Testimony of Megan Stifel[1]

"Online Scams, Crypto Fraud, and Digital Extortion: An Examination of How Transnational Criminal Networks Target Americans"

Subcommittees on Border Security and Enforcement and Cybersecurity and Infrastructure Protection of the Committee on Homeland Security

April 21, 2026

Chairman Guest, Chairman Ogles, and Ranking Member Correa, thank you for the opportunity to testify today. I am Megan Stifel, Chief Strategy Officer at the Institute for Security and Technology[2] and Executive Director of the Ransomware Task Force.[3]

We are making progress in the fight against cybercrime. The national security threat posed by ransomware has decreased in the five years since we launched the Ransomware Task Force, thanks in part to the work of this committee. But we cannot rest on our laurels. Cyber fraud continues to cost our economy billions each year. Nation-state adversaries are leveraging the cybercrime ecosystem to target our critical infrastructure. And rapid advancements in the sophistication of artificial intelligence-enabled cyber tools threaten to erode many of the gains we've made in cybersecurity in the last few years.

Congress has a key role to play in consolidating the gains we've made, ensuring that we do not backslide, and preparing for the next iteration of the cyber threat. It is imperative that Congress pass a long-term—or even permanent—reauthorization of the information sharing authorities in the Cybersecurity Information Sharing Act of 2015. Similarly, Congress must do more to support vulnerable state and local governments, which are not equipped to combat foreign armies or transnational criminal organizations. This Committee, in particular, should continue its bipartisan oversight of the administration to ensure that CISA is able to carry out its mission in the face of significant cuts to its workforce.

Beyond the immediate changes needed, we must also look to the future. We will never achieve our strategic goals in cyberspace without moving upstream to make system-level changes. This requires a firm foundation for efforts like the Common Vulnerabilities and Exposures (CVE) Program, which help the entire ecosystem understand and defend against cyber threats. It demands more accountability for services, like residential proxy networks, that are regularly abused by criminals and nation-state adversaries. And achieving our strategic goals in cyberspace will never succeed without relationships among government

[1] I would like to thank Nicholas Leiserson and Sophia Mauro for their assistance in the preparation of this testimony. No AI assistance was used in developing this testimony.

[2] https://securityandtechnology.org/

[3] https://securityandtechnology.org/ransomwaretaskforce/

agencies and between the government and industry that are built on trust and emerge from truly collaborative engagements.

2026 is a decisive moment. We can see the potential opportunities and dangers from AI on the horizon, but there is still time to act. As Americans, what we need today more than anything is leadership. When we move decisively, we can seize the initiative from adversaries and materially change the cybercrime landscape. I hope today's hearing is an opportunity to jumpstart a new wave of bipartisan, effective, and transformative cybersecurity policy.

I. About IST

The Institute for Security and Technology (IST) is a 501(c)(3) charitable non-profit critical action think tank focused on the implications of technology for our national security. Home of the Ransomware Task Force, IST's cybersecurity program conducts applied research and policy development to address misaligned incentives in the technology ecosystem that leave critical infrastructure vulnerable. IST's current cybersecurity initiatives include:

- **UnDisruptable27** - Supported by Craig Newmark Philanthropies, UnDisruptable27[4] is focused on reducing our reliance on undependable technologies. Created in response to attempts by Chinese army units to hold U.S. critical infrastructure at risk,[5] UnDisruptable works with hospital communities to ensure the resilience of the water utilities they rely on against cyber attacks.
- **K-12 Cyber Defense Coalition** - With stakeholders ranging from chief state school officers to district IT administrators, the K-12 Cyber Defense Coalition[6] helps to drive state and local collaboration, policy development, and information sharing to defend our nation's schools from cyber threats.
- **Strengthening Information and Communications Technology** - One of the most effective interventions to improve cybersecurity is to ensure that software is secure by design. IST has published a comprehensive framework to strengthen and improve CISA's CVE Program[7] and recently published a guide for policymakers comparing international product cybersecurity regulations.[8]
- **Counter Ransomware Initiative Private Sector Advisory Panel** - The International Counter Ransomware Initiative (CRI),[9] created in 2021 and aligned with a Ransomware

[4] https://securityandtechnology.org/undisruptable27/
[5] https://chinaselectcommittee.house.gov/committee-activity/hearings/hearing-notice-the-ccp-cyber-threat-to-the-american-homeland-and-national-security
[6] https://securityandtechnology.org/blog/announcing-the-k12-cyber-defense-coalition/
[7] https://securityandtechnology.org/virtual-library/report/cve-at-a-crossroads/
[8] https://securityandtechnology.org/blog/who-sets-the-rules-the-imminent-gdpr-ification-of-product-cybersecurity/
[9] https://counter-ransomware.org/aboutus

Task Force recommendation, coordinates efforts to combat ransomware across more than 76 member states and organizations. IST is an inaugural member of the Private Sector Advisory Panel, which helps guide CRI activities.[10]

- **International Ransomware Task Forces** - In partnership with foreign governments and organizations, IST is adapting the Ransomware Task Force model in other countries to help them counter international criminal activity. Brazil recently completed its own task force sprint, and IST is currently working with the government of Mexico to stand up a task force of its own.[11]

II. The Cybercrime Threat Landscape

The cybercrime threat landscape is rapidly evolving. Extortion continues to be a major tactic, albeit one that increasingly involves the confidentiality of data, not just its availability. Criminals' reliance on common infrastructure, like residential proxy networks and certain domain registrars, present opportunities for disruption. Beyond extortion-based attacks, business email compromise causes billions in losses each year. Connections between nation-states and criminals persist. And exponentially increasing AI capabilities have the potential to upend the landscape as we know it.

A. Ransomware: From Encryption to Data Extortion

Thanks in part to changes in policy, including the elevation of ransomware to a matter of national security, we have seen significant shifts in the tactics of transnational cyber criminal organizations. Instead of targeting *availability* of systems or data, criminals are increasingly using extortion tactics to breach the *confidentiality* of data. To be clear, this is a better outcome for victims—and for our national security. However, the adaptability of these professional criminals, and their continued profitability, continues to pose a significant risk to the United States.

In order to understand the shift in cyber criminal tactics, one must start with the definition of "ransomware." According to CISA, "Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable."[12] Traditionally, ransomware operators have held data or systems hostage by encrypting them. In exchange for paying a ransom, they provided victims with a decryption key that, in some cases, allows for recovery of data or key system files and returns their information and communications technology to good working order.

[10] https://securityandtechnology.org/blog/ist-contributes-to-icri-for-fourth-year/
[11] https://securityandtechnology.org/blog/mexico-rtf/
[12] https://www.cisa.gov/stopransomware

Because traditional ransomware targets the availability of systems and data, it poses a significant threat to critical infrastructure. Ransomware attacks on pipelines or hospitals can force them to shut down, threatening the economy or even human lives. Refusing to pay can extend the time an enterprise is crippled, causing ripple effects throughout society.

The good news is that traditional ransomware attacks in the United States are on the decline. Across multiple data sets, we see a similar trend: "threat actors [are] shifting to exfiltration only without encryption."[13] Google Mandiant noted a nearly eight-fold increase in the number of data-theft-only extortion incidents they responded to over the past five years, and encryption dropped from being present in 39% of cases in 2024 to 31% in 2025.[14] In its 2025 ransomware survey, Sophos documented a five-year low in the number of incidents that resulted in actual encryption of data.[15]

The bad news is that criminals are adapting. Double-extortion schemes—once an unusual tactic in which ransomware actors steal data as well as encrypting it and then demand a second payment to keep it from being published—are now de rigeur. Google Mandiant, for instance, found that 77% of ransomware incidents in 2025 also involved data theft.[16] Criminals are also targeting smaller organizations[17] and shifting focus overseas. Last year, the United Kingdom suffered two significant ransomware-related incidents that cost the British economy billions.[18]

These trends carry important lessons for policymakers. Cybersecurity technologies, from endpoint detection and response tools to consistent data backups, can effectively prevent ransomware criminals from encrypting large quantities of data or allow for quick recovery if hit by an attack.[19] Coordinated law enforcement takedowns can significantly disrupt ransomware-as-a-service ecosystems, relegating once-prolific criminal groups to obscurity.[20] Ransomware payment rates are also falling to record lows, in part because data-exfiltration does not present the same degree of threat to business operations as encryption.[21]

---

[13] https://admin.bakerlaw.com/wp-content/uploads/2026/03/2026-DSIR-Report.pdf
[14] https://cyberscoop.com/google-threat-intelligence-group-ransomware-report-2026/
[15] https://assets.sophos.com/X24WTUEQ/at/gspkf9pb6jsvt4hrv2z8kjj/sophos-state-of-ransomware-in-enterprise-2025.pdf
[16] https://cloud.google.com/blog/topics/threat-intelligence/ransomware-ttps-shifting-threat-landscape
[17] Verizon, for instance, highlighted that ransomware was present in 88% of small and medium business breaches versus 39% of the entire sample studied. https://www.verizon.com/business/resources/T36/reports/2025-dbir-data-breach-investigations-report.pdf
[18] https://securityandtechnology.org/blog/a-category-three-cyber-hurricane-classifying-the-jlr-hack/
[19] https://www.coveware.com/blog/2026/2/3/mass-data-exfiltration-campaigns-lose-their-edge-in-q4-2025
[20] https://storage.ghost.io/c/af/a0/afa04ee3-414f-4481-8d23-7e7c146f192e/content/files/2026/03/2025YiR-report.pdf
[21] https://www.coveware.com/blog/2026/2/3/mass-data-exfiltration-campaigns-lose-their-edge-in-q4-2025

However, criminals are agile–and we cannot become complacent. Faced with lower profit margins, we've seen criminal groups implementing intermittent encryption in an attempt to avoid detection mechanisms.[22] We have also seen them targeting less capable cyber actors, like school systems and hospitals.[23] This can result in higher human costs, whether in the form of stolen sensitive data or disrupted services. Artificial intelligence tools also have the potential to turbocharge threats, automating significant portions of ransomware workflows.[24] To keep pace with the evolving threat, policymakers must maintain pressure by facilitating law enforcement takedowns while investing more in critical infrastructure below the security poverty line.[25]

B. The Infrastructure of Cybercrime: Proxies in Homes, Undisciplined Registrars

Cybercrime, particularly ransomware, has been professionalizing for the past decade.[26] Today, criminal enterprises cater to unique niches within the ransomware kill chain, from delivering initial access to a victim to helping to launder proceeds through cryptocurrency mixers. The growing specialization within the ransomware ecosystem reduces costs for criminals—one of the drivers of continued profits for transnational criminal organizations, even as payment rates continue to drop.[27] However, as with other complex supply chains, this interplay creates points of friction where disruptions can have significant impact on downstream criminal gangs.

At IST, we have been focusing on two specific enablers of ransomware and other cybercrime: residential proxy networks and digital infrastructure service providers.

Residential Proxies

Residential proxy networks (RPNs), in essence, act as an intermediary to hide the origin of internet traffic, passing messages on behalf of a sender to a receiver and then forwarding along replies.[28] Unlike other proxy networks, RPNs use home, small office, or mobile devices—and their associated Internet Protocol (IP) addresses—as the middleman in the connection.

---

[22] https://arxiv.org/pdf/2510.15133
[23] Although metrics vary, healthcare and government facilities consistently ranked as highly targeted sectors in 2025. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
[24] https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use
[25] https://www.scworld.com/podcast-segment/9082-the-security-poverty-line-part-1-wendy-nather-scw-60
[26] https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/behind-the-rise-of-ransomware/
[27] https://www.coveware.com/blog/2025/10/24/insider-threats-loom-while-ransom-payment-rates-plummet
[28] https://spur.us/blog/what-is-a-residential-proxy

Fueled by software development kits that come bundled with apps and browser extensions,[29] as well as pre-configured streaming devices like the Superbox,[30] RPNs are growing rapidly. While some users of RPNs rely on the networks to preserve their legitimate privacy interests, many others use them to scan and "scrape" the internet, attempting to avoid limitations put in place by service providers.[31]

Criminals are increasingly taking advantage of the deep and liquid market for these residential IP addresses to hide their attempts to gain access; exert command and control over compromised systems; and exfiltrate stolen data. In the week prior to the takedown of the IPIDEA RPN in January 2026, Google observed 550 different threat actors using that network to cover their tracks.[32]

Recently, RPNs have also been used by criminals to gain initial access into home networks. Through clever routing techniques, criminals can use a single residential proxy node (e.g., a laptop with a browser extension configured to join an RPN) to illuminate a home network and then compromise any vulnerable devices it finds on that network. The Kimwolf botnet enrolled over two million devices in a matter of weeks using this technique,[33] making it one of the fastest growing botnets of all time.

It is time for policymakers to take notice.[34] Because many residential proxy nodes are enrolled through quasi-legal means, such as disclosures buried in license agreements, there are limited paths for law enforcement or service providers to disrupt the networks. Without action, consumers will continue to be unwitting enablers of criminal or nation-state activity targeting critical infrastructure—and in the process, may be putting their own home devices and data at risk.

Domain Registrars

Last December, in partnership with the World Economic Forum, IST published a white paper proposing a systemic defense approach to fight cyber-enabled fraud.[35] In particular, I want to highlight one of the digital infrastructure services that is regularly being abused by ransomware actors and other cyber criminals: domain registrars.

---

[29] https://www.fbi.gov/investigate/cyber/alerts/2026/evading-residential-proxy-networks-protecting-your-devices-from-becoming-a-tool-for-criminals
[30] https://krebsonsecurity.com/2025/11/is-your-android-tv-streaming-box-part-of-a-botnet/
[31] https://www.cloudflare.com/press/press-releases/2025/cloudflare-just-changed-how-ai-crawlers-scrape-the-internet-at-large
[32] https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network
[33] https://krebsonsecurity.com/2026/01/the-kimwolf-botnet-is-stalking-your-local-network/
[34] https://securityandtechnology.org/blog/the-light-is-blinking-red-its-time-for-policymakers-to-wake-up-to-the-residential-proxy-threat/
[35] https://reports.weforum.org/docs/WEF_Fighting_Cyber-Enabled_Fraud_2025.pdf

Often described as the internet's phone book, the Domain Name System (DNS) translates domain names (e.g., www.house.gov) into IP addresses.[36] Governed by the Internet Corporation for Assigned Names and Numbers (ICANN),[37] DNS is one of the fundamental services that allows the internet to function. Its centrality is both a blessing and a curse: it also makes DNS a key avenue for cyber criminals to perpetrate fraud or gain unauthorized access to systems.

Malicious cyber actors often register domain names intended to trick users (e.g., by substituting a numeral '1' for a lowercase 'l'). The numbers are staggering, with over 8.6 million malicious domains used for intrusions in 2024. At the same time, an ICANN study of a sample set of domains registered by the approximately 3,000 accredited registrars in the system found that a mere 20 registrars were responsible for creating 84% of malicious domains.[38]

More must be done. Simple actions like limiting the bulk registration of domains to entities with an established reputation and doing basic due diligence to ensure there is an actual entity with a name that resembles a well-established brand could significantly increase the friction for criminals engaged in all manner of nefarious cyber activity. As with other threat vectors, the advent of agentic AI will likely exacerbate the problem, allowing criminals to accelerate malicious domain registration.

C. Business Email Compromise

Although not a focus of our work at IST, business email compromise (BEC) remains a key tactic for threat actors, causing significant damage to the U.S. economy. Per the FBI's latest Internet Crime Complaint Center Report, in 2025, more than 24,000 BEC incidents resulted in more than $3 billion in losses.[39] This contrasts with ransomware ($32 million in reported losses) and data extortion ($122 million) over the same time period. Even given the prevalence of under-reporting to the FBI (e.g., one cryptocurrency tracking firm estimated global ransomware payments to be just shy of $1 billion in 2025), BEC is an enormous problem.[40]

BEC occurs when a criminal gains unauthorized access to a business communications system, most often email.[41] They then use this access to initiate wire transfers or other

[36] https://www.icann.org/en/system/files/files/dns-infographic-13sep22-en.pdf
[37] https://www.icann.org/
[38] https://reports.weforum.org/docs/WEF_Fighting_Cyber-Enabled_Fraud_2025.pdf
[39] https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
[40] This is also borne out in cyber insurance claims data. https://cdn.intelligencebank.com/us/share/NMXD/aP6w/1413d/original/Coalition_2025-Cyber-Claims-Report
[41] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise

fraudulent payments from the business's account to an account that they control. While BEC is generally significantly less lucrative than a successful ransomware attack, it is also less technically complex to carry out.[42]

Because of the limited scope of unauthorized system access associated with BEC, it generally poses less of a national security risk than ransomware. However, even beyond the economic losses tied to this fraud, there are reasons for policymakers to focus on combatting it specifically.

Supply chains for BEC and more sophisticated cybercrimes overlap in a few key areas. Initial access brokers, who opportunistically gain access to organizations through exposed systems or compromised credentials, supply access to both ransomware operators and run-of-the-mill fraudsters.[43] Actors who create spoofed domains to deploy in phishing schemes can enable all types of cybercrime. Upstream disruption of these actors can undermine BEC. Conversely, taking down BEC crime rings can deprive cybercrime infrastructure providers of a revenue stream.

Mitigations against BEC can also prove effective in stopping ransomware. For instance, phishing-resistant multi-factor authentication (MFA) is a key control that can protect against all manner of cyber intrusions.[44] Policymakers can and should continue to emphasize the full range of consequences for failing to adopt foundational cybersecurity measures, whether encouraging voluntary uptake or implementing interventions, whether subsidies or requirements, to protect our homeland security.

D. The Nexus Between Nation States and Cyber Criminals

While the focus of this hearing is on transnational criminal organizations, committee members should also consider the nexus between more traditional nation-state threat actors and the cybercrime ecosystem.

When the Nation Is the Criminal

The Democratic People's Republic of Korea (DPRK) is widely regarded as the most successful cyber criminal organization in history.[45] DPRK hackers pioneered widespread deployment of

[42] https://www.verizon.com/business/resources/T36/reports/2025-dbir-data-breach-investigations-report.pdf
[43] https://www.darkreading.com/threat-intelligence/actions-to-take-to-defeat-initial-access-brokers
[44] https://www.cyber.gov.au/protect-yourself/securing-your-email/email-security/preventing-business-email-compromise
[45] https://msmt.info/view/save/2025/10/22/26294780-c396-407d-bb33-88afe988cd96-The_DPRK%E2%80%99s_Violation_and_Evasion_of_UN_Sanctions_through_Cyber_and_Information_Technology_Worker_Activities_(MSMT_2025_2).pdf

ransomware through the WannaCry attack in 2017.[46] In 2016, they targeted the SWIFT banking network, making off with tens of millions of dollars (but for a typo, they could have stolen ten times as much).[47] However, their greatest success has been in the theft of cryptocurrency, where their hacks have brought in billions of dollars.[48]

Policymakers should consider the implications of the North Koreans' success, especially as the proliferation of open-source artificial intelligence tools with significant cyber capabilities lurks on the horizon. According to estimates, as much as half of the DPRK's hard currency comes from cybercrime.[49] While it has taken significant investment—and experience—to build the DPRK's kleptocratic cyber teams, other pariah states could follow in their footsteps, particularly if AI lowers the barrier to entry.

Moonlighting

Even when regimes are not directly engaging in cyber theft, the individuals supporting their operations may be. Intelligence operatives from Russia[50] and China[51] have been implicated in "moonlighting" operations, where they leverage their skills to conduct criminal activities in their spare time. Iranian state cyber operatives have also been linked to ransomware and extortion campaigns.[52]

Foreign intelligence services also cultivate ties with criminal organizations or use them as buffers to disguise their true identity. Just last month, as part of its retaliatory cyber attacks on the U.S. homeland, the Iranian government used a hacktivist persona to take credit for the intrusions,[53] one of which knocked a U.S. medical device manufacturer offline for weeks.[54] The Department of Justice has alleged ties between the Russian government and the criminal hacktivist group the Cyber Army of Russia Reborn (CARR), which targeted operational technology in the U.S. and around the world following the 2022 Russian invasion of Ukraine.[55]

---

[46] https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
[47] https://www.bbc.com/news/stories-57520169
[48] https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/
[49] https://en.yna.co.kr/view/AEN20240321001100315
[50] https://www.justice.gov/archives/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions?
[51] https://services.google.com/fh/files/misc/apt41-a-dual-espionage-and-cyber-crime-operation.pdf
[52] https://www.cnn.com/2021/11/17/politics/us-iran-hackers-warning/index.html
[53] https://www.wired.com/story/handala-hacker-group-iran-us-israel-war/
[54] https://www.sec.gov/ix?doc=/Archives/edgar/data/310764/000119312526149607/d112875d8ka.htm
[55] https://www.justice.gov/opa/pr/justice-department-announces-actions-combat-two-russian-state-sponsored-cyber-criminal

These intersections point to the urgent national security need to crack down on cybercrime in all its forms. When it helps them gain the upper hand, adversaries have drawn—and will continue to draw—on criminal elements, particularly organized groups. Until we take decisive steps to improve our cybersecurity posture, disrupt cyber criminals, and dismantle their safe havens, our risk level will be unacceptably high.

Drawing on the Cybercrime Ecosystem

Finally, nation-states regularly take advantage of services offered as part of the broader cybercrime economy. As part of the IPIDEA takedown in January 2026, Google tracked espionage activities and groups from China, Iran, the DPRK, and Russia using the service.[56] DPRK state-sponsored thieves use cryptocurrency "mixing" services that are also core to transnational criminal organizations' attempts to launder their stolen funds.[57]

Adversarial nation-states also create demand for initial access through their contracting ecosystems. Individuals at two Iranian IT firms were indicted for building botnets on behalf of the government and using them to conduct distributed denial-of-service (DDoS) attacks on U.S. banks.[58] In April 2020, a Chinese national working for a PRC cyber contractor infected over 81,000 firewalls using a zero-day exploit. Many of the devices were then infected by ransomware.[59]

These cases illustrate the mutualism at play between nation-states and criminal syndicates. Sometimes, government demand creates the conditions for more criminal activity. Other times, criminals develop the business and later sell their wares to governments. In either case, disruptions to transnational criminal organizations have the potential to protect Americans both directly and indirectly: by reducing the victimization of people and organizations, and by reducing the capability and reach of nation-state adversaries.

E. Future Threats: Cybercrime in the Intelligence Age

The rapid development of large language models—and their proclivity for certain cybersecurity-related tasks—could significantly alter the cybercrime landscape over the next few years. We note four key areas to watch.

- **Analysis** - LLMs are already proving incredibly capable at processing and analyzing large volumes of data quickly. In an example earlier this year, AI appears to have helped sift through an enormous trove of data stolen from the Mexican government,

[56] https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network
[57] https://home.treasury.gov/news/press-releases/jy1087
[58] https://www.justice.gov/archives/opa/file/834996/dl?inline
[59] https://home.treasury.gov/news/press-releases/jy2742

producing more than 2500 structured intelligence reports.[60] In addition to changing how criminals target data going forward, attackers have also used AI tools to better monetize existing troves of stolen data.[61]

- **Automation** - Many aspects of the cyber kill chain are amenable to automation. We are already seeing LLMs generate context-sensitive phishing messages[62] (or web elements[63]) with the touch of a button. As with other industries, automating repetitive tasks could produce substantial productivity gains. For cyber criminals, this automation could increase their profitability, even if ransomware payment rates continue to decline.
- **Orchestration** - Last November, Anthropic released the first evidence of AI agents orchestrating the majority of a cyber intrusion.[64] In that particular instance, Anthropic was able to identify and stop the activity. However, the proliferation of agents capable of planning and executing intrusions on their own could cause the barriers to entry into cybercrime to crumble.[65]
- **Vulnerability Discovery** - AI companies have claimed that releasing the current best-in-class models would be dangerous because of their ability to exponentially accelerate the discovery and exploitation of novel vulnerabilities in code.[66] Right now, testing programs are underway to explore these capabilities. Should the core claims made by the companies prove true—or should models continue to progress to the point that they become true—the cybercrime landscape would be irrevocably altered. Cybersecurity has long relied on certain core assumptions, such as the difficulty of vulnerability discovery or that there is time between the announcement of a patch and exploitation at scale. The alleged capabilities of these best-in-class models would cause these assumptions to melt away.

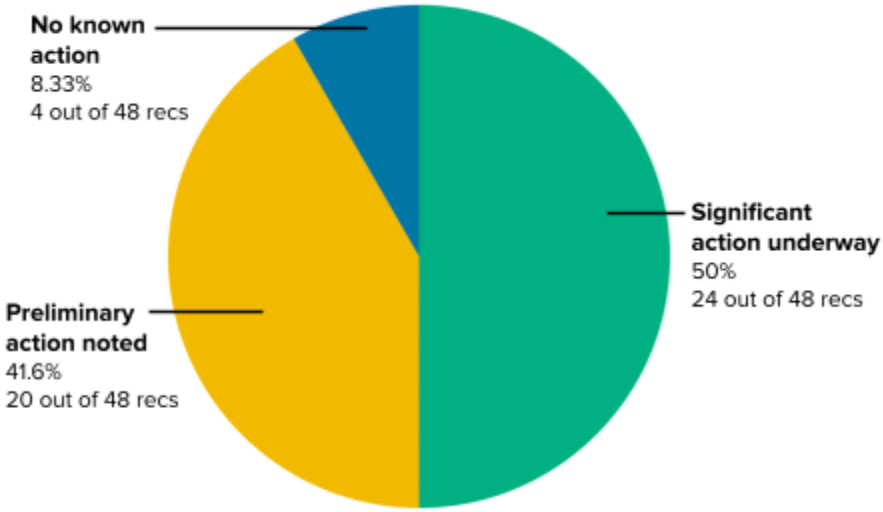
Policymakers should bear in mind that even though AI presents new offensive capabilities, it also creates opportunities for defensive applications. Over time, defensive uses of these technologies may end up dominating, driving down cybercrime. At the same time, even if the defensive uses wind up being superior, the tools will need to be distributed broadly, including to critical infrastructure providers and consumers who have not traditionally had access to cutting-edge cybersecurity products, in order for those benefits to be realized.

---

[60] https://gambit.security/blog-post/a-single-operator-two-ai-platforms-nine-government-agencies-the-full-technical-report
[61] https://www.anthropic.com/news/detecting-countering-misuse-aug-2025
[62] https://www.sciencedirect.com/science/article/pii/S2590005626000986
[63] https://unit42.paloaltonetworks.com/real-time-malicious-javascript-through-llms/
[64] https://www.anthropic.com/news/disrupting-AI-espionage
[65] https://securityandtechnology.org/wp-content/uploads/2024/10/The-Implications-of-Artificial-Intelligence-in-Cybersecurity.pdf
[66] https://www.anthropic.com/glasswing

III. The Ransomware Task Force Report at Five Years

Progress on RTF Recommendations as of April 2026



Released in April 2021, the Ransomware Task Force (RTF) Report is a seminal document that provides actionable recommendations for combating cybercrime across four phases: Deter, Detect, Prepare, and Respond. With participation from across government, industry, and civil society, RTF outputs have informed U.S. and international policy making and have served as a blueprint for private sector actors aiming to protect themselves from transnational criminal organizations.

As we mark the five-year anniversary of the release of the RTF report and its 48 recommendations, we have several observations:[67]

- **There's been significant progress, but it has slowed**. Since our last assessment of progress against the RTF recommendations,[68] two have moved from preliminary action to significant action. Specifically, the insurance industry has seen progress through consortia like CyberAcuView,[69] which is making it easier to understand claims data in aggregate (Recommendation 2.1.7). The government also continues to map the ransomware ecosystem, including supporting infrastructure, and is now regularly using this knowledge to inform takedowns and sanction activities.
- **Several recommendations await final action by the government**. Implementation of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), championed by

[67] For a full accounting of progress against the RTF recommendations, see: https://securityandtechnology.org/wp-content/uploads/2026/04/April-2026-RTF-Progress-Report.pdf
[68] https://securityandtechnology.org/wp-content/uploads/2024/10/April-2024-RTF-Progress-Report-Doubling-Down.pdf
[69] https://cyberacuview.com/

many members of this committee, remains stalled more than four years after its passage (Recommendations 4.2.2, 4.2.3, and 4.2.4).[70] With a final CIRCIA rule in place, we would have a better operational understanding of the ransomware ecosystem and the ability to more easily offer assistance to victims.

- **For the first time, we've seen backsliding**. Since our assessment in April 2024, two of our recommendations have moved from significant action back to preliminary action. Notably for this committee, the failure to fund the state and local cyber grant program since its original appropriation lapsed last year leaves governments at significant risk from ransomware and other cyber intrusions (Recommendation 3.4.2).[71] While this committee has made strides in advancing a long-term reauthorization of the grant program,[72] without funding, states will remain exposed. The Cyber Response and Recovery Fund, authorized in 2021 in response to RTF recommendations, may also be at risk; the January House-passed Homeland Security appropriations bill would have transferred all of the money from this emergency account to base CISA appropriations (Recommendation 4.1.1).[73]
- **Limitations on ransom payments remain underdeveloped**. Of the four RTF recommendations where we have seen no action, three pertain to pre-ransom payment activities, such as conducting a cost-benefit analysis (Recommendation 4.3.2). The record-low ransom rates may open up space for more conversations on how to limit payments, which are the fuel for the entire ecosystem. However, absent strong leadership from policymakers to act as a catalyst, we are unlikely to see significant progress.

On balance, the success of RTF members and partners in implementing recommendations has had a significant impact on the ransomware ecosystem, including driving criminals to pursue alternative, non-encryption-based extortion methods. Key to our approach was starting with a comprehensive strategy that addresses all phases of the challenge and providing clear recommendations to specific actors. We also favored system-level approaches that affect the root causes of cybercrime, rather than trying to treat its symptoms. Finally, we could not have succeeded without deep collaboration with industry. Civil society organizations like IST have a vital role to play as a neutral convener and accelerant to policy engineering projects; however, effectuating real and lasting change requires bringing both government and industry perspectives to the table.

[70] https://www.federalregister.gov/documents/2026/02/13/2026-02948/cyber-incident-reporting-for-critical-infrastructure-act-circia-rulemaking-town-hall-meetings
[71] https://www.nascio.org/wp-content/uploads/2026/02/NASCIO-Advocacy-Priorities-2026_a11y_SLCGP.pdf
[72] https://www.congress.gov/bill/119th-congress/house-bill/5078
[73] https://docs.house.gov/billsthisweek/20260119/Homeland26_01_xml.pdf

RTF Recommendations with Changes Since April 2024

#	Description of RTF Recommendation	Changes since April 2024
2.1.7	Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management.	Significant action underway. The insurance industry has seen progress through consortia like CyberAcuView, which is making it easier to understand claims data in aggregate.
2.3.2	Create target decks of ransomware developers, criminal affiliates, and ransomware variants.	Significant action underway. Recent takedown activity has targeted ransomware-as-a-service and the entire ecosystem, in coordination with industry and international partners.
3.4.2	Expand Homeland Security Preparedness Grants to encompass cybersecurity threats.	*Reversal of significant progress.* The State and Local Cybersecurity Grant Program is currently defunded.
4.2.1	Establish a Ransomware Incident Response Network (RIRN).	*Reversal of significant progress.* The RIRN is defunct, and there is still inconsistent sharing of incident reports across jurisdictions. However, agreements like the initiative between the Department of Homeland Security and DG Connect are indicators of preliminary action aligned with this recommendation.

No known action | Preliminary action noted | Significant action underway

IV. Federal Government Headwinds

Recent actions by the administration have emphasized the importance of countering cybercrime. However, challenges with the federal workforce, funding, and organizational upheaval all threaten to limit progress, as does a strategic approach overly focused on disruption.

A. Continued Emphasis on Disruption…

On March 6, the President released the 2026 Cybersecurity Strategy.[74] Although it lacks specific mention of ransomware, it does highlight the significant challenges cybercrime poses to the U.S. economy and calls for the continued disruption of criminal infrastructure. In tandem with the Strategy's release, the President also signed Executive Order 14390,

[74] https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf

"Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens,"[75] which addresses the damage that cybercrime, including ransomware, is inflicting on U.S. citizens. In particular, EO 14390 focuses on government efforts to disrupt transnational criminal organizations responsible for cybercrime and fraud.

As noted in the RTF report (and echoed in Pillar I of the 2026 Cybersecurity Strategy and Pillar II of the 2023 National Cybersecurity Strategy[76]), disrupting threat actors is an essential component of a comprehensive effort to improve our cybersecurity posture. Disrupting infrastructure raises the costs of crime, while arrests and indictments undermine criminals' faith in each other and in the underground economy.

EO 14390 appropriately views disruption through a wide lens that encompasses "operational, technical, diplomatic, and regulatory" approaches. The continued prevalence of Russian-speaking ransomware gangs,[77] for example, speaks to the need for all countries, including the United States, to call on Russia to uphold its commitments to prevent its territory from being used for damaging cyber attacks.[78] Without sustained diplomatic pressure from the plethora of countries that fall victim to Russian cyber criminals, disruption at the level of individual threat actors will remain challenging.

On the operational front, the first 15 months of the administration have seen a steady drumbeat of law enforcement operations targeting cyber criminals and their enabling infrastructure.[79] The Department of the Treasury's Office of Foreign Assets Control has utilized new authorities under the Protecting American Intellectual Property Act to go after exploit brokers selling dangerous offensive cyber tools to criminals.[80] I look forward to observing implementation of the forthcoming action plan associated with this latest EO, particularly the details on how an operational cell at the National Coordination Center plans to continue increasing the pressure on transnational cyber criminal organizations.

---

[75] https://www.whitehouse.gov/presidential-actions/2026/03/combating-cybercrime-fraud-and-predatory-schemes-against-american-citizens/

[76] https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[77] https://www.trmlabs.com/resources/blog/crypto-crime-in-russia-ransomware-sanctions-evasion-and-disinformation

[78] https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

[79] https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation; https://www.justice.gov/usao-edmi/pr/fbi-disrupts-virtual-money-laundering-service-used-facilitate-criminal-activity; https://www.fbi.gov/contact-us/field-offices/atlanta/news/fbi-atlanta-indonesian-authorities-take-down-global-phishing-network-behind-millions-in-fraud-attempts; https://www.justice.gov/opa/pr/united-states-leads-dismantlement-one-worlds-largest-hacker-forums

[80] https://home.treasury.gov/news/press-releases/sb0404

B. ...But Without Broader Systemic Interventions

I would like to focus on two key challenges with the administration's approach to date. First, the resources that our federal agencies rely on to combat cybercrime have been significantly pared back. And second, the strategic approach does not appear to balance the need to deter individual actors with other systemic steps to make ransomware and cyber-enabled fraud less achievable.

Dealing with Federal Cybersecurity Cuts

Public reporting indicates CISA has lost one third of its workforce,[81] an issue that this committee has raised during oversight hearings.[82] While the cuts have been pitched as returning CISA to its core mission,[83] this is clearly not the case in practice. The Critical Infrastructure Partnership Advisory Council, a core mechanism for coordinating cybersecurity policy across government and industry, has yet to restart since being shuttered last March.[84] What's more, should the Secretary of Homeland Security decide to convene sector-specific advisory committees, coordination will be a challenge given cuts to CISA stakeholder engagement personnel. In an effort to fill some of the gaps left from these cuts, the Acting CISA Director recently announced a hiring sprint to bring on new talent to help protect the nation from the many threats arrayed against us. This quick reversal in hiring practices is clear evidence that the original cuts were too deep.[85]

Cuts to key cyber personnel are not confined to DHS. As discussed in a Senate hearing last year, budget cuts to the FBI's cyber division were expected to reduce personnel by half.[86] Faced with an eight percent cut in personnel, the acting commander of USCYBERCOM testified that the effect on the command's ability to carry out its mission would be "impactful."[87] The Government Accountability Office found in a report last September that 22 of the 23 agencies surveyed failed to fully account for their cyber workforce needs, so the full scope of the personnel cuts remains nebulous.[88] And in the foreign policy arena, the dissolution of significant portions of the State Department's Cyberspace and Digital Policy Bureau,[89] despite its clear statutory mandate,[90] also risks delaying decisive action. EO 14390

[81] https://www.cybersecuritydive.com/news/cisa-departures-trump-workforce-purge/749796/
[82] https://homeland.house.gov/hearing/oversight-of-the-department-of-homeland-security-cisa-tsa-st/
[83] https://securityboulevard.com/2025/04/homeland-secretary-noem-vows-to-put-cisa-back-to-focusing-on-its-core-mission/
[84] https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac
[85] https://federalnewsnetwork.com/cybersecurity/2026/03/cisa-eyes-plan-for-more-than-300-new-hires/
[86] https://cyberscoop.com/senators-fbi-director-patel-clash-over-cyber-division-personnel-arrests
[87] https://breakingdefense.com/2025/08/after-cuts-to-dods-cyber-workforce-experts-see-short-term-readiness-risks-but-also-opportunity/
[88] https://www.gao.gov/products/gao-25-107405
[89] https://www.politico.com/news/2025/07/17/cyber-tech-state-ai-00460679
[90] 22 USC 2651a

sets an ambitious schedule for developing an action plan to follow through on its objectives, but it's unclear what personnel from across the interagency will be able to put it together, much less execute against it.

Funding cuts also threaten progress in the fight against cybercrime. As documented by this committee, the State and Local Cybersecurity Grant Program proved effective in marshaling resources to help state, local, Tribal, and territorial governments improve their defenses;[91] yet it has been zeroed out in the administration's budget. Shared cybersecurity services provided at subsidized rates for state and local governments through the Multi-State Information Sharing and Analysis Center (MS-ISAC) have also been canceled, leaving states to scramble for protection.[92] Ironically, both programs would have helped achieve the objective laid out in EO 14390 to "provide training, technical assistance, and resilience building to support State, local, Tribal, and territorial (SLTT) partners, including to expand defensive capacity, share threat intelligence, and harden SLTT partners' critical infrastructure systems against cybercrime exploitation by TCOs."

The transnational nature of cybercrime makes funding for international cybersecurity capacity-building particularly important, yet programs that aim to bolster international cyber capacity, too, have been cut.[93] Without investments in foreign partners' cybersecurity programs, the ability of the Secretary of State to, per EO 14390, "coordinate [U.S.] actions with allies and partners to enhance the consequences of actions taken against nations that tolerate predatory activity" will be significantly diminished.

Finally, organizational challenges will add further friction to the administration's activities. More than a month after the release of the 2026 Cybersecurity Strategy, there has been no additional information regarding an implementation plan with specific actions for agencies to take to achieve its objectives. There has also been no executive action clarifying the National Cyber Director's role in interagency cybersecurity discussions, raising questions about whether the Director or the National Security Advisor is ultimately responsible for strategic direction.

Stepping into the leadership void, the Director of the Office of Management and Budget (OMB) issued guidance eliminating a common cybersecurity form for contractors.[94] Rather than requiring contractors to fill out a single attestation in order to sell products to the entire

---

[91] https://homeland.house.gov/hearing/cybersecurity-is-local-too-assessing-the-state-and-local-cybersecurity-grant-program/
[92] https://www.cybersecuritydive.com/news/ms-isac-loses-federal-funding-cyber-impacts/761367/
[93] https://www.thecipherbrief.com/column_article/usaid-cuts-demolish-cyber-assistance-to-u-s-allies-and-partners
[94] https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf

government, OMB now encourages agencies to develop their own policies and forms—in seeming contravention of the strategy's mandate to streamline regulation.

Striking the Right Balance

The administration's focus on disrupting cybercrime is admirable. However, it leans too heavily on "offensive" solutions at the expense of system-level "defensive" changes that will help to bolster cybersecurity across the nation. As I wrote in the weeks leading up to the strategy's release:

> "A strategy that prioritizes shaping behavior through offensive operations over improving defense would risk exposing critical infrastructure, intellectual property, and U.S. companies to even greater harm. True national security comes not from striking first, but from leveraging innovation to significantly reduce the security gaps available to attackers, empowering industry to take lawful, coordinated actions, and realigning incentives in the marketplace to support secure software and hardware practices."[95]

At IST, we view cybersecurity challenges, including cybercrime, as primarily a matter of misaligned incentives. In stark contrast to defense of our land, air, and maritime borders, government neither claims nor aims to have a degree of operational control over the cyber domain to stop all incoming attacks. Instead, in cyberspace, government must also rely on the private sector actors that operate our networks and maintain our critical infrastructure to ensure our national security. Unfortunately, the market forces that act as operating constraints on businesses often do not align with national security interests.

The incentives that dominate technology marketplaces instead drive suppliers to produce and sell technology that prioritizes speed-to-market and features over security, resilience, and reliability. Similarly, for users of technology, markets regularly reward purchasing and operating behaviors that serve to weaken an entity's cybersecurity posture.

Aligning incentives so that the private sector, positioned on the proverbial "front lines," goes from being a national security liability to an asset is a considerable challenge. Markets reward behavior detrimental to societal interests for a number of reasons, from the externalization of costs of crime to the lack of empirical examples of large-scale disruptive or destructive cyber attacks that could help participants price risk. This lack of realizable costs is weighed against very clear benefits, such as more agility and lower development and operational costs.

[95] https://nexusconnect.io/articles/imminent-national-cyber-strategy-may-lean-on-offense-at-the-expense-of-defense

However, broad-based efforts to create incentives for cybersecurity behaviors that benefit society as a whole can be very rewarding. Injecting national security considerations into technology markets simultaneously addresses a root cause cybersecurity challenge and creates structures that can adapt as new categories of technological innovation and reliance emerge. Making meaningful progress on incentives creates downstream impact that addresses issues across the technology ecosystem and maximizes the benefits of the effort invested.

In our work at IST, we address three broad categories of cybersecurity challenge:

- **Critical infrastructure security and resilience** - For schools, water utilities, and hospitals, there is not sufficient funding to support cybersecurity practices to help these organizations withstand threats from transnational criminal organizations or nation-states. As a result, we focus on designing efficient programs (like the Federal Communications Commission's E-Rate cybersecurity pilot[96]) to subsidize necessary cybersecurity investments where they are needed most. Chairman Ogles's PILLAR Act is an excellent example of this kind of intervention.
- **Designing and deploying secure information and communications technology and services (ICTS)** - Addressing ICTS security is inherently high-leverage: preventing one single vulnerability in a product before it is shipped to market can save thousands of entities from having to apply millions of patches. When we invest in security by design,[97] develop recommendations to prevent misuse of domain registration,[98] or work to protect the open-source software that underpins so much of our society,[99] we are applying solutions that actually address the systemic problem, not the proximate cause. Ranking Member Thompson's focus on ensuring the CVE Program thrives[100] is aligned with this type of intervention.
- **Building public-private partnerships to disrupt malicious cyber actors** - Disruption remains a core pillar of our work. In particular, we examine incentives that will bring government and non-government partners together, as both have the resources necessary, whether authorities, information, or technical acumen, to effectively conduct takedowns. Our international tabletop exercises strengthen relationships that

[96] https://securityandtechnology.org/wp-content/uploads/2025/07/Cybersecurity-Considerations-for-Universal-Service-Fund-Reform_Final.pdf
[97] https://www.lawfaremedia.org/article/f5--solarwinds--and-the-lethargy-of-the-far-council
[98] https://securityandtechnology.org/virtual-library/report/fighting-cyber-enabled-fraud-a-systemic-defense-approach/
[99] https://securityandtechnology.org/wp-content/uploads/2023/04/Castles-Built-on-Sand.pdf
[100] https://democrats-homeland.house.gov/news/correspondence/ranking-members-thompson-and-lofgren-request-gao-review-of-cve-and-nvd-federal-cybersecurity-programs

lead to joint-sequenced operations.[101] This committee's relentless efforts to reauthorize CISA 2015 is another example of this kind of work.[102]

The administration's focus on disruption is therefore necessary, but not sufficient. I hope that subsequent executive actions will address the broader market incentives that create the conditions for mass exploitation and victimization of Americans. I also hope that the administration reverses cuts and policy changes that make it more difficult to alter these incentives.

V. Recommendations for Congress

Congressional leadership has always been essential for advancing cybersecurity policy. Despite the progress we have made in tackling cybercrime, nation-state threat actors have gotten bolder, and AI cyber tools risk upending the landscape entirely. Lapses in authorizations and appropriations also put hard-won advances at risk. This committee should:

- **Authorize key programs to ensure they are not interrupted** - Several DHS and CISA programs have faced disruption over the past 15 months, in part because they are not explicitly authorized in law. By laying out clear goals and expectations in statute, Congress can put these programs on firmer footing and ensure their future success. Key programs include:
    - **The Common Vulnerabilities and Exposures (CVE) Program** - CVE records act as the universal identifiers for weaknesses in computer code. This essential program, which is relied on by companies in every sector and worldwide, needs a more effective, multistakeholder governance model and a clear delineation from other programs like the National Institute for Standards and Technology's National Vulnerability Database.[103] This committee should advance legislation codifying the program in a way that avoids fragmentation (i.e., other countries or entities setting up competing programs).
    - **The Critical Infrastructure Partnership Advisory Council (CIPAC)** - It is essential that non-federal critical infrastructure owners and operators have mechanisms to offer candid feedback to their U.S. government partners with respect to cybersecurity and resilience policy. This committee should advance legislation amending Section 9002 of the Fiscal Year 2021 National Defense Authorization Act to codify the CISA Director's ability to convene critical

[101] https://securityandtechnology.org/virtual-library/report/cri-tabletop-exercise-after-action-report/
[102] https://homeland.house.gov/hearing/in-defense-of-defensive-measures-reauthorizing-cybersecurity-information-sharing-activities-that-underpin-u-s-national-cyber-defense/
[103] https://nvd.nist.gov/

infrastructure providers, rather than relying on the broad authority of the Secretary of Homeland Security.

- **Pass long-term (or permanent) extensions of cybersecurity authorities** - This committee has produced effective legislation that has improved the nation's cybersecurity posture; it should not be allowed to expire. In particular, Congress should reauthorize:
    - **The Cybersecurity Information Sharing Act of 2015**, which expires on September 30, 2026, and which enables the free flow of cyber threat indicators among the private sector and between the private sector and government.
    - **The State and Local Cybersecurity Improvement Act of 2021**, which expires on September 30, 2026, and which provides assistance to state, local, Tribal, and territorial governments to develop and execute against strategies to improve their cybersecurity.
- **Strengthen the ability of private sector and government actors to work together to disrupt cyber threats** - In furtherance of the goals laid out in EO 14390, this committee can take steps to incentivize deeper collaboration through joint sequenced operations and other efforts to degrade cyber threat actors. The committee can achieve this by:
    - **Authorizing the Joint Cyber Defense Collaborative (JCDC)** - JCDC has yet to live up to the full potential envisioned by the Cyberspace Solarium Commission.[104] Authorization for the JCDC should lay out clear criteria for participation and metrics for success, as well as the types of whole-of-nation plans and campaigns the center should develop.
    - **Directing the Secretary of Homeland Security, acting through the CISA Director, to clarify lawful defensive measures that private-sector actors can take when countering ransomware or other cybercrime** - One key obstacle to a higher tempo of private sector-enabled takedowns, as identified by the RTF report, is legal ambiguity about which defensive measures are allowed under existing law, including the Cybersecurity Information Sharing Act of 2015. The committee should direct the CISA Director to work with industry and the interagency in developing and publishing guidance that clarifies what constitutes a defensive measure.
- **Continue to conduct effective oversight and exploratory hearings** - There are several topics that fall under the committee's jurisdiction that are ripe for additional committee activity, including:
    - **Residential proxy networks** - Despite being used by cyber criminals, fraudsters, and even advanced persistent threats, the enrollment of everyday

[104] https://www.lawfaremedia.org/article/making-joint-cyber-defense-collaborative-work

consumer devices into residential proxy networks appears to be legal. In exploring policy solutions to this issue, committee members may also wish to investigate whether regulations like the Digital Markets Act[105] are impairing the ability of tech companies to effectively govern their app stores.

- **The Cyber Response and Recovery Fund (CRRF)** - Created in the Bipartisan Infrastructure Law nearly five years ago,[106] the CRRF has still never been used to respond to a significant incident. The committee should conduct rigorous oversight to understand what processes have been put in place to expeditiously employ the CRRF and what policy decisions have been made by the executive branch that have prevented its use. This is particularly timely, as the CRRF expires in just over two years.
- **The rise of product security regimes** - IST recently published a report highlighting opportunities for international convergence on product cybersecurity regimes, whether voluntary or mandatory.[107] The report notes that, while few of the regimes are fully implemented today, that will not be the case by the end of next year. Congress should take this opportunity to explore different approaches and how they will affect products sold to U.S. businesses and consumers. Committee members may also wish to examine how product cybersecurity approaches can map to AI tools.
- **Measures to disincentivize extortion payments** - With ransomware and related payments on the decline, there is no better time to explore mechanisms to further disincentivize payments—or at least help authorities better track criminals' financial infrastructure when a payment is made. These could include requirements to coordinate with law enforcement or to explore alternatives before paying extortionists.[108]
- **The effect of AI on vulnerability disclosure** - Over the last six months, vulnerability disclosure programs have seen massive increases in the number of reports they receive.[109] As AI drives the marginal cost of filing a report to zero, this may invalidate core assumptions about vulnerability management, including norms surrounding coordinated vulnerability disclosure. Committee members may wish to explore the effects of the changing vulnerability disclosure landscape on federal systems and on operational technology used by critical infrastructure.

---

[105] https://digital-markets-act.ec.europa.eu/index_en
[106] https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf
[107] https://securityandtechnology.org/virtual-library/report/comparative-analysis-of-product-cybersecurity/
[108] For more thoughts on pre-conditions for a ransomware payment ban, https://securityandtechnology.org/virtual-library/memo/roadmap-to-potential-prohibition-of-ransomware-payments/
[109] https://www.cybersecuritydive.com/news/cve-program-ai-vulnerability-reports-funding/815594/

- **Work closely with other committees on broader cybersecurity issues** - House rules limit the ability of any one committee to comprehensively address cybersecurity issues. Building on the legacy of leadership from Congressman McCaul and Ranking Member Thompson, committee members should provide thought leadership by working with:
    - **The Committee on Appropriations**, particularly with respect to funding the State and Local Cybersecurity Grant Program. Even with its temporarily extended authorization, no funds are currently appropriated to support this program.
    - **The Committee on Financial Services**, to help accelerate the uptake of cyber insurance, including by exploring different backstop mechanisms to stabilize the market in the event of a systemic incident.[110] As a market-based way of pricing risk, insurance has the potential to drive positive cybersecurity improvements throughout the economy.
    - **The Committee on Energy and Commerce**, to support Universal Service Fund reforms to allow schools (and potentially hospitals) to purchase cybersecurity products and services with E-Rate funds.[111] This work is complementary to this committee's work with SLTT governments.
    - **The Committees on Armed Services; Energy and Commerce; and Intelligence**, to address the "Salt Typhoon" incidents targeting U.S. telecommunications infrastructure.[112]

There is a lot of work for Congress to do, but I have faith that the leaders on this committee will continue to prioritize cybersecurity as an urgent, non-partisan issue at the heart of our national security. At IST, we welcome the opportunity to continue to engage with you and your colleagues to support this crucial work. Thank you again for the invitation to testify.

[110] https://www.fdd.org/analysis/2025/06/17/how-a-government-reinsurance-program-can-accelerate-maturation-of-the-cyber-insurance-market/
[111] https://securityandtechnology.org/blog/including-cybersecurity-in-the-e-rate-and-rural-healthcare-programs/
[112] https://securityandtechnology.org/blog/congressional-oversight-on-salt-typhoon-missing-an-opportunity/