units linked to attacks on U.S. infrastructure.<sup>25</sup> These operations underscored that offensive cyber capabilities now function as a routine, though still constrained, instrument of national power in specific operational contexts. While effective in some cases, the operational tempo also introduced new risks, including inadvertent intelligence exposure and the potential for escalation with adversaries.

Another element of the evolution in the United States' offensive cyber posture has been the increasingly active role of law enforcement. In 2024 the Department of Justice dismantled a botnet linked to the PRC's Volt Typhoon actor by accessing compromised routers, removing the malware, and cutting off Chinese operators' command channels.<sup>26</sup> This followed the FBI's 2022 operation to delete Russian GRU-linked Cyclops Blink malware from infected devices.<sup>27</sup> These actions, paired with federal cryptocurrency seizures against state-linked ransomware groups, demonstrate how law enforcement now uses domestic legal tools to impose operational costs on foreign cyber actors. NSA and U.S. Cyber Command authorities provide a complement to domestic Rule 41 actions and forming a layered disruption strategy that mirrors the broader shift toward proactive engagement. Offensive doctrine today sits in a complex middle ground: more proactive than intelligence-era paradigms, more restrained than some of our closest allies, and still bound by an evolving mix of statutory, policy, and organizational constraints. Whether this balance can deter adversaries who increasingly prepare for conflict in cyberspace remains an open question.

## Persistent Engagement & ***the “Defend Forward” Approach***

Persistent engagement is the foundation of modern U.S. cyber operations. Developed by U.S. Cyber Command and popularized by its former commander, Gen. Paul Nakasone, the doctrine reflects a belief that cyber defense cannot succeed at the boundary of U.S. networks alone.<sup>28</sup> Adversaries operate continuously, probing for vulnerabilities, pre-positioning malware, and refining tactics. “Defend forward” is the operational expression of this doctrine. It authorizes U.S. forces to take action and aims to disrupt campaigns before they threaten U.S. systems. This may involve seizing adversary servers overseas, dismantling malware infrastructure, or conducting precision operations that temporarily disable foreign cyber units. Supporters argue that defend forward has prevented attacks that could have had strategic consequences. For example, Cyber Command operations

---

<sup>25</sup> Kube, Courtney and Ken Dilanian, “Trump Approved Operations that Disabled Russian Troll Farm during 2018 Midterms,” February 26, 2019, NBC News, accessed November 17, 2025 < <https://www.nbcnews.com/politics/national-security/trump-approved-operation-disabled-russian-troll-farm-during-2018-midterms-n976381>>.

<sup>26</sup> “U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure,” January 31, 2024, Press Release, U.S. Department of Justice, accessed December 9, 2025, <<https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>>.

<sup>27</sup> “Justice Department Announces Court-Authorized Disruption of Botnet Controlled by Russian Federation’s Main Intelligence Directorate (GRU),” April 19, 2022, Press Release, U.S. Department of Justice, accessed December 9, 2025, < <https://www.justice.gov/archives/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation>>.

<sup>28</sup> Nakasone, Paul M., “A Cyber Force for Persistent Operations,” 1st Quarter 2019, Joint Force Quarterly 92, accessed November 17, 2025, < [https://cs.brown.edu/courses/cs180/sources/2019\\_01\\_22\\_JFQ\\_CyberRoleForPersistentOperations\\_Nakasone.pdf](https://cs.brown.edu/courses/cs180/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf)>.

reportedly disrupted Russian attempts to interfere with the 2018 and 2020 U.S. elections. Similarly, operations against Iranian groups in 2019 and 2020 reportedly limited their ability to conduct retaliatory strikes following U.S.–Iranian tensions. Importantly, these aforementioned authorities do not enable U.S. military forces to operate on U.S.-based systems owned and operated by the private sector or provide for insight into the status of U.S. private sector infrastructure even when under assault by foreign actors.

A parallel development that reinforces persistent engagement is the expanding role of U.S. law enforcement in conducting disruption operations. In 2023 the Department of Justice dismantled the long-running Qakbot botnet, using Rule 41 search and seizure authority to access compromised systems, remove the malware, and reroute the botnet’s traffic through FBI-controlled servers.<sup>29</sup> Although framed as a criminal action, the operation had broader national security impact by denying foreign actors a platform used for espionage and ransomware. These activities serve as a domestic counterpart to defend forward, demonstrating that proactive disruption now occurs across military, intelligence, and law enforcement channels rather than in DoW alone.

A similar dynamic is visible in the work of the U.S. Secret Service, which has increasingly carried out cyber disruption operations that parallel the logic of persistent engagement. In 2023, Secret Service investigators led seizures of crypto-currency culminating an investigation into fraudulent cyber actors.<sup>30</sup> Although pursued under criminal authorities, these actions effectively removed key platforms used not only by financially motivated actors but also by state-linked groups that rely on the same illicit infrastructure to obscure operational funding. The result is a form of domestic cyber disruption that complements military defend forward missions by shrinking the digital ecosystem in which adversaries operate and by denying them trusted pathways for sustaining campaigns against U.S. targets.

Even within the Department of War, there is debate over how aggressively Cyber Command should act. Some planners view persistent engagement as essential to countering Russian and Chinese campaigns that operate below the threshold of armed conflict. These concerns echo debates common in the early days of counterterror operations, where high operational tempo strained both personnel and organizational structures.

Despite this, persistent engagement remains central to U.S. cyber strategy. It reflects a pragmatic recognition that adversaries are already in U.S. networks and that a defensive posture confined to the homeland is insufficient. But its long-term sustainability remains an open and essential question for policymakers.

---

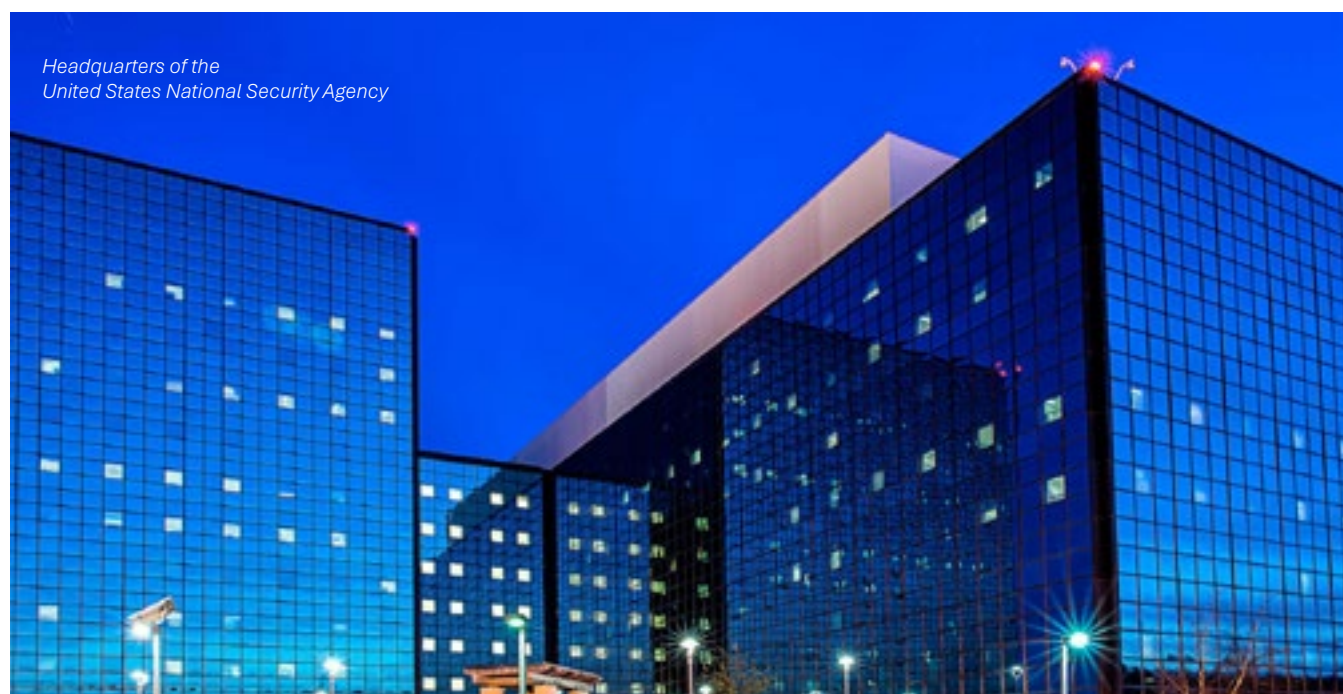
<sup>29</sup> “Qakbot Malware Disrupted in International Cyber Takedown,” August 29, 2023, Press Release, U.S. Department of Justice, accessed December 9, 2025, <<https://www.justice.gov/archives/opa/pr/qakbot-malware-disrupted-international-cyber-takedown>>.

<sup>30</sup> “Cyber Scam Organization Disrupted Through Seizure of Nearly \$9M in Crypto” November 21, 2023, Press Release, U.S. Secret Service, accessed December 9, 2025, <<https://www.secretservice.gov/newsroom/releases/2023/11/cyber-scam-organization-disrupted-through-seizure-nearly-9m-crypto#:~:text=The%20seized%20funds%20were%20traced%20to%20cryptocurrency,technique%20often%20referred%20to%20as%20%20chain%20hopping%20>>.

## The ***Five Eyes***

The United States is not alone in grappling with how to organize and employ offensive cyber capabilities, and the experience of its closest intelligence partners offers useful contrast. Among the Five Eyes, the United Kingdom has taken perhaps the most forward-leaning and publicly articulated approach. In 2016, London formally acknowledged its ability to conduct offensive cyber operations through a partnership between GCHQ and the Ministry of Defence, later codified in the establishment of the National Cyber Force (NCF) in 2020. The NCF integrates civilian intelligence and military operators under a unified command structure, allowing the United Kingdom to plan and execute offensive campaigns ranging from counterterrorism disruption to actions aimed at degrading Russian disinformation networks.<sup>31</sup>

Australia has postured the Australian Signals Directorate's (ASD) mandate to include sustained offensive cyber operations in defense of national interests, authorizing ASD to counter and disrupt foreign cyber campaigns targeting Australian infrastructure.<sup>32</sup> Australian officials have publicly acknowledged using offensive capabilities to disrupt foreign criminal organizations and hostile state-linked actors, an unusually transparent posture that reflects both political intent and a desire to deter further intrusion. Across the Five Eyes, these models differ in structure but share a common recognition: offensive cyber power is no longer an adjunct capability but a core instrument of national strategy, and each government has had to reconcile longstanding intelligence traditions with the operational demands of modern conflict.



<sup>31</sup> "National Cyber Force Transforms Country's Cyber Capabilities to Protect the UK," Press Release, November 19, 2020, National Cyber Force, GCHQ, accessed December 6, 2025, < <https://www.gchq.gov.uk/news/national-cyber-force>>.

<sup>32</sup> "Offensive Cyber," Australian Signals Directorate, accessed December 6, 2025, < <https://www.asd.gov.au/about/what-we-do/offensive-cyber>>.





# 6 The Future of *Cyber Deterrence*

Cyber deterrence requires a blended approach that integrates resilience, attribution, escalation management, and cross-domain responses.

# The Future of *Cyber Deterrence*

Deterrence in cyberspace has proven exceptionally challenging. Traditional deterrence models are built on the logic of mutually assured destruction, credible punishment, and clear attribution and do not translate cleanly to digital operations. Cyber intrusions often fall below the threshold of armed conflict, attribution can take weeks or months, and adversaries frequently use proxies or contractors to obscure their involvement.<sup>33</sup> Moreover, cyber tools are difficult to signal, because capabilities must remain secret to be effective, yet secrecy can limit deterrence messaging.

Exacerbating this reality is the low cost of entry for cyber transgressors which enables large numbers of would be cyber attackers to acquire the tools needed to achieve threshold capability. As a result, some U.S. efforts have sought to attempt deterrence by denial that increases the work factor required for transgressors to succeed rather than deterrence by punishment, which would require a comprehensive effort to attribute, find, engage, and impose consequences. This approach emphasizes hardening systems, improving resilience, reducing attack surfaces, and increasing the cost and difficulty of adversary operations. The Cybersecurity and Infrastructure Security Agency (CISA) has emphasized “shifting left” on defense through zero-trust architectures, better patch management, and faster vulnerability disclosure.<sup>34</sup> While these measures can reduce risk, denial alone cannot deter extremely capable adversaries that are capable of maintaining persistent access for strategic leverage.

An effective approach requires clear differentiation between categories of cyber activity and a disciplined framework for escalation management. At the lower end of the spectrum, espionage and intelligence preparation of the battlefield short of pre-positioning, largely focused on covert access, intelligence collection, and the establishment of persistent presence, remain a generally accepted feature of statecraft. While these activities may signal intent or create future leverage, they typically fall below the threshold that warrants overt response, instead calling for intelligence collection, defensive hardening, and quiet countermeasures.

By contrast, cyber operations that produce disruptive effects, particularly those degrading or denying essential services or prepositioning to do so in sectors such as energy, healthcare, finance, or communications, cross a meaningful threshold. Such actions justify a broader set of responses, including public attribution, law enforcement action, cyber countermeasures, sanctions, and diplomatic engagement. At the highest end of the spectrum, sustained or catastrophic cyber attacks

---

<sup>33</sup> Task Force on the People’s Republic of China, “Code Red: A Guide to Understanding China’s Sophisticated Typhoon Cyber Campaigns,” October 28, 2025, The McCrary Institute for Cyber and Critical Infrastructure Security, Auburn University, accessed November 19, 2025, < <https://mccraryinstitute.com/code-red-a-guide-to-understanding-chinas-sophisticated-typhoon-cyber-campaigns/> >

<sup>34</sup> Lord, Bob, Jack Cable, and Lauren Zabierek, “Categorically Unsafe Software,” May 13, 2024, Cybersecurity and Infrastructure Security Agency, accessed November 19, 2025, < <https://www.cisa.gov/news-events/news/categorically-unsafe-software#:~:text=Shift%20left.,of%20the%20individual%20software%20developer.>> >

against counter-value targets demand full-spectrum response options, potentially extending across cyber, economic, diplomatic, and, where legally justified, conventional military domains.

Effective deterrence and escalation control also depend on graduated attribution and aligned authorities. Technical attribution may justify classified intelligence activity and defensive measures, while operational attribution enables law enforcement action and diplomatic signaling. Strategic attribution opens the door to public attribution, which may prove beneficial in taking actions like sanctions or cyber operations under Title 10 or Title 50 authorities. Confirmed state-sponsored attacks causing significant harm will likely warrant the use cross-domain responses. In practice, deterrence is strongest when these response options are integrated with resilience and collaboration at scale. This looks like coordinated recovery exercises across critical infrastructure sectors, court-authorized public-private disruption of botnets and illicit infrastructure, real-time intelligence sharing with state and private partners, and ladder response frameworks that combine cyber, financial, diplomatic, and military tools. Together, these approaches reinforce a model of deterrence that does not rely on any single instrument, but instead seeks to shape adversary behavior through credibility, coordination, and sustained strategic pressure.

An additional element of today's deterrence conversation is whether the United States should more clearly signal its ability to hold an adversary's counter-value assets, including economic systems, political institutions, or civilian infrastructure, at risk through cyber means. Adversaries such as China and Russia already treat U.S. critical infrastructure as latent leverage in a crisis, creating an asymmetric environment in which only one side's civilian systems are vulnerable. While the United States has been cautious about discussing counter-value cyber options, even implicit acknowledgment that such capabilities exist, bounded by strict legal and policy constraints, could help restore strategic balance. The aim would not be to threaten preemptive disruption, but to ensure adversaries understand that coercive leverage is not one-sided and that attacks on American civilian targets could trigger consequences extending beyond the immediate tactical effect.

A further complication is that U.S. cyber policy must operate across multiple domains simultaneously: intelligence collection, military competition, diplomacy, and civilian infrastructure protection. And unlike other national security challenges like terrorism and kinetic warfare, the government does not have authority to engage and defeat those that hold the U.S. at risk. The vast majority of critical infrastructure upon which health, safety, economic vitality and national security depends is built, sustained and defended by the private sector. Deterrence strategies that work in one domain may be counterproductive in another. For example, exposing an adversary operation may strengthen deterrence by attribution but may compromise an intelligence collection channel or threaten a sensitive foreign partnership.

Given these complexities, the future of cyber deterrence likely lies in a blended approach. This includes improving resilience at scale, expanding public-private collaboration, strengthening intelligence sharing, and integrating cyber strategies into broader frameworks of integrated deterrence. It also requires new statutory authorities, clearer decision-making processes, and modernized organizational structures capable of sustaining long-term competition. Above all, it demands a realistic acknowledgment that deterrence in cyberspace will never mirror Cold War models.



# Prospects for a ***U.S. Cyber Force***

The idea of establishing a standalone U.S. Cyber Force has gained momentum in recent years, driven by concerns that the current organizational structure is ill-suited to long-term strategic competition in cyberspace.<sup>35</sup> The cyber domain, once considered a technical adjunct to intelligence operations, has become a decisive arena of national power. Yet its organizational home remains distributed across multiple military services and dependent on the dual-hat arrangement with the NSA.

Calls for a Cyber Force stem from several structural challenges. First, the military services have struggled to develop consistent training pipelines and career-long pathways for cyber operators. The Army, Navy, Air Force, and Marine Corps each maintain their own cyber components, but these units often compete for talent and lack uniform standards for recruitment, training, and retention. The Cyber Mission Force (CMF), established in 2014, drew personnel from multiple services, but early reports revealed significant disparities in readiness, experience, and qualification across teams.<sup>36</sup>

Second, the acquisition requirements for cyber differ substantially from those of traditional military services. Cyber capabilities often rely on rapid software development, small-scale procurements, and near-constant update cycles. Yet the Department of War acquisition system remains geared toward multiyear procurement programs for platforms such as aircraft and ships. A dedicated Cyber Force could, in theory, adopt acquisition models more suited to digital operations, similar to the rapid innovation structures used in special operations or intelligence communities.<sup>37</sup>

Third, a standalone Cyber Force would provide career progression and institutional identity for cyber operators, who currently navigate fragmented bureaucratic pathways within the services. Many cyber personnel face promotion systems designed around kinetic warfighting rather than technical mastery, leading to attrition and difficulty retaining high-skill operators.<sup>38</sup>

Establishing a Cyber Force also presents significant challenges. Extracting cyber expertise from the service stovepipes other than a prospective cyber service may reduce or remove the losing service's ability or willingness to ensure that service owned digital infrastructure is built and operated with resilience against cyber threats foremost in mind. Additionally, separation from NSA, which may or may not be warranted if the U.S. were to create a separate Cyber Force, would force the new Cyber Force to develop independent infrastructure, access pathways, and analytic capabilities. Former senior officials have cautioned that such a separation could set back U.S. capabilities by years. Congress has taken a cautious approach. The 2023 and 2024 National Defense Authorization Acts directed DoD to conduct feasibility assessments and develop potential transition plans but stopped short of mandating a new service.

---

<sup>35</sup> Loneragan, Dr. Erica and RADM (Ret.) Mark Montgomery, "Building the Future U.S. Cyber Force: What Right Looks Like," September 9, 2025, Foundation for the Defense of Democracies, accessed November 21, 2025, < <https://www.fdd.org/analysis/2025/09/09/building-the-future-us-cyber-force/>>.

<sup>36</sup> Magee, Aden, "The Sad and Sorry Tale of Cyber Command's Seven-Year Failure," September 4, 2025, War on the Rocks, accessed November 21, 2025, < <https://warontherocks.com/2025/09/the-sad-and-sorry-tale-of-cyber-commands-seven-year-failure/>>.

<sup>37</sup> Lynch, Evan, "DOD Strives to Revolutionize Cyber Acquisition," July 1, 2025, The Cyber Edge by Signal, accessed November 21, 2025, < <https://www.afcea.org/signal-media/cyber-edge/dod-strives-revolutionize-software-acquisition>>.

<sup>38</sup> Hultz, Chad, "Cybersecurity Recruitment Crisis in the Armed Forces: A Political Blind Spot," September 22, 2025, Military.com, accessed November 21, 2025, < <https://www.military.com/daily-news/opinions/cybersecurity-recruitment-crisis-armed-forces-political-blind-spot.html>>.

Despite these challenges, the momentum behind Cyber Force proposals reflects a recognition that cyber operations require an institutional foundation capable of sustaining strategic competition. As adversaries expand their own cyber forces the United States will need to consider whether its current structure can provide the organizational stability, workforce development, and operational agility demanded by the cyber domain. The debate remains unresolved, but its importance will only grow as U.S. cyber missions continue to expand.

## NSPM-13 and the ***Changing Landscape of U.S. Operational Authority***

National Security Presidential Memorandum 13 (NSPM-13), issued in 2018, fundamentally reshaped U.S. cyber operational authority by delegating greater decision-making to the Department of Defense and reducing the interagency friction that defined cyber operations for more than a decade. To understand its impact, it is necessary to contrast NSPM-13 with its predecessor, Presidential Policy Directive 20 (PPD-20). Under PPD-20, nearly all offensive cyber operations required extensive interagency coordination and often direct White House approval.<sup>39</sup> Proponents argued that this structure ensured diplomatic oversight and prevented operations that could inadvertently escalate tensions. Critics countered that the process was slow, risk-averse, and unsuited to countering agile adversaries conducting continuous cyber campaigns.

In practice, NSPM-13 narrowed the category of operations requiring White House review rather than eliminating interagency oversight altogether. This change aligned U.S. policy with Cyber Command's operational philosophy of defend forward and persistent engagement. The delegation of authority meant Cyber Command could disrupt foreign cyber units, take down malware infrastructure, and preempt adversary campaigns without navigating lengthy approval chains. Supporters argue that the policy enabled the United States to carry out critical operations during the 2018 and 2020 election cycles, contributing to the mitigation of Russian influence operations.<sup>40</sup>

Despite some concerns, NSPM-13 remains the most significant evolution in cyber operational authority to date. It reflects a policy shift that prioritizes operational agility and recognizes that adversaries are unlikely to be deterred by a slow-moving interagency process, though there remain bureaucratic and operational limitations within the interagency processes structured around this policy. At the same time, it underscores the need for updated legal frameworks and improved oversight structures capable of managing 21st-century cyber operations. Without such

---

<sup>39</sup> Pomerleau, Mark, "New Authorities Mean Lots of New Missions at Cyber Command," May 8, 2019, C4ISRNet, accessed November 21, 2025, <


<sup>40</sup> Lyngaas, Sean, "PPD-20 Successor has yielded 'Operational Success,' Federal CISO Says," April 16, 2019, CyberScoop, accessed November 21, 2025, <

modernization, the United States risks either constraining itself unnecessarily or overextending its operational reach in ways that carry unintended strategic consequences.

## Role of the ***Private Sector***

As the United States assesses the balance between offensive cyber operations and national resilience, it must also confront the indispensable role of the private sector in shaping the contours of active cyber defense. Many of the capabilities relevant to modern cyber conflict, such as threat intelligence collection, rapid incident response, and the ability to deploy deception or interdiction tools at scale, reside not within government networks but inside major technology firms, cloud providers, and critical infrastructure operators. Private entities already perform elements of active defense by hunting adversaries within their systems, deploying beacons, mitigating malicious traffic, and collaborating with federal agencies during botnet takedowns.<sup>41</sup>

Although these actions fall short of offensive operations in the traditional sense, they demonstrate how the private sector can seek to shape adversary behavior and deny operational freedom through forward-leaning measures that are lawful, risk-calibrated, and technically sophisticated. What remains unresolved is how far private actors should be permitted to go when defending their networks from state-sponsored threats, and how the government should structure oversight, liability protections, and coordination frameworks to ensure that such activity enhances national security without triggering escalation or infringing on civil liberties. As adversaries increasingly target U.S. companies to gain strategic leverage, the question is not whether the private sector will play a role in active cyber defense, but whether that role will be integrated into a coherent national strategy or continue to evolve in an ad hoc and legally ambiguous “gray zone.”



**“...denial alone cannot deter extremely capable adversaries** that are capable of maintaining persistent access for strategic leverage.”

<sup>41</sup> “Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats,” October 2016, Active Defense Task Force, Center for Cyber and Homeland Security, The George Washington University, accessed December 6, 2025, < <https://cpb-us-e2.wpmucdn.com/wordpress.auburn.edu/dist/8/7/files/2021/01/into-the-gray-zone.pdf>>.





# 7 Organizational & *Policy Challenges Ahead*

The United States faces interlocking challenges in cyber workforce, coordination, legal authorities, resilience, and international competition that demand a coherent, long-term strategy aligning policy, institutions, and operations to sustain advantage in an increasingly contested cyber domain.

# Organizational & Policy *Challenges Ahead*

As the cyber domain becomes increasingly central to geopolitical competition, the United States faces several structural and policy challenges that will shape the future of its cyber posture. These challenges span workforce development, interagency coordination, legal reform, operational doctrine, and broader questions about national cyber resilience. While none of these challenges are insurmountable, addressing them will require sustained political attention and an understanding that cyber policy cannot remain static.

One major challenge is workforce development. Cyber talent remains scarce across government and the private sector. NSA and U.S. Cyber Command compete not only with one another but with the traditional professional specialties of the U.S. military and with private-sector companies offering compensation packages for cyber and IT specific talent far beyond what government service can match. The Defense Department has attempted to mitigate this gap through scholarship programs, direct commission pathways, and specialized training pipelines, but the problem remains acute. The workforce issue is also intertwined with the potential creation of a Cyber Force, which would require thousands of trained personnel and a clear career progression model. Without addressing talent shortages, structural reforms risk the creation of new organizations that lack the personnel needed to function effectively. While the use of transformative technologies like Generative AI might make a significant contribution there is little reason to assume that it will do so in the very near term or solve the challenge of generating and sustaining deep professional expertise across careers.

An additional challenge lies in interagency coordination. Cyber operations intersect with diplomacy, intelligence collection, homeland security, and military planning. Yet each of these communities operates under different legal authorities, cultural norms, and operational priorities. The Department of Homeland Security (via CISA) is responsible for protecting civilian infrastructure, while the FBI leads domestic threat response. NSA and Cyber Command operate globally, but their roles diverge significantly. Without a more integrated approach, the United States risks gaps in response, intelligence sharing, and defensive coordination.

Moreover, there exist relevant concerns surrounding statutory modernization. Title 10 and Title 50 authorities were not written with cyberspace in mind. Policymakers continue to debate how to define cyber operations that blur traditional boundaries. Should the United States adopt a new statutory framework specifically for the cyber domain? Should covert action authorities be updated to acknowledge cyber's unique characteristics? Should Congress create clearer oversight mechanisms for Cyber Command's operations? These questions remain unresolved, and the lack of clarity threatens to impede both operational agility and strategic restraint.

A fourth challenge involves national cyber resilience. Most critical infrastructure in the United States is owned by the private sector, and federal authorities have limited regulatory power in many

sectors. CISA's guidance and advisories provide valuable information, but they are non-binding, as of yet. As adversaries like the PRC embed disruptive access into civilian systems, the United States must consider whether voluntary standards are sufficient. The Biden administration's National Cybersecurity Strategy called for shifting responsibility from end users to major technology providers, but this shift will take years to implement and faces political resistance. Meanwhile, adversaries continue to evolve.

And now, the prospect of cyberattacks generated using Artificial Intelligence (AI) systems are a very real threat, that is likely to grow in scale, sophistication, and persistence. U.S. policy has barely begun to scratch the surface of what may be needed to defend against AI-enabled attacks.<sup>42</sup>

A final challenge lies in the international domain. Adversaries have little incentive to adopt norms that restrict offensive cyber operations. China and Russia promote "cyber sovereignty" as a model for state control of digital infrastructure, while rejecting U.S.-led proposals for limiting operations against critical infrastructure. China, Russia, and Iran purposefully add ambiguity to cyber operations using contractors, proxies, and criminal groups, providing them with plausible deniability. At the same time, allies depend on U.S. cyber support and intelligence sharing to defend their own networks. This dynamic places considerable pressure on U.S. policy frameworks. The United States must balance domestic constraints, alliance commitments, and resource limitations while shaping global norms in a contested and rapidly evolving domain.

Collectively, these challenges underscore a central theme: U.S. cyber policy must evolve beyond episodic adjustments and embrace a long-term strategic vision. The decisions made in the coming years about force structure, legal authorities, operational doctrine, and international engagement will determine whether the United States retains strategic advantage in cyberspace or continues to cede ground to capable and determined adversaries.

For the United States to achieve and sustain advantage in cyberspace, cyber policy must be coherently aligned across the executive branch. This requires statutory authorities, organizational structures, operational processes, and public-private partnerships to function in concert rather than in parallel. Effective cyber operations are those that integrate intelligence, military, and law enforcement activities to reduce gaps and duplication; operate with sufficient agility to outpace adversaries' decision cycles; and rest on resilient critical infrastructure capable of withstanding and recovering from attack. They must also contribute to deterrence by imposing credible risk of detection, disruption, or retaliation, while remaining adaptive as threats, technologies, and adversary behavior evolve. Absent this alignment, even sophisticated capabilities risk being employed episodically, inconsistently, or too late to shape strategic outcomes.

---

<sup>42</sup> Cunningham, Mary, "Anthropic Says Chinese Hackers Used its Claude AI Chatbot in Cyber Attacks," November 14, 2025, CBS News, accessed December 8, 2025, < <https://www.cbsnews.com/news/anthropic-chinese-cyberattack-artificial-intelligence/> >



# 8

## Conclusion

U.S. cyber policy now exists in a central domain of strategic competition, but continues to be constrained by legacy authorities, unresolved institutional tensions, and an incomplete adaptation to persistent, contested cyberspace.



# Conclusion

The trajectory of U.S. cyber policy illustrates a national security enterprise still adapting to a domain that has matured faster than the institutions designed to govern it. What began three decades ago as a narrow concern about critical infrastructure protection and intelligence collection has evolved into a continuous, contested, and strategically significant arena of statecraft. Throughout this evolution, the United States has struggled to balance offense and defense, secrecy and transparency, and operational agility with the need for careful oversight.

The creation of U.S. Cyber Command, the adoption of persistent engagement and defend forward, the statutory designation (NDAA 2019) of cyber operations as a traditional military activity, and the delegation of operational authority under NSPM-13 all reflect a recognition that cyberspace is not a peripheral domain. It is now central to how adversaries plan for conflict, exert influence, and challenge U.S. interests. In response, Washington has embraced a more proactive doctrine that aims to disrupt threats before they reach American networks. These efforts have yielded, particularly in countering foreign interference in U.S. elections and degrading malicious infrastructure overseas.

Yet the transition has not been seamless. The dual-hat arrangement between NSA and Cyber Command remains both a strategic strength and an operational constraint, embodying the tension between intelligence and military missions. Title 10 and Title 50 authorities continue to blur in cyberspace, creating statutory ambiguity that complicates operations, oversight, and interagency coordination. Meanwhile, the adversary landscape grows more complex. China embeds pre-crisis access across U.S. critical infrastructure, Russia blends cyber operations with influence campaigns and conventional conflict, and Iran and North Korea routinely challenge U.S. networks with disruptive attacks.

These developments have prompted renewed debate about whether the United States needs deeper structural reform, potentially including the establishment of a standalone Cyber Force. While such a step may one day be necessary, today's capability gaps center more on workforce shortages, disparate service-level support, the absence of a long-term cyber career model, and insufficient technology development and acquisition frameworks. Without addressing these foundational issues, structural reorganization alone will not resolve the underlying challenges.

The future of U.S. cyber policy will hinge on decisions made in the coming years. Policymakers must modernize statutory authorities, strengthen oversight mechanisms, and build a more integrated interagency framework. They must also confront the reality that deterrence in cyberspace will not mirror Cold War models. Instead, it will require resilience at scale, agile operational capacity, and a doctrine capable of shaping adversary behavior while managing escalation risks.

Above all, cyber policy must become more predictable, coherent, and strategically grounded. The United States cannot afford a patchwork system that relies on ad-hoc processes or outdated legal frameworks. As adversaries refine their capabilities and expand their reach, the nation must adopt a forward-leaning strategy that protects critical infrastructure, strengthens alliances, preserves

intelligence advantages, and ensures that the United States can compete, deter, and prevail in a domain defined by speed, ambiguity, and constant competition.

Cyberspace is now a foundational dimension of national power, military readiness, economic stability, and democratic resilience. Should the United States fail to adapt, adversaries will shape the rules and rhythms of this domain to their benefit. If it succeeds, Washington can ensure that cyberspace remains an arena where American innovation, capability, and strategic discipline provide a decisive advantage. However, if the United States does not resolve these structural questions in the medium-term, it is likely to retain tactical cyber superiority while continuing to lose strategic leverage, providing a tradeoff adversaries are increasingly prepared to exploit.

*Aerial shot of the Pentagon*





## About *The McCrary Institute*

The McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University is **dedicated to defending the systems that power our national and economic security, our communities and our way of life.**

Positioned at the intersection of policy, applied research and public-private partnerships, **the Institute serves as a trusted convener of national leaders** — shaping strategy, aligning priorities and driving real-world cybersecurity solutions to protect the nation's critical infrastructure.

## Our *Leadership*

**Frank J. Cilluffo**

Director

**Nicholas Sellers**

Associate Director & Chief Operating Officer

**Victoria Dillon**

Deputy Director & Chief Communications Officer

**Kyle Klein**

Deputy Director for Policy & Partnerships

**Craig Whittinghill**

Deputy Director for Applied Research & Services