

# America Exposed

---

*How the Politicization of Cyber Is  
Crippling U.S. National Security*



September 2025

# Table of Contents

## **Executive Summary**

Key Takeaways

Key Recommendations for Congress

## **1. Introduction**

## **2. Dismantling U.S. Cyberdefenses: 2025 Policy Reversals**

**2.1:** Weakening of the Cybersecurity and Infrastructure Security Agency (CISA)

**2.2:** Disbanding of the Foreign Influence Task Force (FITF) at the FBI

**2.3:** Closure of the Counter Foreign Information Manipulation and Interference Office (R/FIMI) at the State Department

**2.4:** Removal of Gen. Timothy Haugh, Head of the National Security Agency (NSA) & U.S. Cyber Command

**2.5:** Suspension of Offensive Cyberoperations against Russia

**2.6:** Elimination of USAID Cybersecurity Assistance Programs

**2.7:** “Signalgate” & the Erosion of Security Protocols

## **3. Strategic Consequences and National Vulnerabilities**

**3.1:** Critical Infrastructure: Growing Exposure

**Case Study 1:** Colonial Pipeline (2021)

**Case Study 2:** Log4j (2021-22)

**Case Study 3:** St. Paul Ransomware (2025)

**3.2:** Adversary Posture: Iran, Russia, and China

**Iran:** Retaliation and Rapid Disruption

**Russia:** Logistics Targeting and Influence Operations

**China:** Pre-Positioning and Cognitive Warfare

**3.3** Generative AI & the Changing Cyber Battlefield

## **4. The Urgency of Congressional Oversight**

## **5. Conclusion**

# America Exposed

## ***How the Politicization of Cyber Is Crippling U.S. National Security***

---

By Liana Keesing and Lila Batcheller

### **Executive Summary**

For decades, presidents and Congress treated cybersecurity as a bipartisan imperative. Republican and Democratic administrations alike recognized that defending America's digital infrastructure is as essential as safeguarding our borders and maintaining our military strength. Programs such as the Cybersecurity and Infrastructure Security Agency (CISA), the FBI's Foreign Influence Task Force, and the State Department's counter-disinformation offices were created on this consensus and became cornerstones of America's resilience against hostile state and non-state actors.

That consensus has now been broken. What began as fringe rhetoric about "censorship" and a "deep state" has hardened into formal directives and budget cuts that hollow out the very institutions designed to protect our infrastructure, elections, and democratic integrity. The second Trump administration has pursued a series of rollbacks at precisely the moment when Russia, China, Iran, and other adversaries are intensifying their attacks. The dismantling of the FBI's Foreign Influence Task Force, deep staffing cuts at CISA, the suspension of offensive cyber operations against Russia, and the weakening of foreign influence enforcement are not routine adjustments — they are deliberate retreats from carefully constructed bipartisan tools of defense and deterrence.

The consequences of these cuts are already visible. U.S. critical infrastructure is more vulnerable; pipelines, hospitals, and election systems are being targeted; and adversaries are exploiting the very

gaps created by these decisions. By undercutting the institutions that protect Americans from attack — whether through direct network intrusions or information operations designed to destabilize public trust — the administration has created a strategic imbalance, leaving the United States weaker, more exposed, and increasingly reactive rather than prepared. Adversaries have taken note and are escalating accordingly, with Russian military hackers, Chinese state-backed groups, and Iranian propagandists already exploiting the vacuum.

If this trajectory continues, the risks will compound dramatically. Within a single election cycle, Americans could face widespread disruptions to power grids, fuel supplies, emergency communications, and hospital systems. AI-enabled propaganda could overwhelm voters with fabricated stories, erode confidence in election results, and drive domestic unrest. Foreign adversaries could deter U.S. military responses abroad by threatening mass disruption at home. In short, the hollowing out of America's cyberdefenses does not just invite more attacks — it virtually guarantees that our adversaries will succeed in striking at the very foundations of American security, prosperity, and democratic stability.

Congress must act decisively to repair this damage. Lawmakers across the political spectrum should restore bipartisan guardrails by reauthorizing and strengthening CISA's authorities, ensuring oversight of U.S. cyber capabilities, reaffirming the threat posed by foreign malign influence operations, and safeguarding the independence of U.S. intelligence reporting. These steps are not partisan. They are the minimum required to protect America's security, economy, and sovereignty in an era of intensifying digital conflict.

## Key Takeaways

- 1. Systematic Dismantling of U.S. Cyber Defenses:** Since 2025, the Trump administration has rolled back the core institutions and programs that underpinned national cyber resilience. Weakening CISA, shuttering influence-focused offices, and removing top leadership at NSA and U.S. Cyber Command have collectively hollowed out capacity, disrupted continuity, and eroded deterrence.
- 2. Critical Infrastructure Under Siege:** U.S. pipelines, hospitals, courts, and airlines are experiencing escalating cyberattacks, from Chinese “pre-positioning” campaigns to disruptive ransomware incidents. At the same time, the federal scaffolding that once provided threat intelligence and rapid coordination is collapsing, leaving local operators to “fight nation-state actors on municipal budgets.”
- 3. Adversaries Pressing the Advantage:** Iran, Russia, and China are already exploiting U.S. retrenchment to expand disruptive and influence cyber operations. Iranian retaliation, Russian logistics targeting, and Chinese cognitive warfare are converging with the spread of generative



AI, which is accelerating the speed, scale, and sophistication of attacks.

- 4. Breakdown of Oversight and Consensus:** For decades, national security drew bipartisan unity, from Cold War containment to post-9/11 reforms. That tradition is now eroding as cyber defense becomes politicized, and too few in Congress are willing to challenge the shift. The absence of robust, bipartisan oversight leaves the nation more vulnerable and undermines the shared foundation that once anchored U.S. resilience.

## Key Recommendations for Congress

- 1. Reauthorize and strengthen core cyber authorities, backed by full funding:** Congress should move quickly to renew foundational statutes such as the Cybersecurity Information Sharing Act of 2015 and ensure that they are reinforced with explicit, sustained appropriations. Protecting and expanding these authorities — alongside robust funding for CISA, the FBI, the State Department, and sector agencies — is essential to maintaining national cyber resilience.
- 2. Enforce execution of appropriated funds and prevent executive overreach:** Congress must ensure that funds it allocates for cybersecurity are actually spent as intended, not delayed, repurposed, or quietly rescinded by the executive branch.
- 3. Conduct targeted oversight after major cyber failures:** When cyber incidents expose leadership negligence or political interference, Congress should respond with hearings, inspector general reviews, and bipartisan investigations.
- 4. Reaffirm the reality and severity of foreign malign influence operations:** Congress must treat disinformation and cognitive warfare from China, Russia, and Iran as serious national security threats, not partisan talking points. By publicly acknowledging the scale of the problem and ensuring that agencies tasked with countering these operations have the mandate and resources to act, lawmakers can blunt adversaries' efforts to fracture American society.
- 5. Protect the independence and integrity of cyber threat intelligence:** Congress should guarantee that cyber threat intelligence reaches decision-makers and allies unfiltered by political manipulation. Safeguards must prevent the politicization of analytic judgments, insulate intelligence professionals from retaliation, and establish protected reporting channels that preserve accuracy, credibility, and trust across government and with international partners.

# 1. Introduction

Throughout American history, national security has served as a unifying imperative, transcending party lines in moments of crisis. Despite party differences, our political leaders have often come together to confront external threats. During the Cold War, both sides supported nuclear deterrence strategies and the founding of NATO. Containment of Soviet power was not just a Democratic or Republican policy but a durable, bipartisan doctrine. After 9/11, Democrats and Republicans jointly created the Department of Homeland Security and the Office of the Director of National Intelligence. More recently, even in an era of heightened polarization, initiatives like the U.S. Space Force drew bipartisan backing as new domains of warfare emerged. These efforts reflected a bipartisan understanding that evolving threats demand a unified national response. However, as this section explores, recent actions by the Trump administration, shaped by post-2020 political grievances and distrust of the institutions charged with safeguarding elections, have begun to unwind that shared sense of purpose and politicize cyberdefense, to the detriment of U.S. national security.



***Cyber campaigns can operate persistently in the shadows, allowing foreign powers to inflict real harm on American institutions, disrupt critical infrastructure, and undermine democratic cohesion without firing a shot.***

From the dawn of the cyber age until just before President Donald Trump's return to office, both Republicans and Democrats treated cyberwarfare as a vital national security concern. In the early 2000s, cyber operations were viewed primarily as espionage or low-level nuisances. But that view shifted dramatically in the face of escalating attacks. The [2007 cyberattacks on Estonia](#), attributed to Russian actors, targeted a NATO member's digital infrastructure and signaled the beginning of a new kind of hybrid warfare. A year later, during the [Russo-Georgian War](#), cyberattacks ran in parallel to kinetic military action. The 2010 discovery of the [Stuxnet worm](#) — widely believed to be a U.S.-Israeli cyber operation targeting Iran's nuclear program — demonstrated that digital operations could inflict strategic physical damage. These milestones transformed cyber capabilities from curiosities into core components of national defense strategy. Under President Barack Obama, cybersecurity [was elevated](#) to a top economic and security priority, and the first White House Cybersecurity

Coordinator was appointed. By the early 2010s, the cyber domain was being treated alongside land, sea, and air as a full-fledged warfighting arena, prompting the Pentagon to elevate [Cyber Command](#) and [expand](#) civilian agencies' mandates.

The 2016 election was a watershed moment. Russia's multifaceted interference campaign — including the [attempted hacking](#) of election infrastructure in all 50 states, [theft and timed release](#) of politically sensitive emails, and [coordinated disinformation](#) across social media — shattered outdated notions of cyber conflict. For years, the popular imagination of cyberwarfare resembled a Hollywood set piece: two engineers dueling through scrolling green code. But 2016 made clear that the most effective digital campaigns would combine hacking with what U.S. officials now call “[Foreign Malign Influence Operations](#).” In this model, cyber intrusions are just one instrument in a blended arsenal that includes espionage, social engineering, and the deliberate distortion of truth, all aimed at shaping perceptions, eroding trust, and manipulating decision-making at scale. The target is not just a network's hardware, but the beliefs and cohesion of the society connected to it — a form of conflict the Chinese Communist Party [labeled](#) “cognitive warfare.”

As the Russian campaign exemplified, cyber operations don't require a declaration of war. Unlike traditional military conflict, cyber campaigns can operate persistently in the shadows — below the threshold of armed conflict — allowing foreign powers to inflict real harm on American institutions, disrupt critical infrastructure, and undermine democratic cohesion without firing a shot. A full-scale strike may never come, but relentless, low-level aggression can still paralyze essential systems, corrode public trust, and sap national resilience.

Although Trump cast doubt on the intelligence community's assessment of 2016 and criticized the resulting [Mueller investigation](#), Congress responded to the threat with urgency and bipartisan resolve during his own administration. Republicans and Democrats alike backed a sweeping overhaul of the federal cyber posture. In 2018, Congress [established](#) CISA within DHS, which Trump signed into law. The FBI [launched](#) the Foreign Influence Task Force (FITF) to coordinate domestic counterintelligence efforts. The State Department's Global Engagement Center (GEC), initially founded during the Obama administration, was [expanded](#) with bipartisan support during the first Trump administration to counter increased disinformation from Russia, China, and Iran.

These efforts reflected a broad consensus: foreign cyber operations were not only violating American sovereignty, they were undermining our nation's ability to govern itself. Republican lawmakers such as Sen. [Ben Sasse](#) (R-NE) and Rep. [Will Hurd](#) (R-TX) emphasized the severity of the threat and called for enduring, bipartisan action. Sen. Rob Portman (R-OH) [described](#) foreign disinformation as “one of the most pressing challenges facing the United States and our allies around the world.”

Behind this shift was a recognition, sharpened by the aggression of 2016, that the cyber domain is fundamentally distinct from traditional kinetic warfare. It doesn't erupt on distant battlefields;

instead, it unfolds inside American communities. Unlike tanks or missiles, cyber tools target the digital infrastructure and psychological terrain of domestic life, [often blurring the lines](#) between espionage, sabotage, and psychological warfare. Moreover, the impact of cyberattacks defies traditional sectoral boundaries, threatening both national security and economic security alike. Threat actors have targeted agricultural supply chains, energy grids, water systems, and financial networks not only to cause disruption, but to erode confidence in the federal government’s ability to safeguard the nation’s economic backbone.

That reality increasingly hit home for lawmakers as attacks reached their own districts, from ransomware disrupting an [Indiana hospital network](#) in 2018, to [phishing campaigns](#) targeting U.S. utilities in 2019, to the 2020 [SolarWinds](#) breach exposing vulnerabilities across federal agencies and the private sector. As then-CISA Director Jen Easterly [explained](#), “This is a world where a major crisis halfway across the planet could well endanger the lives of Americans here at home — disrupting our pipelines, severing our telecommunications, polluting our water facilities, crippling our transportation modes — aimed at sowing panic and chaos.”

The growing scale and proximity of these threats led to a deeper integration of cyberdefense efforts that coordinated across the government, such as CISA, the FITF, and the GEC. These programs shared threat intelligence, strengthened attribution capabilities, and built partnerships with state and local governments, the private sector, and international allies. Their mandate was designed to meet the evolving threat landscape, treating foreign malign influence — from disinformation and phishing attacks to AI-generated media — as an extension of traditional cyber conflict that could touch every domain Americans depend on, from farms to finance, from power grids to polling places.

These programs, and particularly CISA, also served as essential bridges between government and industry. Recognizing that much of America’s critical infrastructure is owned and operated by private companies (like telecommunications, energy, and cloud services), these collaborations played a critical role in real-time threat sharing, joint incident response, and coordinated messaging during crises.

But this bipartisan consensus that underpinned this infrastructure began to unravel after the 2020 election. Trump’s refusal to accept the outcome and repeated assertions of election fraud placed key components of the cybersecurity apparatus (particularly those focused on disinformation and public-private information sharing) into the center of a political storm. CISA Director Chris Krebs [was fired](#) for publicly affirming the integrity of the 2020 election, while the FBI and DOJ [were accused](#) of political bias and pressured to overturn the election results. Disinformation about a “deep state” conspiracy undermined [public trust](#) in once-neutral institutions. Agencies designed to protect democratic systems were recast as enemies of the people.



Even so, under the administration of President Joe Biden, cybersecurity remained a top [bipartisan](#) priority, with Republican and Democrats alike helping to sustain momentum for new [investments](#) and [initiatives](#). The urgency of these efforts was underscored by major incidents that affected millions of Americans: in 2021, a ransomware attack on [Colonial Pipeline](#) caused fuel shortages across the East Coast, while a similar attack on [meat processor JBS](#) temporarily disrupted one-fifth of the nation's beef supply. Despite attempts by some Trump-aligned figures, such as Rep. Jim Jordan (R-OH), to frame cyber information-sharing efforts as part of a so-called "[censorship industrial complex](#)," broad bipartisan consensus endured. Lawmakers across the aisle largely agreed that the growing frequency and severity of cyberthreats demanded a coordinated, well-funded national response.

The fragility of America's information ecosystems became even more apparent in 2024, when a widespread [CrowdStrike outage](#) crippled emergency services, grounded flights, and snarled logistics nationwide. Such incidents laid bare the interdependence and brittleness of digital infrastructure, as well as the impossibility of securing it without layered, coordinated defenses.



***Influenced by loyalists hostile to the institutions that validated the 2020 election, the Trump administration has begun dismantling the very cyber infrastructure Republicans helped build. What had once been a shared mission to defend America's digital sovereignty has become a casualty of political retribution.***

Since Trump's return to office, however, everything has changed. Congressional Republicans who believed that traditional elements of cyberdefense (such as infrastructure protection and counter-espionage) would remain insulated from political retribution have been proven wrong. Under Elon Musk's Department of Government Efficiency (DOGE), CISA has [reportedly lost](#) a third of its staff, and been threatened with staffing cuts of [up to 90%](#). Programs like FITF have been [disbanded](#). Enforcement of the Foreign Agents Registration Act (FARA), which sets rules for foreign lobbyists, has been officially [deprioritized](#), particularly when it comes to covert lobbying conducted through shell organizations, influencers, or online platforms. Influenced by loyalists hostile to the institutions that validated the 2020 election, the Trump administration has begun dismantling the very cyber infrastructure Republicans helped build. What had once been a shared mission to defend America's digital sovereignty has become a casualty of political retribution.

Meanwhile, adversaries have only grown bolder. China’s “[Spamouflage](#)” campaign continues to flood American social media with coordinated propaganda, as Issue One documented in the 2024 report “[Flooding the Gap](#).” The Chinese cyber group [Volt Typhoon](#) has penetrated U.S. critical infrastructure in operations reportedly designed to pre-position for potential conflict. Russia has [resumed the targeting](#) of power grids, water systems, and health networks, while promoting divisive content across domestic platforms. Iranian-linked cyber units have [engaged](#) in election-related influence operations and infrastructure reconnaissance. In 2024 and early 2025 alone, [multiple intelligence assessments](#) have warned of rising threat activity from these states, underscoring how rapidly the digital battlefield is escalating.

If left unchecked, these developments could quickly spiral from nuisance-level interference to crises that test the very stability of American governance. A ransomware attack that shuts down a major hospital system, a foreign intrusion into air traffic control networks, or a coordinated campaign to disable voter registration databases on the eve of an election are no longer [speculative](#) “worst-case” scenarios — they are foreseeable outcomes given the vulnerabilities now widening by design. The reality is that foreign adversaries do not need to defeat the United States militarily; they need only to paralyze confidence in government and incapacitate essential services. In that environment, deterrence collapses, and the ability of the U.S. to project strength abroad is fatally compromised.

These threats are intensifying in both frequency and sophistication. Yet because of decisions made in the first 200 days of the current Trump administration, America is now less prepared to confront them. The erosion of bipartisan support for cyberdefense has already left the nation dangerously exposed, with cascading risks from paralyzed critical infrastructure to compromised military readiness. This is not a theoretical risk; it is a live battlefield. Without swift and decisive action, America will cede the digital terrain to adversaries who have already made cyberspace the front line of modern conflict.

## **2. Dismantling U.S. Cyberdefenses: 2025 Policy Reversals**

The Trump administration has taken deliberate steps to dismantle the bipartisan cyberdefense framework built over the past decade. What began as conspiracy-laden talking points has become official policy. Agencies have been gutted, experienced leaders pushed out, and core cyber deterrence strategies scrapped, not for reasons of strategy but as acts of political retribution.

These actions go beyond routine policy shifts. They represent a systematic unraveling of the institutions and norms that once anchored America’s cyber readiness. The sections that follow detail these reversals — from the weakening of CISA to the elimination of foreign influence task forces — and examine their consequences for U.S. national security.



***What began as conspiracy-laden talking points has become official policy. Agencies have been gutted, experienced leaders pushed out, and core cyber deterrence strategies scrapped.***

## **2.1 Weakening of the Cybersecurity and Infrastructure Security Agency (CISA)**

Formed in 2018 through bipartisan [legislation](#) authored by House Foreign Affairs Chairman Michael McCaul (R-TX) and signed into law by Trump, CISA was designed as the federal government’s central hub for securing both digital and physical infrastructure. CISA’s [expansive mission](#) spanned election integrity, electric grid defense, supply chain security, and the protection of digital systems underpinning agriculture, healthcare, manufacturing, water treatment, and communications. Through initiatives like the [Multi-State Information Sharing and Analysis Center](#) (MS-ISAC), CISA provided state, local, tribal, and territorial (SLTT) governments with free 24/7 network monitoring, incident response assistance, penetration testing, and security advisories. Just as importantly, CISA served as the national convener for public-private collaboration, bringing together utilities, technology companies, and critical infrastructure operators through mechanisms like the [Critical Infrastructure Partnership Advisory Council](#) (CIPAC) and the [Joint Cyber Defense Collaborative](#) (JCDC). These structures allowed government and industry to coordinate on shared threats, exchange real-time intelligence, and mount joint responses to fast-moving crises.

CISA was, by design, a national nerve center for cyber readiness. Yet its success also made it a unique political target. In 2020, after then-CISA Director Krebs publicly [affirmed the security](#) of the presidential election, Trump fired him and launched [sustained attacks](#) on the agency. House Republicans began to accuse CISA of acting as a “[censorship arm](#)” of the federal government for its coordination with social media platforms to track foreign disinformation — an effort the U.S. Supreme Court upheld as lawful in [Murthy v. Missouri](#) in 2022. What began as political rhetoric has now hardened into a policy agenda, reflected in documents like [Project 2025](#), aimed at dismantling CISA not just as an agency but as a cornerstone of America’s digital security posture.

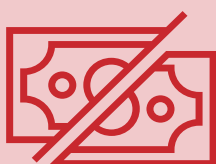
Since taking office in 2025, the Trump administration has mounted a coordinated campaign against the agency on three interlocking fronts: (1) defunding core programs, (2) slashing personnel, and

(3) retaliating against former leadership. The consequences are stark: fewer analysts tracking foreign adversaries, diminished support for state and local election officials, and a breakdown in national coordination to counter state-sponsored cyberthreats.

First, the Trump administration has defunded core elements of CISA's infrastructure protection mission. In March 2025, the agency [abruptly terminated](#) \$10 million in funding to the Center for Internet Security, effectively dismantling MS-ISAC and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). The loss of EI-ISAC was compounded by the [suspension](#) of at least 17 CISA personnel who focused on elections, including 10 regional election security specialists. These moves disrupted outreach to state and local election officials and left jurisdictions without the rapid warning systems they relied on to protect voting infrastructure. While private firms exist to provide some of these services, years of [inadequate election funding](#) mean that most jurisdictions lack the resources to replace these capabilities.

The damage was not confined to elections. The elimination of MS-ISAC dealt a serious blow to the broader backbone of national cyberdefense. As the federal government's primary cyber threat-sharing hub for SLTT governments across all sectors, MS-ISAC had supported everything from public hospitals and water utilities to school districts, municipal transportation systems, and state court networks. Its disappearance removed a lifeline for defending essential services, including real-time alerts, malware analysis, and coordinated incident response. Compounding this damage, the administration [disbanded](#) CIPAC and [failed to renew](#) a contract underlying the JCDC. These were not peripheral advisory bodies. They were the primary channels linking federal defenders to the companies that own and operate most U.S. critical infrastructure, from pipelines and power grids to cloud providers and telecom carriers. By dismantling them, the administration severed the channels that enabled joint planning, rapid threat sharing, and coordinated crisis response across government and industry.

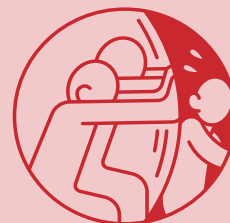
### A Three-Front Campaign Against CISA



***Defunding Core Programs***



***Slashing Personnel***



***Retaliation Against Former Leadership***

Second, CISA has faced steep personnel reductions. Since February, [approximately 1,000 employees](#) — nearly a third of CISA’s workforce — have departed through layoffs, buyouts, or voluntary resignation. This includes [more than 130](#) probationary employees recruited through programs like the [Cyber Talent Management System](#) to address long-standing technical shortfalls in areas such as ransomware mitigation and cloud security. Though a federal court later [ordered their reinstatement](#) on procedural grounds, the episode caused major disruption and demoralization across mission teams. Compounding the instability, the administration revoked CISA’s original national security [exemption](#) from DOGE’s “Deferred Resignation Program,” allowing employees to resign immediately while receiving pay through September 2025. Dozens departed, including senior staff associated with CISA’s flagship [Secure by Design](#) initiative, which works with tech manufacturers to reduce systemic cyber risk, further draining leadership and institutional knowledge.

Meanwhile, the administration signaled plans to [continue slashing](#) up to 90% of CISA’s workforce and budget, a move that would severely compromise the agency’s ability to fulfill its mission. Said [one official](#) familiar with internal deliberations: “The administration is taking a hatchet to CISA ... [The work at CISA] can’t come back if these cuts go through.” Mark Montgomery, director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, [warned](#) that the firings “are actually harming national security on a daily basis — this goes well beyond disruption and is actually destabilization.” He added that the cuts are also “weakening public-private collaboration, which is the critical lynchpin to building a resilient cyber defense.”



***As foreign adversaries grow more aggressive, the decision to weaken CISA sends a clear and dangerous signal that partisan loyalty is being prioritized over national security.***

Third, the administration has escalated its campaign against CISA by targeting its former leadership. In April 2025, Trump signed an [executive order](#) revoking the security clearance of Krebs, the former CISA director, and directing the Department of Justice to investigate his tenure. Krebs, [appointed by Trump](#) in 2018 as CISA’s first director, had publicly affirmed the integrity of the 2020 election, contradicting Trump’s claims of widespread fraud. The order also suspended clearances for individuals associated with Krebs, including personnel at SentinelOne, where he served as chief intelligence and public policy officer. These actions have been widely interpreted as [retaliatory](#) and



have drawn warnings from experts like former CISA Director Easterly, who [cautioned](#) that politicizing such roles risks “dangerously degrading” U.S. cyberdefenses.

The administration’s actions represent not only the hollowing out of a single agency, but a broader unraveling of the institutions meant to safeguard the United States in the digital age. As foreign adversaries grow more aggressive, the decision to weaken CISA sends a clear and dangerous signal that partisan loyalty is being prioritized over national security.

## **2.2 Disbanding of the Foreign Influence Task Force (FITF) at the FBI**

On February 5, 2025 — her first day in office — Attorney General Pam Bondi [abruptly disbanded](#) the FBI’s Foreign Influence Task Force (FITF), shuttering the government’s primary law enforcement unit dedicated to countering foreign malign influence in American democracy. The decision, made without public evidence or consultation, cited vague concerns over “politicization.” No replacement structure was announced. Career officials were either reassigned or left the Bureau entirely, and ongoing investigations were reportedly stalled or transferred to units lacking the necessary technical and legal expertise. The move came despite clear intelligence assessments warning of renewed efforts by Russia, China, and Iran to interfere in the upcoming 2026 midterms.

The response from national security experts has been [swift and alarmed](#). Former intelligence leaders and lawmakers, including many who originally supported the creation of the FITF, have described the move as a catastrophic abdication of responsibility. Frank Figliuzzi, former FBI assistant director for counterintelligence, [put it bluntly](#): “It’s now a free-for-all for foreign intel services seeking influence.”

The FITF’s dismantling represents a sharp reversal from what had been a rare point of bipartisan consensus. Created in 2017 under then-FBI Director Christopher Wray, the task force was launched in [direct response](#) to Russia’s sweeping interference in the 2016 presidential election. Its mission was clear: detect, investigate, and disrupt foreign influence operations targeting the United States. To that end, FITF [brought together](#) specialists in counterintelligence, cybercrime, and criminal law, forming a centralized and nimble unit capable of identifying emerging threats and responding in real time.

FITF worked closely with U.S. intelligence agencies, state election officials, and major technology companies, sharing actionable intelligence and coordinating defensive efforts. Its scope ranged from uncovering covert social media operations to investigating illicit lobbying under FARA. [In doing so](#), the task force exposed disinformation campaigns, secured indictments against Russian and Iranian operatives, and helped defend the integrity of multiple U.S. election cycles.

Though much of its work happened behind the scenes, the task force was widely credited with strengthening national resilience against foreign manipulation. What was once a model for

integrated national security operations is now gone. The void left by FITF's closure is not just a bureaucratic gap, but a signal to foreign adversaries that the United States has dismantled a key line of defense against information warfare.



***The void left by FITF's closure is not just a bureaucratic gap, but a signal to foreign adversaries that the United States has dismantled a key line of defense against information warfare.***

## **2.3 Closure of the Counter Foreign Information Manipulation and Interference Office (R/FIMI) at the State Department**

On April 16, 2025, Secretary of State Marco Rubio announced the [closure](#) of the State Department's Counter Foreign Information Manipulation and Interference office (R/FIMI), formerly known as the Global Engagement Center (GEC). Established in 2016 under the Obama administration, the GEC was tasked with countering foreign disinformation campaigns, particularly from adversaries like Russia, Iran, and China, aimed at undermining or influencing the policies and security of the United States and its allies.

Among its core contributions, the GEC published landmark public analyses that shaped U.S. and allied policy: In 2020, it produced the first comprehensive [U.S. government mapping](#) of Russia's disinformation and propaganda ecosystem, and in 2023, it released a [widely cited report](#) detailing how China seeks to reshape the global information environment (including tactics such as platform manipulation and censorship). The center also built practical capacity. Its [Technology Engagement Division](#) ran a recurring Tech Demo Series to source and test counter-disinformation tools, and the [Disinfo Cloud platform](#) gave U.S. agencies and foreign partners an unclassified marketplace to discover and evaluate relevant technologies. Beyond analysis and tech, the GEC funded on-the-ground resilience: via the Information Access Fund and other assistance programs, the center [issued](#) tens of millions of dollars in awards year over year — about \$15.7 million in FY 2019-20 and \$16.9 million in FY 2020-21 — to bolster independent media, fact-checking networks, and civic groups. The office had garnered bipartisan [support](#) for its role in combating propaganda and safeguarding U.S. interests.

However, just like CISA and the FITF, the GEC faced increasing [criticism](#) from conservative circles, alleging that it overstepped its mandate by suppressing conservative viewpoints under the guise of combating disinformation. Following the expiration of its congressional mandate in December 2024, the GEC was restructured into R/FIMI. Despite the rebranding, skepticism among certain conservatives persisted regarding the office’s activities. Rubio baselessly [cited concerns](#) over censorship and the misuse of taxpayer funds, stating that the office “spent millions of dollars to actively silence and censor the voices of Americans they were supposed to be serving.” In reality, the office had [no authority](#) to regulate speech or platforms in the United States and its mandate was strictly focused on exposing and countering foreign propaganda abroad, making claims of censorship fundamentally misleading.

The closure of R/FIMI resulted in the [elimination](#) of approximately 50 full-time positions and the reallocation of its \$65 million budget. As Sen. Jeanne Shaheen (D-NH) — the top Democrat on the Senate Foreign Relations Committee — [put it](#), Trump is “completely ceding the global information space to our adversaries, who are only too happy to fill the void with anti-American propaganda. Moscow and Beijing celebrate each time this administration dismantles another critical foreign policy tool.”

## **2.4 Removal of Gen. Timothy Haugh, Head of the National Security Agency (NSA) & U.S. Cyber Command**

On April 3, 2025, Trump [dismissed](#) Gen. Timothy Haugh from his dual roles as Director of the National Security Agency (NSA) and Commander of U.S. Cyber Command, marking a significant shift in the nation’s cybersecurity leadership. Haugh, a four-star Air Force general with more than three decades of service in intelligence and cyberoperations, had been appointed to these positions in February 2024. His tenure was characterized by efforts to bolster U.S. cyberdefenses amid escalating threats from adversaries like China and Russia.

The abrupt termination of Haugh’s leadership came without a public explanation from the administration. [Reports](#) indicate that the decision followed a meeting between Trump and far-right activist Laura Loomer, who advocated for Haugh’s removal, citing alleged disloyalty and ties to former military officials perceived as critical of Trump. Loomer publicly [claimed credit](#) for the dismissal, stating that Haugh and his deputy, Wendy Noble, were “disloyal to President Trump” and thus “have been fired.”

Sen. Mark Warner (D-VA), vice chair of the Senate Intelligence Committee, [expressed alarm](#) over the politicization of national security roles, emphasizing Haugh’s distinguished service. Rep. Jim Himes (D-CT), ranking member of the House Intelligence Committee, [described](#) the decision as “deeply disturbing,” arguing that such actions compromise the integrity and effectiveness of U.S. intelligence operations.

Abrupt personnel changes, driven by perceived political loyalty rather than merit, undermine the nation's ability to respond effectively to cyberthreats and erode trust within the intelligence community and with international cybersecurity partners. The dismissal of Haugh and the ensuing leadership upheaval signify a troubling shift in the prioritization of political loyalty over national security expertise.

Like the executive order targeting former CISA Director Krebs, Haugh's removal appears less about performance and more about retribution — sending a chilling message to the intelligence and defense communities that professional integrity may be punished if it conflicts with political narratives. This politicization corrodes institutional trust, deters future public service, and emboldens foreign adversaries who benefit from American dysfunction.

## 2.5 Suspension of Offensive Cyberoperations against Russia

In March 2025, the Trump administration ordered U.S. Cyber Command to [suspend](#) all offensive cyber and information operations targeting Russia. This directive, issued by Defense Secretary Pete Hegseth, marked a significant shift in U.S. cybersecurity policy, raising questions about the administration's stance toward Russia.

The suspension encompassed not only active cyberattacks but also the planning of such operations, effectively halting initiatives designed to deter or disrupt Russian cyber activities. This decision is particularly concerning given Russia's [extensive history](#) of cyber aggression against the United States. Russian state-sponsored actors have been implicated in numerous cyberattacks targeting U.S. critical infrastructure, including the [2014 infiltration](#) of the State Department's email system, the [2020 SolarWinds](#) supply chain attack compromising multiple federal agencies, and the [2017 NotPetya](#) malware attack, which disrupted operations across various sectors, including healthcare, energy, and transportation. Additionally, Russian-linked groups have targeted [U.S. water treatment facilities](#), [hospitals](#), and [local governments](#), exploiting vulnerabilities to gain unauthorized access and, in some cases, manipulate control systems.

Offensive cyberoperations are not merely tools of retaliation; they are essential instruments for proactive defense. Cyberoperations enable the United States to disrupt adversaries' capabilities before attacks materialize, gather critical intelligence on emerging threats, and impose costs on malicious actors to deter future aggression. As outlined in the Department of Defense's [2023 Cyber Strategy](#), such operations are integral to “campaigning” — undertaking actions to limit, frustrate, or disrupt adversaries' activities below the level of armed conflict and to achieve favorable security conditions.

By suspending offensive cyberoperations without securing concrete assurances from Russia to cease its cyber activities, the administration has carried out the Kremlin's cyberwarfare strategy on

its behalf — without Russia needing to lift a finger. This decision is the cyber equivalent of lowering a city's defenses while siege engines are gathering at the gates. In fact, less than a month after Hegseth announced a pause on offensive operations, Western New Mexico University's website and digital systems were [held hostage](#) by the infamous Russian hacking group Qilin, claiming to have access to employee payroll data, Social Security numbers, and driver's licenses.

## 2.6 Elimination of USAID Cybersecurity Assistance Programs

In early 2025, the Trump Administration initiated a [sweeping dismantling](#) of the U.S. Agency for International Development (USAID), eliminating the entire agency, along with 83% of its programs. Among the most consequential cuts was the termination of over [\\$175 million](#) dedicated to cybersecurity and technology assistance for U.S. allies and partners.

These cybersecurity programs were instrumental in bolstering the digital defenses of partner nations vulnerable to cyberthreats, particularly from state-sponsored actors. For instance, a five-year, [\\$95 million contract](#) with IBM aimed to deploy cybersecurity experts to countries such as Albania, Azerbaijan, Kosovo, and Moldova. The initiative focused on establishing security operations centers, training local cybersecurity personnel, and enhancing the resilience of critical infrastructure.



***The elimination of USAID's cyber programs doesn't just reduce goodwill — it actively erodes the foundations of allied resilience and weakens the forward posture of U.S. cyber strategy in contested regions.***

The selection of these countries was strategic. Albania, a NATO member, has faced significant cyberattacks, including a [major incident in 2022](#) (attributed to Iranian actors) that almost led to the country invoking NATO's Article 5, the collective defense clause that treats an attack on one member as an attack on all. Azerbaijan, located at the crossroads of Eastern Europe and Western Asia, plays a [vital role](#) in regional energy security and counterterrorism efforts. Kosovo, as a young nation with aspirations for Euro-Atlantic integration, has been [targeted](#) by cyberattacks aimed at disrupting its governmental functions and economic activities. And Moldova, bordering Ukraine and in close proximity to Russia, occupies a pivotal position in Eastern Europe's security landscape and has faced a surge of [over 300%](#) in cyberattacks since the invasion of Ukraine.



The sudden shutdown has opened a gap in allied cyberdefenses just as adversary activity intensifies. [Albania](#) and [Azerbaijan](#) are weathering fresh campaigns from Iran- and Russia-linked actors. Meanwhile, Moldova's increasing vulnerabilities [led the EU](#) to send an emergency cyber reserve to protect its September 2025 parliamentary elections from Russian hacking, which aims to tilt the playing field toward anti-US, EU, and NATO political forces. This strategic withdrawal erodes U.S. leadership in global cybersecurity and cedes ground to authoritarian adversaries.

China, in particular, has already [shown a desire](#) to capitalize on this void through its [Digital Silk Road](#) initiative, which offers developing nations comprehensive digital infrastructure packages, including telecommunications networks, cloud computing services, and cybersecurity solutions. While these offerings provide much-needed technological capacity, they [embed](#) Chinese hardware and software deeply into the digital foundations of foreign governments. This creates persistent access points for Chinese intelligence services, expands Beijing's ability to conduct cyber-espionage, and undermines the ability of the United States to share sensitive information with affected allies.

The consequences are immediate and concrete. Intelligence sharing is complicated by the risk of compromise. Regional allies become more vulnerable to coercion through digital surveillance. And U.S. military planners lose both trust and technical interoperability with partner nations, degrading coordinated cyberdefense efforts and raising the costs of collective deterrence. The elimination of USAID's cyber programs doesn't just reduce goodwill — it actively erodes the foundations of allied resilience and weakens the forward posture of U.S. cyber strategy in contested regions.

## 2.7 “Signalgate” & the Erosion of Security Protocols

A defining feature of the current administration's approach to national security has been its persistent disregard for basic cybersecurity and information protection protocols — a pattern that has already resulted in multiple breaches, institutional instability, and elevated risks to U.S. operations and infrastructure. In March 2025, “[Signalgate](#)” exploded into public view when journalist Jeffrey Goldberg was accidentally added to a Signal group chat where top Trump administration officials — including Defense Secretary Hegseth and National Security Advisor Mike Waltz — were actively discussing classified military operations against Houthi rebels in Yemen. The chat reportedly contained sensitive operational details, including target coordinates, strike timing, and weapons platform configurations.

Around the same time, the General Services Administration experienced a significant security lapse when a Google Drive folder containing sensitive documents, including White House floor plans and vendor bank details, was [inadvertently shared](#) with over 11,200 staff members.

Additionally, under a sweeping initiative to “streamline” federal data, DOGE has sought to consolidate massive volumes of sensitive information — including records from the IRS, DHS, HUD, and the Social Security Administration — into a [single centralized database](#). National security

experts have [warned](#) that such aggregation, if not rigorously protected, creates a single point of failure: a treasure trove for nation-state hackers and insider threats alike. The danger has been compounded by DOGE's reliance on [minimally vetted](#) hires (some as young as 19) who were granted broad access to sensitive systems despite limited experience and no established security credentials. In at least one instance, DOGE staff [accessed](#) secure networks tied to the National Nuclear Security Administration and the Defense Department's classified communications infrastructure.



***A defining feature of the current administration's approach to national security has been its persistent disregard for basic cybersecurity and information protection protocols.***

These incidents collectively reflect a pattern of negligence and disregard for established security protocols, undermining the integrity of national cybersecurity infrastructure and eroding trust in governmental data handling practices. In an era where cyberthreats are increasingly sophisticated and pervasive, such lapses not only jeopardize immediate operations but also erode the trust and integrity essential to national security infrastructure.

### **3. Strategic Consequences and National Vulnerabilities**

Since January 2025, the Trump administration's cyber and national security rollbacks have begun to manifest in concrete, strategic vulnerabilities now being actively exploited by our adversaries. By gutting core institutions, suspending offensive operations, and dismantling international cyber partnerships, the United States has ceded initiative to adversaries who are wasting no time exploiting the resulting gaps. These changes have weakened deterrence, destabilized global alliances, and emboldened China, Russia, and Iran to test the limits of American resolve.

The net effect is an asymmetric environment in which pipelines, hospitals, and other vital systems face sharper, more frequent intrusions while federal capacity to defend, deter, or recover is diminishing. Generative AI compounds the problem, super-charging adversary tradecraft and compressing warning timelines across every domain.

The sections that follow examine three interlocking vulnerabilities: (1) the exposed seams in U.S. critical infrastructure, with energy and health care as representative case studies; (2) the expanding reach and resolve of major state actors; and (3) the disruptive potential of AI-enabled operations. Together, these dynamics reveal a strategic environment in which U.S. preparedness is eroding just as the scale, speed, and sophistication of foreign threats intensify.



***The Trump administration’s cyber and national security rollbacks have begun to manifest in concrete, strategic vulnerabilities now being actively exploited by our adversaries.***

### **3.1 Critical Infrastructure: Growing Exposure**

The U.S. government [formally designates](#) 16 sectors as “critical infrastructure,” spanning energy, healthcare, transportation, government services and facilities (including election infrastructure), financial services, agriculture, and other domains essential to national security, economic stability, and public safety. These systems were not designed for sustained digital conflict. Many rely on aging technology, fragmented oversight, and uneven security standards. For years, federal agencies like CISA served as the connective tissue, providing cyber threat intelligence, on-call incident response, and sector-specific coordination that helped raise the collective floor. That scaffolding is now eroding.

Federal intelligence officials [have been clear](#): These systems are not only vulnerable, but are being actively and systematically targeted. “Chinese government-linked hackers have burrowed into U.S. critical infrastructure,” [warned](#) then-FBI Director Wray in April 2024, “waiting for just the right moment to deal a devastating blow.” Former CISA Director Easterly has [echoed the same concern](#), stating that Chinese actors are “burrowing deep into our critical infrastructure to be ready to launch destructive cyberattacks in the event of a major crisis or conflict.” This is not theoretical. A [May 2025 joint advisory](#) from CISA, the NSA, and the FBI assessed “with high confidence” that Beijing-affiliated Volt Typhoon actors are pre-positioning across U.S. networks, with the intent to disrupt critical services at a time of their choosing. The U.S. Intelligence Community’s own [2025 Annual Threat Assessment](#) concluded that China has “demonstrated the ability to compromise U.S. infrastructure” and could deploy that access in the context of a future conflict.

That threat is already being felt on the ground. In February, a ransomware incident [shut down](#) Cleveland Municipal Court operations for more than two weeks, forcing the Ohio National Guard's Cyber Reserve to [step in](#) to contain and remediate the breach. In April, medical-device manufacturer Masimo disclosed that a cyberattack [had disrupted](#) manufacturing operations, delaying delivery of clinical equipment and underscoring the supply chain implications of poorly defended infrastructure. That same month, a breach at dialysis provider DaVita [exposed the personal data](#) of more than one million patients and required weeks of mitigation. In early August, the U.S. federal judiciary announced it had been [targeted](#) by a "sophisticated and persistent cyberattack" on its electronic case files system. Hawaiian Airlines suffered a cyberattack in June that [disrupted](#) some IT systems. Each of these incidents reflects a broader pattern: adversaries are not simply testing U.S. systems — they are imposing real-world costs and [probing for systemic weakness](#).

Meanwhile, the safety net that previously helped contain and coordinate these threats is weakening. The once-robust partnership between federal cyber agencies and critical infrastructure operators has frayed. In recent months, industry leaders have described the relationship as being in "[suspended animation](#)," pointing to canceled briefings, missing points of contact, and the collapse of trusted forums like [CIPAC](#), which allowed industry groups to discuss sensitive cybersecurity information without exposing that information to the public. "With CISA," one senior energy executive told [Cybersecurity Dive](#), "there is no partnership. It's gone." Another energy industry representative [shared](#) that the oil and natural gas industry is currently refusing to share the products of its cyber working groups with the government "until we are assured that we have those [CIPAC] protections." On July 25, 2025, CISA's flagship coordination hub, the JCDC, [lost over 100 contractors](#) after DHS failed to renew its support contract. This left the program staffed by just 10 people during a time of heightened Chinese cyber activity.

The disruption is not limited to Washington. Across the country, state and local officials have reported diminished federal engagement. Field staff who previously served as trusted, on-the-ground cybersecurity advisors are "[simply no longer there](#)," in the words of one local official, and federal communications to operators have reportedly slowed or stopped. With fewer alerts, briefings, and surge teams, municipalities and utilities are finding themselves increasingly isolated in the face of growing threats. "We will need to be more self-reliant," one senior state official told [StateScoop](#), summarizing the emerging consensus among state and local cybersecurity leaders. At the same time, ISACs — the Information Sharing and Analysis Centers that act as early-warning hubs for states and small operators — have seen their federal support [cut or redirected](#), straining the very networks that exist to help operators manage cyber risk collectively.

The implications are clear. The threat environment is worsening while the connective tissue that once tied together federal capabilities and local operators is fraying. As one local government chief technology officer [put it](#), "We're trying to fight nation-state actors on municipal budgets." For cities,

hospitals, courts, water systems, and small electric utilities, that's not just unsustainable, but actively dangerous.

The following three case studies trace a simple arc: Colonial Pipeline reveals the cost of limited federal leverage, Log4j shows what coordinated authority can deliver, and St. Paul illustrates the risks when capacity and partnership erode.

## Case Study 1: Colonial Pipeline (2021)

When ransomware operators struck Colonial Pipeline in May 2021, during the Biden administration, they forced a [six-day shutdown](#) of the largest fuel pipeline in the United States, halting nearly half of the East Coast's fuel supply. The effects were immediate and dramatic: [Gas stations](#) from Georgia to Virginia ran dry, [emergency declarations](#) were issued in 17 states plus D.C., and national average gas prices [spiked](#) to their highest level since 2014. [Panic buying](#) compounded the shortages, with images of motorists hoarding fuel in plastic containers spreading across social media and amplifying public anxiety.

At the time, CISA lacked the statutory authority or staffing depth to compel security practices in the energy sector. Responsibility instead fell to the Transportation Security Administration (TSA), which scrambled to issue emergency cybersecurity [directives](#) only *after* the attack had already exposed the sector's fragility. In the critical first days, federal coordination was ad hoc, recovery was slow, and much of the response burden fell to Colonial's private contractors. The episode revealed the dangers of treating critical infrastructure cybersecurity as largely voluntary and under-resourced.

In response, Congress and the executive branch expanded CISA's authorities, staffing, and cross-sector partnerships, including the creation of the [JCDC](#), which brought together more than 25 major pipeline operators and industrial control system partners to proactively share threat intelligence and strengthen security practices. Then-CISA Director Easterly later cited the JCDC as one of the agency's most important [post-Colonial reforms](#).

Those gains are now at risk. On July 25, 2025, DHS allowed the JCDC's [contractor support](#) to lapse, cutting its operational staff from more than 110 to just 10. The decision comes amid a surge in Chinese state-backed activity targeting U.S. critical infrastructure — campaigns that the JCDC had been instrumental in [responding to and tracking](#).





## Case Study 2: Log4j (2021-22)

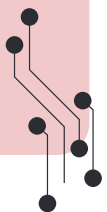
In December 2021, security researchers uncovered a vulnerability in the widely used open-source Log4j software library that experts quickly labeled one of the most severe cyber risks [ever identified](#). Known as “Log4Shell,” the flaw was exploitable with minimal skill and attracted [rapid interest](#) from nation-state actors in China, Iran, North Korea, and Russia. The scale of exposure made it one of the most far-reaching software vulnerabilities ever discovered.

Unlike earlier crises, the federal response to Log4j was swift, coordinated, and effective — in large part because CISA had both the statutory authority and institutional capacity to lead. Just one day after public disclosure, CISA began issuing mitigation guidance and mobilizing its partners. By December 17, it released [Emergency Directive 22-02](#) under authority granted by the Federal Information Security Modernization Act ([FISMA](#)), requiring all civilian executive branch agencies to identify, mitigate, and patch vulnerable systems within days. It also stood up a [centralized website](#) and a [public GitHub repository](#) to consolidate vetted technical guidance and help defenders triage risk.

Behind the scenes, CISA activated its newly launched JCDC. As documented in a report from DHS’s [Cyber Safety Review Board](#), members shared sensitive, often unpublished intelligence with CISA in real time, allowing the agency to generate threat analyses, detection tools, and patching guidance at national scale. CISA stood up Slack channels for direct bidirectional communication with industry and government stakeholders, enabling the rapid distribution of indicators of compromise and tactics, techniques, and procedures. Multiple JCDC partners later told investigators that this approach accelerated mitigation and information-sharing by days or even weeks compared to past efforts.

The result was remarkable: Despite near-universal exposure, the United States avoided catastrophic disruptions to energy, healthcare, financial services, and other critical sectors. What could have spiraled into a systemic cyber event instead became a case study in national-scale resilience. The Log4j response showed what CISA can achieve when it is fully staffed, funded, and authorized, and foreshadowed the kinds of reforms later codified in the [Cyber Incident Reporting for Critical Infrastructure Act](#) (CIRCI) in 2022.

As CISA and the JCDC face staffing reductions and political headwinds, the success of the Log4j response is a critical reminder: The next major security vulnerability may not be so forgiving if the nation’s lead cyber agency is weakened before it can act.



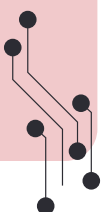


### Case Study 3: St. Paul Ransomware (2025)

In late July 2025, the city of St. Paul, Minnesota, detected a “deliberate, coordinated, digital attack” on its systems, [forcing officials](#) to shut down networks and revert to manual operations across core services — payroll, permit processing, library circulation, online utility payments, and more. The mayor declared a local emergency; the city stood up a [mass password-reset operation](#) for 3,500 employees while libraries lost public Wi-Fi and printing for weeks. “The magnitude and complexity of the cybersecurity incident [has] exceeded the city’s response capacity,” Gov. Tim Walz (D-MN) said as he [activated](#) the Minnesota National Guard’s cyber protection unit to help stabilize operations.

Federal investigators were involved, but the response underscored how much of the operational burden now sits on state and local shoulders. The FBI [confirmed](#) it was “working with partners,” while CISA [referred questions](#) back to the city rather than front-footing a visible federal surge. At the same time, multiple state and local cyber leaders report they are receiving fewer communications and support than in prior years. “We will need to be more self-reliant,” one [StateScoop survey](#) of officials summarized; a municipal chief technology officer in Florida put it more bluntly: “This isn’t a local government problem. This is a national security problem and it requires federal-level attention.” Others say the CISA regional staff who used to show up “are simply no longer there.”

The threat actor claiming responsibility — the “Interlock” ransomware group that the FBI, CISA, and MS-ISAC had [warned about](#) a week earlier — highlights why diminished federal backstops matter: cities face nation-state-grade tradecraft and financially motivated crews with limited capacity to absorb shocks. St. Paul’s [own updates](#) emphasize it worked “with local, state, and federal partners,” but the wider context is stark: key information-sharing lifelines like the MS-ISAC have had federal support cut, with state and local groups [warning](#) that gaps will “make [them] more susceptible to cyberattacks.” As one former NSA cyber chief [cautioned](#), reductions have cost the government “operational capability” and the relationships and expertise needed to “dive in on some of these hard problems.”



## 3.2 Adversary Posture: Iran, Russia, and China

The growing vulnerabilities in U.S. infrastructure present a strategic opportunity for America's principal adversaries, each of whom has long treated cyberoperations as a core tool of statecraft. Iran, newly embarrassed by recent strikes on its nuclear facilities, has already intensified its cyber activity, turning to wipers, ransomware, and information operations to create cascading effects and exert political pressure at low cost. Russia continues to blend disruptive cyber intrusions with influence operations, probing energy systems and state-local infrastructure to impose costs and test geopolitical red lines. And China remains the most methodical and long-term threat, quietly pre-positioning in U.S. critical infrastructure while harvesting strategic intelligence in support of its broader economic and military objectives.

These campaigns directly exploit the fault lines outlined in Section 3.1 and are made more dangerous by the recent dismantling of federal capabilities that once deterred, detected, or responded to such operations. With diminished surge capacity, weaker attribution capabilities, and signals of unilateral retreat, the U.S. now faces an emboldened set of adversaries adapting their playbooks in real time. The sections that follow examine how Tehran, Moscow, and Beijing are evolving their tactics in this new environment — and the distinct challenges each poses to national security.

### Iran: Retaliation and Rapid Disruption

Iran increasingly uses cyberspace as an extension of its military and regional strategy. Since the start of the Israel– Hamas war in October 2023, Tehran has synchronized intrusions and influence to punish adversaries, complicate decision-making, and coerce at minimal cost. The tempo has accelerated sharply: what were bi-monthly operations in 2021 [surged](#) to 11 in October 2023 alone, and Iranian-linked intrusions have since spilled far beyond their traditional regional focus, stretching from [Albania](#) to [Bahrain](#).

That trajectory makes retaliatory action against the United States more likely, especially following the June 21, 2025, U.S. airstrikes on Iranian targets. Within 48 hours of the strikes, Arizona officials [reported](#) “moderate confidence” that Iranian state or proxy actors defaced the state’s candidate portal, substituting candidate photos with an image of Ayatollah Ruhollah Khomeini. The same infrastructure probed additional state agencies. The episode is emblematic of Iran’s playbook: quick, symbolic operations that create friction in civic systems and manufacture political pressure. Notably, Arizona Secretary of State and Issue One [Faces of Democracy member](#) Adrian Fontes (D-AZ) did not reach out to CISA for support, [explaining](#), “Up until 2024, CISA was a strong and reliable partner in our shared mission of securing American digital infrastructure, but since then the agency has been politicized and weakened by the current administration. Given their recent conduct, and broader trends at the federal level, we’ve lost confidence in [CISA’s] capacity to collaborate in good faith or to prioritize national security over political theater.”



***Up until 2024, CISA was a strong and reliable partner in our shared mission of securing American digital infrastructure... Given their recent conduct, and broader trends at the federal level, we've lost confidence in [CISA's] capacity to collaborate in good faith or to prioritize national security over political theater."***

**- Arizona Secretary of State Adrian Fontes**

Beyond opportunistic defacements, Iran continues to pursue more strategic intrusions against U.S. government and defense-adjacent networks. In 2024, [four Iranian nationals](#) tied to a hacking organization targeted U.S. companies as well as the Treasury and State Departments — part of a multi-year effort to compromise firms with defense-related information and to erode confidence in federal networks. Former CIA officer and FBI Special Agent Tracy Walder [has described](#) potential Iranian cyber activity as the “No. 1 threat” following renewed U.S. engagement in the region, and former White House CIO Theresa Payton [warns that](#) likely targets span everyday citizens, elected officials, media, and critical infrastructure.

Federal warnings mirror these assessments. On June 30, 2025, CISA, the FBI, DC3, and NSA [jointly cautioned](#) about heightened Iranian activity exploiting common weaknesses — poorly secured networks, outdated software, and default credentials — while [private-sector telemetry](#) recorded a marked uptick in Iran-linked operations in May-June 2025, frequently aimed at disrupting supply chains and stealing operational data.

Iran frames these campaigns as [defensive and ideological](#), integrating technical breaches with intimidation campaigns to unsettle targets and magnify strategic effect. As federal surge capacity and attribution capabilities are being pared back, this low-cost, high-impact model is more likely to succeed, raising both the frequency and the consequences of Iranian cyberoperations against U.S. interests.

## **Russia: Logistics Targeting and Influence Operations**

Russia wields cyberspace and information operations as integrated instruments of [national power](#): tools to coerce, disrupt, and shape narratives below the threshold of armed conflict. This doctrine, articulated in 2013 by Gen. Valery Gerasimov, [envisions](#) a form of “total war” in which nonmilitary

means — cyberoperations, disinformation, and economic pressure — can eclipse the impact of traditional weapons. This posture [has only intensified](#) in recent years, with Russian services targeting Western logistics, government networks, and public discourse to impose costs and gain leverage against the United States and its allies. In May 2025, for example, CISA and partner agencies [warned that](#) GRU Unit 26165 (APT28) is running a multi-year espionage campaign against Western logistics and technology firms involved in coordinating and transporting aid to Ukraine, stealing credentials, schedules, and cargo details that illuminate supply routes and operational seams.

Against that backdrop, the administration’s decision in March 2025 to order U.S. Cyber Command to pause offensive cyber and information operations against Russia sent precisely the wrong signal. The pause, reported by [major outlets](#) and condemned by [congressional leaders](#), telegraphed unilateral disarmament in the midst of active Russian campaigns. Even where elements were narrowed or temporarily reversed, the public ambiguity undercut deterrence in the midst of active Russian campaigns.

The operational threat is concrete. Russian actors [have repeatedly probed](#) high-value government systems, as seen in the [July 2025 breach](#) of federal court filing networks, [an intrusion](#) that exposed sealed matters and forced emergency workarounds in multiple districts. Russia’s capacity and willingness to penetrate trusted digital supply chains is well established, with the [2020 SolarWinds compromise](#) still a benchmark for the scale and sophistication of Russian cyber-espionage.

Moscow pairs its cyber intrusions with persistent information operations designed to confuse, divide, and weaken the United States from within. The narratives are [consistent and strategic](#): themes of Western decline, alleged “Russophobia,” and Russia’s self-portrayal as a multipolar stabilizer. These lines echo Soviet-era “active measures,” blending espionage, disinformation, and subversion to legitimize attacks on U.S. systems and fracture domestic consensus.

While [Russia’s efforts](#) in the 2016 presidential election are well known, its ongoing influence campaigns receive far less scrutiny, despite their growing scale and sophistication. A [December 2024 report](#) by Issue One found that foreign adversaries flooded American platforms with disinformation during the 2024 election cycle, and Russia was by far the most active, responsible for at least 110 of the roughly 160 online false narratives tracked by NewsGuard. In 2025, researchers and platforms continue to catch Russian operations aimed at U.S. audiences: DFRLab [traced](#) the Kremlin-aligned “Doppelganger/Undercut” network reaching millions of users with English-language memes and AI-narrated videos across mainstream sites, and Google’s Q2 bulletin [details](#) thousands of takedowns of Russia-linked channels posting in English that are supportive of Russia and critical of the United States and the West.

Recent U.S. messaging has not matched the threat. In remarks to a United Nations working group on cybersecurity earlier this year, a senior State Department official flagged China and Iran but



[did not highlight Russia](#), an omission that diverged from European counterparts and from Russia's well-documented record. As cyber expert James Lewis [put it](#), "It's incomprehensible to give a speech about threats in cyberspace and not mention Russia, and it's delusional to think this will turn Russia and the FSB into our friends."

In this environment, standing down offensive and counter-influence operations signals retreat and reduces the leverage that coordinated, persistent U.S. cyber operations have historically provided.

## **China: Pre-Positioning and Cognitive Warfare**

The administration has [repeatedly signaled](#) that China is the pacing challenge in U.S. national security — yet recent rollbacks undercut the very infrastructure needed to meet that challenge. Weakening CISA's surge capacity, dismantling influence-counteracting capabilities, and undermining core pieces of federal cyber response create precisely the gaps Beijing is designed to exploit.

China's approach blends state power, commercial innovation, and information control into a single, long-horizon strategy. Under [civil-military fusion](#), universities, state-owned enterprises, and "private" tech firms feed talent, tooling, and research directly into security services and the People's Liberation Army (PLA). [PLA doctrine](#) treats control of the information environment as decisive in both peace and conflict. Cyber operations, therefore, are not only for theft or disruption; they are integrated with cognitive warfare to condition decision cycles, normalize narratives promoted by the People's Republic of China (PRC), and gradually wear down institutional resilience.

Analysts describe the present as a "[golden age](#)" of PRC hacking: a shift from smash-and-grab theft to disciplined, mission-specific intrusions that pre-position access, harvest strategic intelligence, and hold critical functions at risk. Recent compromises of U.S. scientific and national-security agencies through widely used enterprise software illustrate the trend and the stakes. These campaigns are part of a continuum, from the [OPM breach](#) (2015) to the [Microsoft Exchange exploitation](#) (2021) to today's [Volt/Salt](#) Typhoon [pre-positioning](#) in U.S. critical infrastructure.

Each episode underscores the same message: Beijing treats persistent access to U.S. government, health, and energy systems as a strategic asset, not a one-off operation. CrowdStrike's [2025 Global Threat Report](#) captures the scale and speed of this surge, noting a 150% increase in China-nexus activity and a clear evolution in tradecraft toward stealthy, objective-driven operations. These efforts have translated into more quiet footholds in the very places discussed in Section 3.1 — pipelines, hospitals, state and local networks — paired with synchronized information operations (such as the [Dragonbridge](#) and [Spamouflage](#) campaigns) designed to magnify disruption, sap public confidence, and complicate U.S. response.

Declaring China the pacing threat while trimming the tools that counter Volt/Salt Typhoon is incoherent. Cutting \$14 million from [JCDC](#) and shrinking threat-hunting slows known exploited

vulnerability (KEV) updates, dulls public-private response, and lengthens PRC dwell time across critical networks.

### 3.3 Generative AI & the Changing Cyber Battlefield

Building on the infrastructure exposures in Section 3.1 and the adversary campaigns in Section 3.2, recent advancements in generative AI have become a force multiplier, accelerating existing threat vectors and expanding the cyber battlefield. Tehran, Moscow, Beijing, and their proxies are already using AI to scale reconnaissance, automate exploit discovery, and tailor influence operations. By lowering skill thresholds and compressing warning timelines, AI transforms one-off intrusions into high-frequency campaigns against pipelines, hospitals, and state-local networks. This section outlines four trends — democratized offensive tooling, automated vulnerability discovery, personalized deception, and machine-speed operations — that make this a uniquely dangerous moment for a cyber retreat.

First, AI democratizes offensive capability. [Assessments](#) from the UK’s National Cyber Security Centre (NCSC) conclude that widely available AI will increase both the volume and impact of cyberattacks by lowering skill and cost thresholds for criminals, terror groups, and state proxies alike, [including](#) more convincing phishing and social-engineering operations. Those warnings [now extend](#) through 2027, with NCSC flagging that organizations unable to defend against AI-enabled tradecraft face heightened risk. At the nation-state level, [OpenAI and Microsoft](#) jointly reported in February 2024 that actors linked to China, Russia, Iran, and North Korea were already experimenting with generative AI to support reconnaissance, social engineering, and malware-adjacent tasks. The trajectory also matches longer-standing [academic forecasts](#) that AI would “endow low-skill individuals with previously high-skill attack capabilities.”

Second, AI accelerates automated vulnerability discovery. DARPA’s [AI Cyber Challenge](#) (AixCC) is explicitly driving and publicly demonstrating AI systems that automatically find and patch software flaws at scale, underscoring that machine-speed vulnerability work is no longer theoretical. In parallel, [peer-reviewed](#) research shows frontier models can autonomously exploit real-world “one-day” vulnerabilities at high success rates when provided technical descriptions. The policy implication is clear: If attackers can discover and test exploits faster, defenders need equally automated detection, patching, and response pipelines.

Third, AI enables highly personalized social engineering and synthetic media at scale. The FBI [has warned](#) of campaigns impersonating senior U.S. officials using AI-generated messages, and [more broadly](#) of criminals leveraging generative AI to increase the believability and throughput of fraud. The FTC cautions that [voice cloning](#) is making imposter scams more persuasive and harder to spot. While many of these warnings focus on consumer protection, the same deceptive techniques can be [repurposed for espionage](#): enabling adversaries to impersonate trusted voices, extract credentials,

or generate blackmail material through synthetic relationships and social engineering. These capabilities pose serious counterintelligence and operational security risks for the intelligence community and national security workforce.

Finally, AI accelerates the pace and scale of cyberattacks beyond what traditional, human-led defenses can manage. The NCSC's forward-looking [assessments](#) warn that AI is expanding attack surfaces and allowing adversaries to move faster through every stage of the attack lifecycle from reconnaissance to exploitation. Without comparable automation on the defensive side, detection and response will fall behind. Industry reporting echoes the concern: Microsoft's [2024 threat brief](#) highlights growing experimentation with AI by state actors, while recent guidance from [CISA](#) and [NSA](#) emphasizes the urgent need to secure AI-enabled systems not just from traditional breaches, but from model tampering and misuse that can be carried out at machine speed.

AI's democratization of capability, automated vulnerability discovery, personalization of deception, and machine-speed execution raise the baseline risk across U.S. networks. That reality makes recent rollbacks — reduced surge capacity, trimmed threat-hunting and analytics, and cuts to public-private coordination — especially shortsighted. The very institutions that translate intelligence into patches, maintain vulnerability catalogs, and coordinate incident response are now being outpaced by AI-enabled adversaries. In an era of autonomous offense, starving the sensors and switchboards that bind government and industry isn't fiscal prudence, but strategic risk.

## 4. The Urgency of Congressional Oversight

The degradation of America's cyberdefense capacity in the first 200 days of the current administration is not simply a matter of policy differences, but a constitutional issue. Congress has an explicit Article I responsibility to authorize and fund federal cybersecurity programs, and to ensure that those funds are used as intended. When the executive branch cuts, freezes, or refuses to execute congressionally mandated cyber programs, it is not only weakening national security; it is encroaching on the legislative branch's constitutional prerogatives.

In a rapidly escalating cyber threat environment, the stakes could not be higher. Cyber adversaries do not pause while Washington settles political scores. Congress must act to restore a bipartisan commitment to cyberdefense by using its most powerful tools: statutory authorities, appropriations, and rigorous oversight.

### 1. Reauthorize and strengthen core cyber authorities, backed by full funding

The Cybersecurity Information Sharing Act of 2015 (commonly called "CISA 2015") is set to expire at the end of September 2025. Congress should move quickly to reauthorize it by passing [S.1337](#),

a bipartisan bill led by Sens. Gary Peters (D-MI) and Mike Rounds (R-SD), along with its House companion [H.R. 5079](#). Reauthorization is essential to maintaining the legal framework for public-private collaboration and cyber threat intelligence sharing, core authorities underpinning CISA.

However, renewing these authorities alone will not sustain the nation's cyberdefenses. Congress must wield its Article I "power of the purse" to create, reinstate, and sustain federal cyber programs by providing explicit appropriations. Opportunities to do so must be extended across the interagency, from CISA and the FBI to the State Department and sector risk management agencies.

The FY26 budget process offers an immediate opportunity to exercise that power. The Trump administration's budget request proposed cutting CISA's funding by nearly one-third. In June 2025, the House Appropriations Committee scaled that back significantly, approving a [\\$2.7 billion allocation](#), which was still a reduction of roughly 4.6%. That was a positive step, but more could be done. The bill has yet to pass the House, and the Senate has not yet acted either. The final appropriations cycle will be critical for Congress to push back on harmful cuts, ensure that CISA and other agencies have the resources to carry out their mandates, and protect programs that remain at risk of elimination despite their central role in defending U.S. critical infrastructure.



***Congress has an explicit Article I responsibility to authorize and fund federal cybersecurity programs, and to ensure that those funds are used as intended.***

## **2. Enforce execution of appropriated funds and prevent executive overreach**

When an administration withholds, delays, or repurposes funding that Congress has already allocated — whether through staffing freezes, program shutdowns, "efficiency" mandates, or so-called "pocket rescissions" [a move that both the Government Accountability Office and Senate Appropriations Chair Susan Collins (R-ME) [have called illegal](#)], it undermines both cyber readiness and the separation of powers. Congress must demand transparency on staffing losses, program terminations, and unspent funds, and, where necessary, condition future appropriations on compliance with statutory mandates. Congress should hold hearings to compel the DHS, FBI, and

other agencies to account for attrition rates and mission impacts, ensuring the executive branch does not step over Congress’ constitutional role in directing national priorities.

### 3. Conduct targeted oversight after major cyber failures

When serious cyber incidents occur, oversight must be immediate and unflinching, especially when failures stem from leadership negligence or politically motivated interference. Incidents like “SignalGate” and the mishandling of classified cyberthreat briefings under officials such as Defense Secretary Hegseth require public inquiry. Hearings, inspector general reviews, and bipartisan fact-finding delegations should be used to identify root causes, recommend corrective measures, and hold accountable those whose actions — or inactions — imperiled national security.



***What lawmakers do in the coming months will determine whether the United States rebuilds its cyber posture — or hands victory to adversaries already working to exploit our divisions.***

### 4. Reaffirm the reality and severity of foreign malign influence operations

The threat of coordinated disinformation and cognitive warfare — particularly from China, Russia, and Iran — is neither hypothetical nor partisan. Cyber campaigns by our adversaries aim to fracture public trust, distort decision-making, and undermine democratic governance itself. Congress must publicly recognize these operations as national security threats, depoliticize their assessment, and ensure that agencies tasked with countering them have both the mandate and resources to act. Politicizing, ignoring, and downplaying such threats only serves the interests of America’s foes.

### 5. Protect the independence and integrity of cyber threat intelligence

Lawmakers need timely, unfiltered threat intelligence to respond to evolving dangers. Yet under this administration, signs of politicization are already surfacing. Director of National Intelligence Tulsi Gabbard’s new “Director’s Initiative Group” has [sought access](#) to agency chats and emails to use AI tools to flag employees deemed “disloyal,” and in late July, she released a lightly redacted, politically charged intelligence report challenging assessments of Russian interference [over CIA objections](#) about risks to sources and methods.

These actions do more than erode trust; they jeopardize diplomatic channels with intelligence partners and compromise the credibility of U.S. analysis. Congress should establish protected, direct reporting lines for cyber threat intelligence — insulated from political review or manipulation — to ensure accuracy, continuity, and timely action. Congress should also make explicit that national security professionals must not be fired, reassigned, investigated, or have their security clearances suspended or revoked for perceived disloyalty or for analytic judgments that diverge from political narratives; personnel actions must rest only on documented performance or adjudicated security risk. These safeguards would ensure that intelligence reaches key decision-makers and allies when it matters most, regardless of the ideological winds in D.C.

## **Conclusion**

Cybersecurity is not an executive branch prerogative but a national imperative and a constitutional responsibility. Congress must reassert its role by locking in authorities, enforcing the use of appropriated funds, demanding accountability for failures, and restoring the partnerships and intelligence flows that keep America's digital front lines secure. What lawmakers do in the coming months will determine whether the United States rebuilds its cyber posture — or hands victory to adversaries already working to exploit our divisions.





## **Acknowledgments**

This report was written by Liana Keesing and Lila Batcheller.

Design by Sydney Richards.

## **About Issue One**

Issue One is a leading crosspartisan political reform group in Washington, D.C. We unite Republicans, Democrats, and independents in the movement to fix our broken political system and build a democracy that works for everyone. We educate the public and work to pass legislation on Capitol Hill to bolster U.S. elections, build a healthier digital information environment for our democracy, improve the ability of Congress to solve problems, strengthen ethics and accountability, and limit the influence of big money over politics.

issueone.org | [in](#) | [✈](#) | [f](#) | [X](#)

## **Media Contact**

Cory Combs

ccombs@issueone.org | (202) 204-8553

