STATEMENT FOR THE RECORD

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEES ON BORDER SECURITY AND ENFORCEMENT AND CYBERSECURITY AND INFRASTRUCTURE PROTECTION

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

Tuesday, April 21, 2026 | 10:00 a.m.

TESTIMONY OF

CYNTHIA KAISER

Senior Vice President, Halcyon Ransomware Research Center

Former Deputy Assistant Director, FBI Cyber Division

I. Introduction

Chairman, Ranking Member, and distinguished Members of the Subcommittees: thank you for the opportunity to appear before you today. My name is Cynthia Kaiser. I currently serve as Senior Vice President of the Halcyon Ransomware Research Center, where my team tracks, analyzes, and publishes research on ransomware actors and their impact on American society. Before joining Halcyon, I spent two decades at the Federal Bureau of Investigation, most recently as Deputy Assistant Director of the FBI Cyber Division. I have dedicated my career to understanding and dismantling the criminal networks that target our citizens, our institutions, and our way of life.

I appear today representing Halcyon, a cybersecurity company whose mission is to defeat ransomware—the most disruptive and dangerous form of cybercrime afflicting America today. I commend this Committee for convening this hearing. The President's recent Executive Order 14390 on Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens correctly identifies these threats as top-tier national security concerns and calls for a whole-of-government response. I am here to reinforce that call, ground it in data, and offer concrete ideas for what more we can and must do.

I want to begin with a statement that I believe this Committee, and every American, should hold in mind throughout this hearing: the people perpetrating these crimes are not merely technical actors engaged in financial misconduct. They are predators. They are callous. They are, in many cases, knowingly endangering and ending human lives—and they do not care. This Committee has the power to ensure that they face serious consequences for the harm they chose. For the harm they have caused.

II. The Scale and Human Cost of Cybercrime Against Americans

The FBI's Internet Crime Complaint Center released its 2025 Internet Crime Report earlier this year. The picture it paints should make every American angry—and I mean genuinely, viscerally angry. Let me walk you through why.

In 2025 alone, cybercriminals stole over $20 billion from Americans. That is not a Pentagon budget line or an abstract economic figure—it is a generation worth of wealth: retirement savings wiped out, small businesses destroyed, families left without resources they spent a lifetime building. Over 75,000 Americans were victimized by sextortion schemes last year. During a single FBI operation described in that report, 38 victims were referred to an FBI Victim Specialist for suicide intervention. Thirty-eight people so devastated by cybercrime that agents feared victims would take their own lives.

Ransomware is growing in size and in ability. We know that reports to FBI only represent a fraction of attacks and crime against US organizations and citizens. Even so, ransomware attacks reported to the FBI have increased by over 20 percent since 2023.

Attacks that used to take weeks, now take just a few hours. AI has made it a lot easier for our adversaries to lie, and they are tricking more and more people into giving them access to company networks. Thousands of US businesses are attacked every year, and private sector data indicates that ransomware gangs target small and medium-sized businesses four times as often as large organizations.

The even sharper increase that FBI reported in ransomware attacks against critical infrastructure is especially worrisome. Last year, healthcare overtook all other critical sectors to become the single most targeted industry for ransomware. Attacks against hospitals and medical facilities nearly doubled, from 238 attacks in 2024 to 460 in 2025. Attacks against critical manufacturing and financial services also hit record highs, each increasing by close to 40 percent. Criminal organizations focused on these sectors because of deliberate strategic choices they made to maximize harm and maximize payment.

I want the Members of this Committee to sit with that healthcare number for a moment: 460 ransomware attacks on American hospitals and health systems in a single year. That is more than one attack every single day, targeting the places Americans go when they are most vulnerable—when they are giving birth, receiving cancer treatment, or fighting for their lives in an emergency room.

A. These Adversaries Are Making Deliberate Choices to Target the Vulnerable

When ransomware gangs shifted their targeting to hospitals, it was not an accident. It was a business decision. Ransomware actors—who are criminal entrepreneurs as much as they are hackers—have calculated that hospitals, facing life-or-death consequences for every minute of downtime, are more likely to pay ransoms than other targets. They are explicitly leveraging the fragility of human health to maximize their profits.

Healthcare was once considered an informal off-limits target even within criminal ransomware communities. That is no longer the case. These actors have looked at children in NICUs, at dialysis patients, at trauma centers serving rural communities where the next nearest hospital is 70 miles away—and they have decided those patients are acceptable collateral damage, even useful leverage. That is more than just recklessness. It is a moral choice. And I think we can all agree: it is one of the most reprehensible moral choices a person can make.

Research published by the University of Minnesota, linking a database of hospital ransomware attacks to Medicare claims data, found that ransomware attacks on hospitals caused at least 47 deaths between 2016 and 2021. That number is certainly higher today. When a hospital is taken offline, ambulances are diverted. Labs are shuttered. Surgeries are postponed. For a heart attack or stroke patient, the difference of even one hour in receiving treatment can mean death or permanent disability. The hackers responsible for these attacks know this. They are not naïve. They have simply decided that these deaths are someone else's problem.

If a contractor knowingly tampered with the medical equipment of critically ill patients to extort money from a hospital, we would not debate what degree of crime had been committed. We would prosecute them to fullest extent of the law. Perpetuating this type of attack on a computer does not change the crime, and it should not change the punishment.

III. Ransomware is Organized, Professional, and Without Moral Constraint

I want to address something that I believe is sometimes lost in the technical and policy discussion about cybercrime: the character of the people doing these acts.

The most active ransomware groups—Akira, Qilin, INC, Play, and others identified in the FBI's 2025 report—operate like businesses. They have HR processes. They have branding. Some have customer service lines for victims trying to negotiate ransom payments. They are organized, professional, and utterly without moral constraint when it comes to the harm they cause.

Our grandparents, our small businesses on Main Streets, our doctors—none of them should live in fear about what someone might be doing on a keyboard thousands of miles away.

But the current legal and policy response does not consistently reflect that reality. The FBI and its partners are doing extraordinary work with the authorities they have. But the gap between the severity of these crimes and the consequences that follow needs to close.

The Halcyon Ransomware Research Center identified 70 new ransomware variants last year alone—on top of 67 identified by FBI the year before. Criminal ransomware ecosystems are adaptive, decentralized, and self-replenishing. Two of last year's new groups, Lynx and Dragonforce, rose within months to become among the highest-volume ransomware operators worldwide. When law enforcement dismantles one group, others fill the void unless we are also raising the cost and risk of entry into this business. We are not doing that sufficiently today.

IV. The President's Executive Order and National Cyber Strategy: A Strong Foundation

Executive Order 14390, signed March 6, 2026, reflects a welcome and necessary escalation of the federal government's commitment to fighting cybercrime. The Order correctly identifies ransomware and cyber-enabled fraud as activities carried out by Transnational Criminal Organizations (TCOs)—many of which operate with the willing or tacit support of foreign regimes—and directs a coordinated, whole-of-government response.

Several elements of the Order are particularly significant. The directive to develop an action plan identifying specific TCOs and proposing solutions to prevent, disrupt, investigate, and dismantle them reflects the kind of targeted, intelligence-driven approach that has proven effective against other serious criminal enterprises. The creation of an operational cell within the National

Coordination Center to synchronize federal disruption efforts is a meaningful structural step. And the International Engagement provisions—which direct the Secretary of State to demand enforcement action from nations harboring cybercriminals and to coordinate sanctions, visa restrictions, and trade penalties with allies—address one of the core structural enablers of ransomware: the impunity enjoyed by criminals operating in permissive jurisdictions.

The new National Cyber Strategy reinforces this by elevating ransomware and cybercrime to top-tier national security threats and articulating six pillars for action. I was particularly encouraged by the Strategy's framing around shaping adversary behavior. The only way to address the societal, business, and technical threats posed by ransomware is to raise costs and inject uncertainty into criminal ecosystems at the same time that we put the technical tools in place to kick them off victim networks and slam the doors behind them.

The Executive Order and Strategy together create a strong policy foundation. Now we must build on it.

V. Using Existing Authorities in Novel Ways to Stop the Worst Actors

The federal government has more tools available than it is currently using at full force against the most dangerous ransomware actors. I want to highlight three areas where I believe existing authorities could be applied more aggressively and creatively, and where I urge this Committee to provide support and, where necessary, legislative clarification.

A. Terrorism Designations for Those Who Target Hospitals and Critical Infrastructure

The federal definition of terrorism under 18 U.S.C. § 2331 includes "violent acts or acts dangerous to human life" that "appear to be intended to intimidate or coerce a civilian population." Under 8 U.S.C. § 1182(a)(3)(b), terrorist activities include "seizing or detaining, and threatening to kill, injure, or continue to detain" a person "in order to compel a third person" to act as a condition for release.

When a ransomware gang encrypts a hospital's systems and demands payment under threat of continued system lockout—knowing that patients are being diverted, that dialysis is being delayed, that surgery schedules are being canceled—I believe a serious legal argument exists that this conduct falls within those definitions. At minimum, it merits a formal, deliberate analysis by the Departments of State, Justice, and Treasury, who collectively hold designation authority under Executive Order 13224.

I am not alone in this view. John Riggi, the National Advisor for Cybersecurity and Risk at the American Hospital Association, has testified before Congress that ransomware attacks targeting hospitals should be investigated with the same urgency as terrorism. The Director-General of the World Health Organization has briefed the UN Security Council that these attacks "at worst... cause patient harm and death." U.S. and French ambassadors at that same session emphasized the escalating harm.

I want to be direct about what terrorism designations would and would not accomplish. They are not a cure-all. They would not capture every ransomware actor. Nor should they. The deliberative designation process led by the State Department is designed precisely to ensure we act surgically. But for the most egregious actors—those who knowingly and repeatedly target hospitals, who have caused documented patient deaths, who operate at scale against the institutions that keep Americans alive—terrorism designations would unlock a powerful set of

additional tools: asset freezing, heightened Intelligence Community collection authorities, expanded travel restrictions, and significant diplomatic consequences for nations harboring these individuals.

We should also begin a national conversation—one I would urge this Committee to facilitate—about whether potential gaps in cyber insurance coverage caused by terrorism designation triggers could be addressed through the Terrorism Risk Insurance Act framework when Congress considers reauthorization in 2027. The goal is not to punish victims. It is to ensure that the most dangerous actors in the ransomware ecosystem face consequences proportionate to the harm they cause.

B. Murder and Manslaughter Charges Where Attacks Cause Death

Under federal law, the felony murder rule allows a defendant to be charged with first-degree murder when they commit a dangerous felony that results in another person's death, even if they did not cause the death directly. Under New York law, a defendant can be charged with second-degree murder when, "under circumstances evincing a depraved indifference to human life," they "recklessly engage[] in conduct which creates a grave risk of death to another person, and thereby cause[] the death of another person."

The University of Minnesota study I referenced earlier documented at least 47 deaths attributable to hospital ransomware attacks between 2016 and 2021. As ransomware attacks on healthcare have nearly doubled since that study's endpoint, the true number of lives lost to this crime is almost certainly in the hundreds. Federal prosecutors should be empowered—and encouraged—to evaluate whether homicide charges are appropriate in cases where ransomware actors targeted hospitals, where deaths resulted, and where the actors demonstrated clear foreknowledge that their actions endangered life.

This is not a theoretical exercise. Consider what happened just two months ago, on February 19, 2026, when ransomware actors struck the University of Mississippi Medical Center. UMMC is not simply a large hospital. It is the medical backbone of an entire state: Mississippi's only academic medical center, operating seven hospitals and 35 clinics statewide, and home to the state's only Level 1 trauma center, only children's hospital, and only organ and bone marrow transplant program. When attackers took down UMMC's network—knocking Epic, its electronic health records system, fully offline and forcing clinical staff to revert to pen and paper—they did not merely disrupt a business. They degraded the emergency medical capacity of an entire state. Clinics closed across Mississippi. Outpatient surgeries and cancer treatment appointments were canceled. For nine days, the state's only facility equipped to handle the most severe trauma cases operated under manual downtime procedures, with staff tracking patient care, medications, and orders on paper. Nearby hospitals reported surging emergency department volumes as they stepped in to absorb patients UMMC could not fully serve.

As the American Hospital Association's John Riggi noted in response to the attack, disruptions like this are especially dangerous in rural states where the next nearest trauma center may be over 100 miles away. The hackers behind the UMMC attack knew exactly what they were targeting. They contacted the hospital afterward with demands. They understood they had taken down a system that Mississippi patients depend on for survival—and they used that leverage deliberately.

Campbell County Health in Wyoming offers another instructive example: its entire hospital network was crippled for over two weeks, forcing emergency patients to be transferred across distances of 70 miles for eight hours while its single emergency department was offline. The link

between these interruptions and patient mortality is documented in the peer-reviewed literature. The Executive Order directs the Attorney General to pursue the "most serious, provable offenses" arising from cybercrime. Homicide charges in appropriate cases would be consistent with that directive—and would send a signal to ransomware actors that is long overdue.

C. Sanctions and Treasury Authorities Against Ransomware Financial Infrastructure

The ransomware economy depends on a financial infrastructure: cryptocurrency exchanges, money laundering networks, and payment processors that move ransom proceeds across borders. The Treasury Department's Office of Foreign Assets Control has used sanctions authority to designate ransomware actors and the exchanges that service them. I urge this Committee to support the expansion of that program, in alignment with the Executive Order's international engagement provisions.

Blockchain tracing by firms like TRM and Chainalysis shows that annual ransomware payments, while down from their 2023 peak, remain at well over $800 million. Disrupting the financial ecosystem that makes ransomware profitable—through expanded sanctions, cooperation with foreign financial intelligence units, and pressure on cryptocurrency infrastructure providers—remains one of the highest-leverage interventions available to the government. The International Counter Ransomware Initiative, now comprising over 60 nations, provides a ready-made multilateral framework for coordinating these actions.

VI. Recommendations for This Committee

I offer the following specific recommendations for this Committee's consideration:

- Direct the Departments of State, Justice, and Treasury to formally evaluate and report back to Congress on whether existing terrorism designation authorities under Executive Order 13224 can be applied to ransomware actors who knowingly target hospitals and critical life-safety infrastructure.
- Request a report from the Department of Justice on the feasibility and appropriateness of pursuing homicide charges in cases where ransomware attacks on healthcare facilities resulted in documented patient deaths.
- Encourage the Attorney General to issue guidance making clear that cyber-enabled attacks with life-safety consequences will be prosecuted using the most serious applicable charges, consistent with the directive in Executive Order 14390 to pursue the most serious provable offenses.
- Support the full funding and reauthorization of the State and Local Cybersecurity Grant Program. State and local governments are disproportionately targeted by ransomware, and they often lack the resources to defend themselves. Governments and government services was the fourth most targeted sector in 2025. Cutting this funding would be a gift to ransomware criminals.
- Convene a Congressional working group, including representatives from the insurance industry, to evaluate amendments to the Terrorism Risk Insurance Act ahead of its 2027 reauthorization that would address cyber terrorism, ensuring that terrorism designations for ransomware actors do not inadvertently harm victims who need insurance coverage to recover.

- Work with the National Security Council to ensure that federal cybersecurity experts are meaningfully integrated into the terrorism designation review process when ransomware actors targeting healthcare are under consideration.

VII. Conclusion

The people running ransomware organizations that target American hospitals are not mysterious hackers operating in a moral gray zone. They are criminals who have made deliberate choices. Choices to target the sick, the vulnerable, the elderly, and the newborn, because they have calculated that doing so maximizes their profits. They have no shame about this. They have demonstrated, repeatedly, that they will not stop unless we make stopping necessary.

The FBI and its federal partners are doing everything they can with the authorities they currently have. I know this from the years I spent working alongside those agents. But the worst of the worst—those targeting healthcare, those who have caused documented deaths, those operating with impunity under the protection of hostile foreign governments—deserve to face consequences that match the gravity of what they have done.

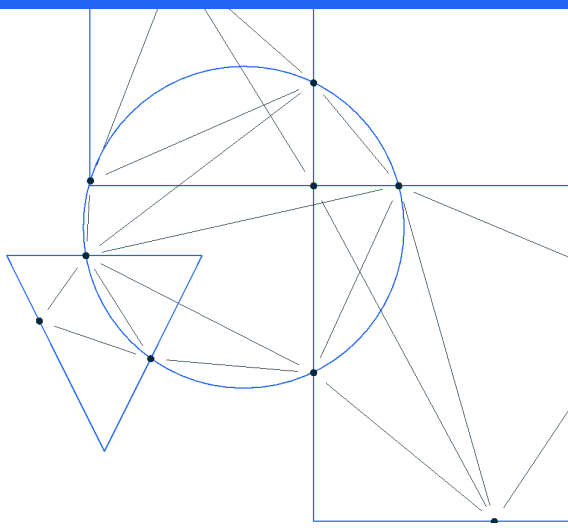
The President's Executive Order has given us a mandate. The National Cyber Strategy has given us a framework. This Committee has the power to sharpen both, fill the gaps, and send a message to the criminal ecosystem that America is no longer willing to treat ransomware as merely a cost of doing business in the digital age.

These hackers are counting on us to respond with incremental measures. I urge you to prove them wrong.

I thank the Subcommittees for this opportunity and look forward to your questions.

Cynthia Kaiser
Senior Vice President, Halcyon Ransomware Research Center
Former Deputy Assistant Director, FBI Cyber Division
Submitted: April 21, 2026

TRM



Testimony of Ari Redbord, Global Head of Policy, TRM Labs

Joint Hearing of the Subcommittee on Border Security and Enforcement and the Subcommittee on Cybersecurity and Infrastructure Protection

April 21, 2026

Introduction

Chairs Guest and Ogles, ranking members Correa and the ranking member of the Subcommittee on Cybersecurity and Infrastructure Protection, and distinguished members of both subcommittees, my name is Ari Redbord. I am honored to appear before you on behalf of TRM Labs, where we work every day with law enforcement, financial institutions, and national security agencies to detect, investigate, and prevent illicit activity in the digital asset ecosystem and beyond.

Before joining TRM, I spent more than a decade as a federal prosecutor at the United States Department of Justice and later served as a senior official at the US Treasury Department's Office of Terrorism and Financial Intelligence. In those roles, I confronted terrorist financiers, sanctions evaders, narcotics trafficking organizations, and transnational criminal enterprises operating across jurisdictions and continents.

I do not say this lightly: I have never seen a financial crime threat as pervasive, as economically destructive, or as dangerous to ordinary American families as the one I am here to describe today.

I want to begin with something that I think gets lost in the conversation about transnational criminal organizations. We talk about TCOs operating from compounds in Southeast Asia. We talk about Chinese underground banking networks processing hundreds of billions of dollars. We talk about North Korean hackers operating thousands of miles away.

All of that is real, and I will address each of those threats in detail.

But I want this committee to understand who is actually being harmed. It is a grandmother in Ohio who sent tens of thousands of dollars to someone she believed was her grandson in distress, only to learn it was a scammer exploiting her trust. It is a 40-something in North Carolina who believed she had found both a relationship and an investment opportunity, after months of daily communication, and lost everything he had, including money borrowed from her parents. It is a veteran in Texas who transferred his home equity to what he believed was a legitimate investment platform after weeks of engagement with someone posing as a trusted advisor. It is a family in New York whose life savings were gone in 72 hours, moved across seven cryptocurrency wallets in three countries before they even realized what had happened.

These are not victims of some distant financial abstraction. They are our constituents, and the criminal networks that target them are sophisticated, well-resourced, and operating at industrial scale against the American public.

We need to get this right — and we need to do it together — because these are not abstract losses, they are life savings, homes, and futures of Americans, and the networks taking them are organized, relentless, and scaling faster than our response.

About TRM Labs

TRM Labs is a blockchain intelligence company that works with hundreds of financial institutions, cryptocurrency businesses, and law enforcement and national security agencies worldwide. Our AI-powered platform allows investigators to follow illicit money wherever it moves, tracing cryptocurrency transactions through wallets, exchanges, mixers, and cross-chain bridges to help investigators build investigations and mitigate risk.

We also publish original research on crypto crime trends, threat actor behavior, and the evolving intersection of digital assets and national security, including the annual TRM Crypto Crime Report, which serves as a foundational resource for policymakers, law enforcement, and compliance professionals worldwide.

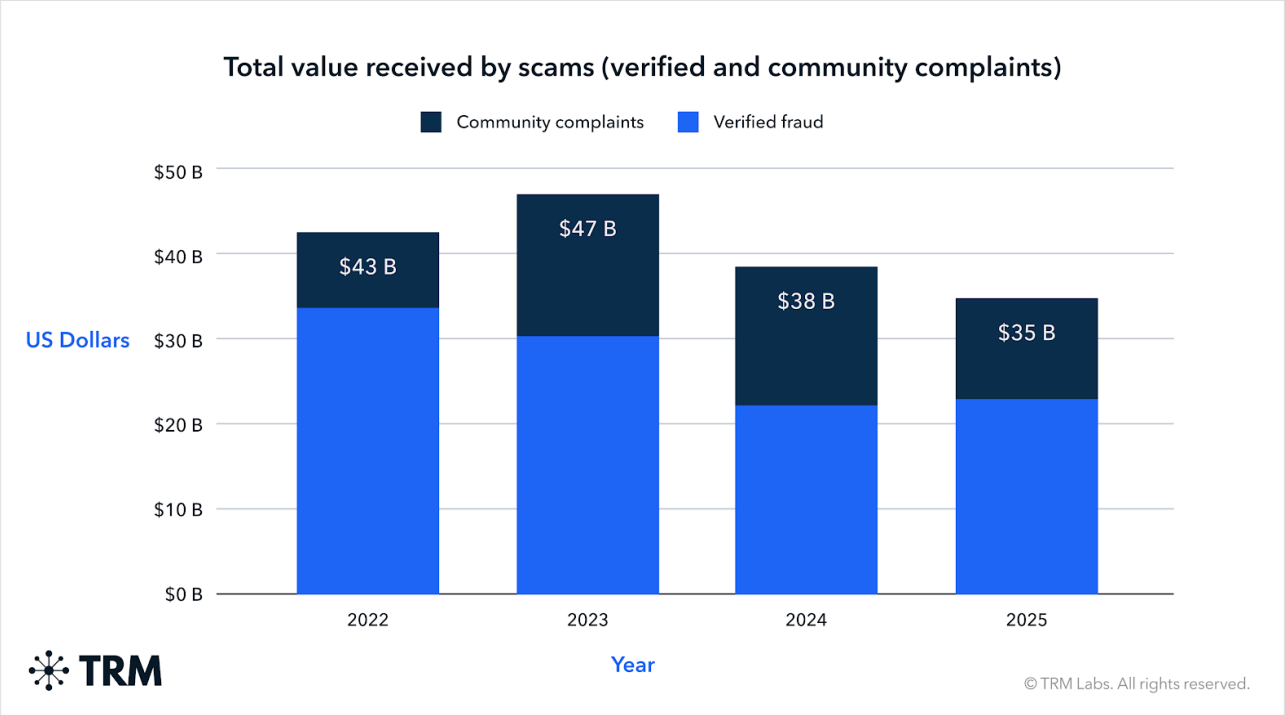
I want to be clear about what blockchain intelligence actually provides in the context of the threats before this committee. When a victim of a pig butchering scam sends cryptocurrency to a fraud platform, that transaction is recorded on a public, permanent, immutable ledger.

The wallet that received those funds can be traced. The subsequent movement of those funds through additional wallets, exchanges, and obfuscation techniques can be followed with the right tools and training. Unlike cash, which disappears into the financial system anonymously, cryptocurrency leaves a trail. The challenge is not that the evidence does not exist. The challenge is that law enforcement, financial institutions, and policymakers do not always have the tools, the legal authority, or the coordination frameworks to act on that evidence fast enough to matter.

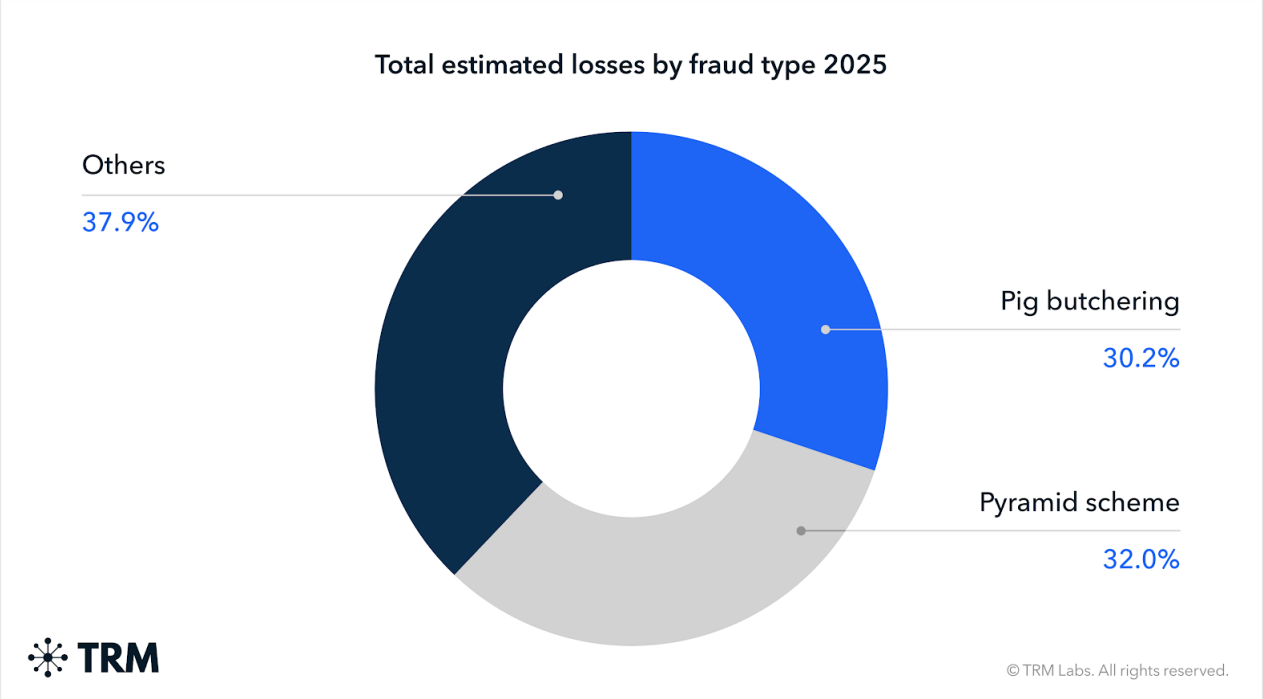
The scope of the problem

TRM's 2026 Crypto Crime Report documented approximately USD 158 billion in illicit cryptocurrency flows in 2025 — a 145% increase from USD 64.5 billion in 2024 and the highest level recorded in five years. Fraud and scams alone accounted for roughly USD 35 billion in confirmed flows to fraud-linked wallets.

The FBI's Internet Crime Complaint Center has documented record losses from cyber-enabled fraud, with investment fraud and romance scams representing the fastest-growing and most devastating categories of victim harm. But those figures capture only what victims report. TRM estimates that only about 15% of victims come forward — deterred by shame, skepticism that law enforcement can help, or simple uncertainty about where to turn. When that underreporting gap is factored in, global annual losses from cyber-enabled fraud against individuals likely exceed USD 200 billion.



Verified fraud activity from TRM Labs and Beacon Network, as well as alleged fraud activity sourced from Chainabuse, a victim reporting platform.



But scams are only one category of illicit activity driven by transnational criminal networks. Sanctions evasion, driven largely by Russia-linked activity and the rapid growth of the

ruble-pegged stablecoin A7A5, surged over 400% year over year. Cryptocurrency stolen through hacks reached USD 2.87 billion across nearly 150 incidents in 2025, with North Korea responsible for USD 1.92 billion of that total.

How transnational criminal organizations operate

Pig butchering and scam centers

The dominant fraud typology driving the losses I have just described is commonly known as pig butchering, a term originating from the Chinese phrase "sha zhu pan," which describes the practice of "fattening" a victim financially before the slaughter. Understanding how these operations actually work is essential to understanding both the scale of the problem and the nature of the policy response required.

These operations begin with weeks or months of deliberate, patient relationship-building — conducted over messaging apps, dating platforms, social media, and even text messages sent to wrong numbers — a technique criminals use to establish initial contact. The operator, often working from an organized compound staffed by hundreds of people, establishes genuine emotional connection with the target before any financial matter is raised. Victims describe feeling that they had found a genuine friend, romantic partner, or trusted mentor.

Only after that relationship has been cultivated does the operator introduce investment, typically framed as an opportunity being shared out of personal generosity. Victims are shown a professional-appearing trading platform, given access to fabricated account dashboards showing growing returns, and permitted to make small early withdrawals to establish credibility. When the victim has committed the maximum available funds, including frequently borrowed money or retirement savings, the platform disappears. Customer service stops responding. The money is gone.

What is critical for this committee to understand is that these operations are not the work of individual grifters. They are organized enterprises operating with the discipline and infrastructure of multinational corporations.

The compounds in Myanmar, Cambodia, and Laos are large physical facilities, some housing thousands of workers. In many documented instances, those workers are themselves victims of human trafficking, recruited with false promises of legitimate technology or hospitality jobs and held under threat of violence, debt bondage, or confiscation of passports.

The networks running these compounds are affiliated with Triad-connected organized crime syndicates that have operated in Southeast Asia for decades, and they have brought to cyber fraud the same organizational sophistication they applied to narcotics, gambling, and human trafficking operations. The business model is extraordinarily efficient. Operating costs are low, victim conversion rates are measurable and optimizable, and the proceeds are laundered

through established underground banking networks that have moved value across borders for generations.

Investigating pig butchering

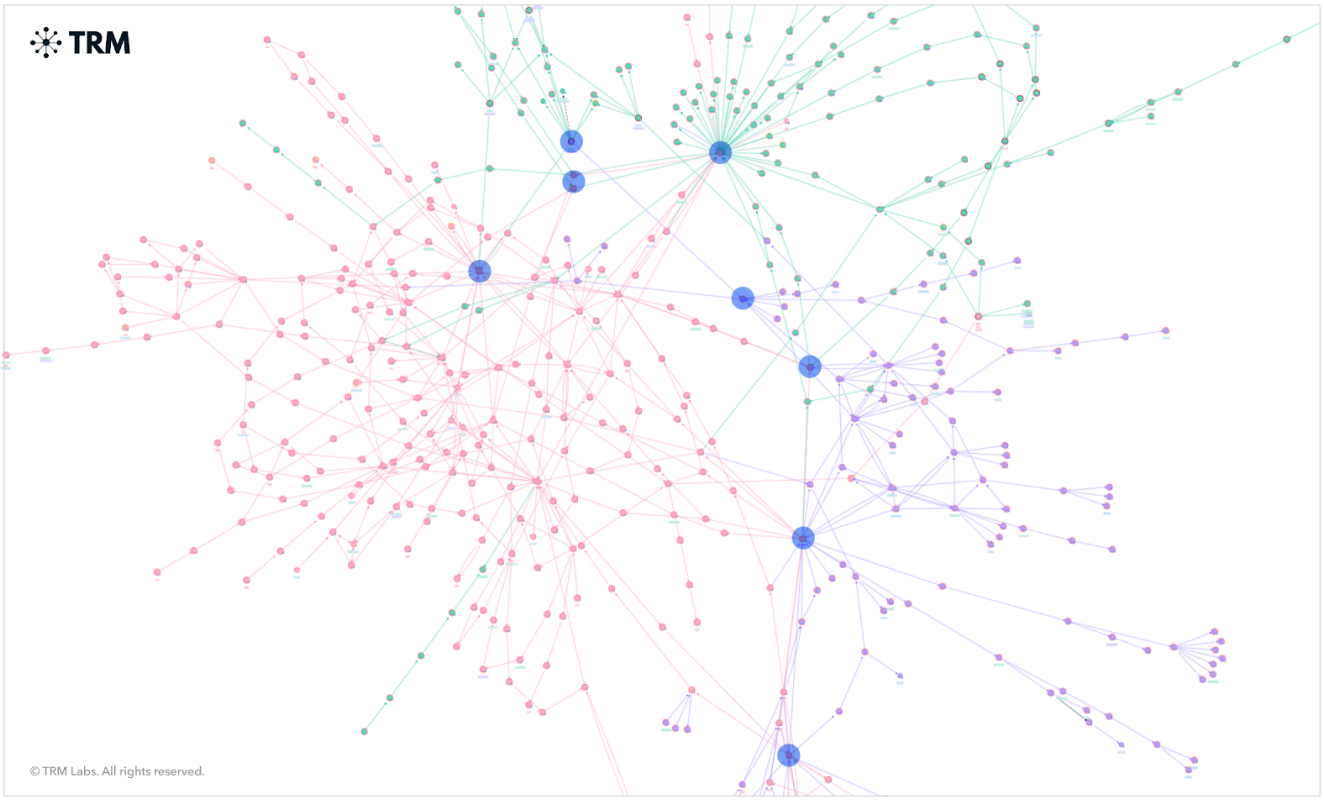
Investigations involving networks of scammers are often complex. TRM's analysis of on-chain transaction data, combined with proprietary source intelligence, has identified several key characteristics of pig butchering scams.

Once cryptocurrency reaches a scammer's wallet, it is typically shuffled from wallet-to-wallet in a complex web of transactions between scammers and money launderers (sometimes the same people), with each wallet accumulating funds from additional victims along the way. Funds often move circuitously, making it difficult for investigators to follow the money and to separate victim funds from other tokens. These fund movements consistently include multiple hops through intermediary addresses.

Victim funds typically end up reaching a few main exchanges, where they are often swapped for stablecoins before continuing to be cycled through the money laundering network both via the main exchanges and unhosted wallets.

TRM data indicates that cryptocurrency wallets that receive victim funds from individual pig butchering scams are also often associated with other scams. Furthermore, in a random sample of addresses to which victims stated they sent funds, over 75% exhibited signs of sophisticated on-chain money laundering activity.

The below graph illustrates a typical example of a pig butchering scheme studied by TRM Labs, showing the interconnected networks spanning multiple scams. Each color represents the scammer addresses in three different cases. As shown by the connections between the three coloured webs, the scammers appear to be operating multiple scams either in succession or in conjunction. In addition, the scammers appear to be relying on the same underlying money laundering network, with the same addresses appearing in multiple cases.



This TRM graph illustrates a typical example of a pig butchering scheme showing the interconnected networks spanning multiple scams.

Chinese money laundering networks

The proceeds of pig butchering operations, narcotics trafficking, and every other major illicit finance stream documented by TRM flow through the same critical infrastructure: Chinese underground banking networks that have become the dominant professional money laundering system in the world.

TRM's Shadow Bankers report documented that Chinese-language escrow and money laundering networks processed over USD 103 billion in 2025, growing from approximately USD 123 million in 2020. That growth reflects both the explosion of cryptocurrency as a settlement mechanism and the organizational sophistication of the networks operating them.

These underground banking systems operate through what are known as mirror exchange arrangements. A broker collects cartel cash in the United States and provides equivalent value through off-record methods to a counterpart in Mexico or elsewhere, keeping dollars in the United States and making value available abroad without any cross-border wire transfer occurring. Cryptocurrency has made these arrangements faster and cheaper.

Brokers coordinate through encrypted messaging applications like WeChat and Telegram, using code words and cultural reference points that exploit the language and cultural barriers

facing Western law enforcement. Transactions are layered through mixers, cross-chain bridges, privacy coins, and rapid micro-transactions across multiple blockchains to break investigative trails.

These networks do not exclusively serve one criminal constituency. They serve Mexican cartels laundering narcotics proceeds, North Korea converting stolen cryptocurrency to usable currency, pig butchering fraud operators moving victim funds to safety, Russian sanctions evaders moving value outside the traditional financial system, and Iranian actors funding weapons procurement networks.

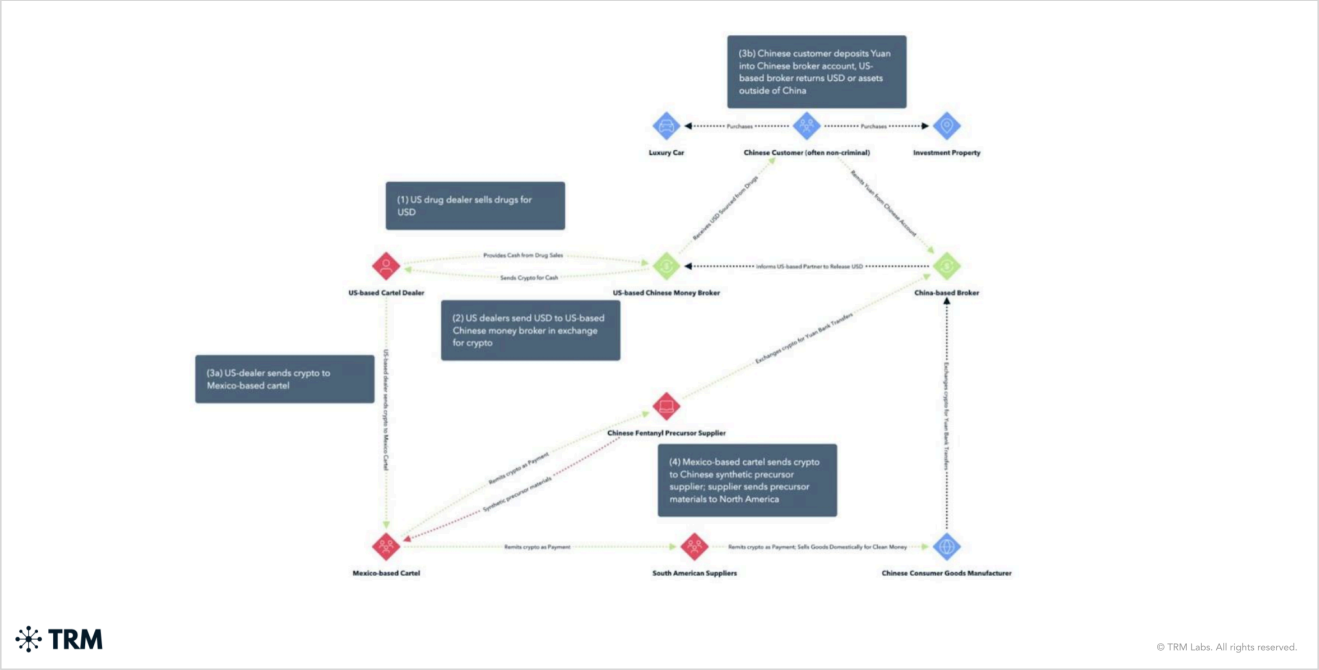
In one documented case that TRM tracked, a Los Angeles-based operation laundered over USD 50 million in Sinaloa Cartel narcotics revenue through Chinese underground bankers using trade-based schemes layered with cryptocurrency transactions. The same brokers who handled that transaction were handling fraud proceeds from Southeast Asian scam operations. The financial infrastructure of transnational crime is not siloed by crime type. It is shared, interconnected, and mutually reinforcing.

FinCEN's designation of Huione Group (a Cambodia-based network) as a primary money laundering concern in 2025 identified that organization as receiving USD 39.6 billion in transaction volume. That single designation illustrates the scale at which these networks operate and the degree to which they have become embedded in the global financial system.

Mexican cartels and the southern border

Over the last few years, the cartels have integrated cryptocurrency into their operations; the connection to the southern border is direct and concrete. TRM research on cartel cryptocurrency use documented that of more than 120 Chinese companies supplying precursor chemicals for fentanyl and methamphetamine production, 97% were willing to accept cryptocurrency payments.

Mexican cartels, including the Sinaloa Cartel and its affiliated networks, are using cryptocurrency to purchase the chemical inputs for fentanyl production from Chinese suppliers to compensate workers and operatives across multiple jurisdictions, and to launder drug proceeds through layered wallet transactions and Chinese underground banking arrangements.



TRM Graph Visualizer, with explanations, showing how the cartels and Chinese brokers use cryptocurrencies to launder drug money.

These are not isolated transactions. They are systematic. In June 2024, a Department of Justice indictment charged Edgar Joel Martinez-Reyes with leading a network that used trade-based money laundering and cryptocurrency purchases to clean drug proceeds, with law enforcement seizing USD 5 million in cash and significant drug quantities in connection with that case. In January 2024, Martin Mizrahi was convicted of converting bulk narcotics cash into Bitcoin and layering transactions through multiple wallets.

OFAC has made its first public identifications of cartel cryptocurrency addresses on the Ethereum blockchain and has sanctioned 17 cryptocurrency addresses linked to fentanyl precursor suppliers.

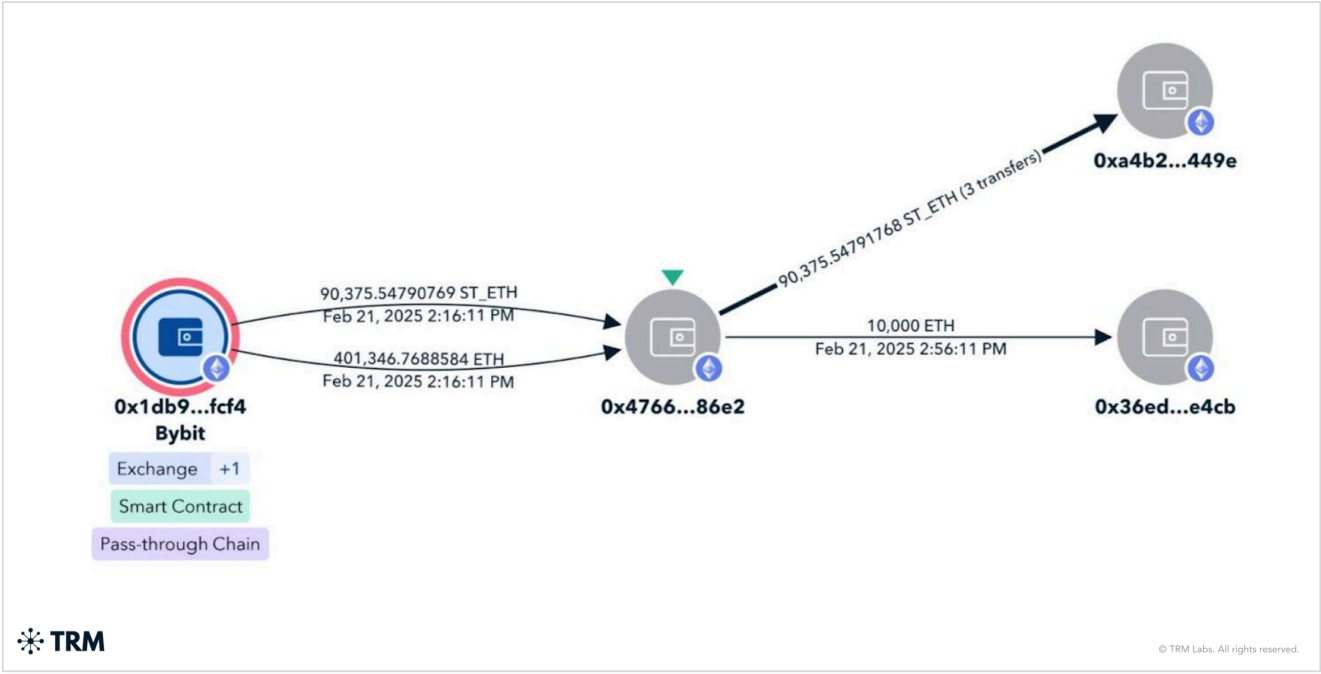
The implication for this committee is that the digital technology question and the border security question are not two separate inquiries. The financial infrastructure enabling fentanyl trafficking into the United States and the financial infrastructure laundering the proceeds of fraud committed against American citizens are substantially the same infrastructure.

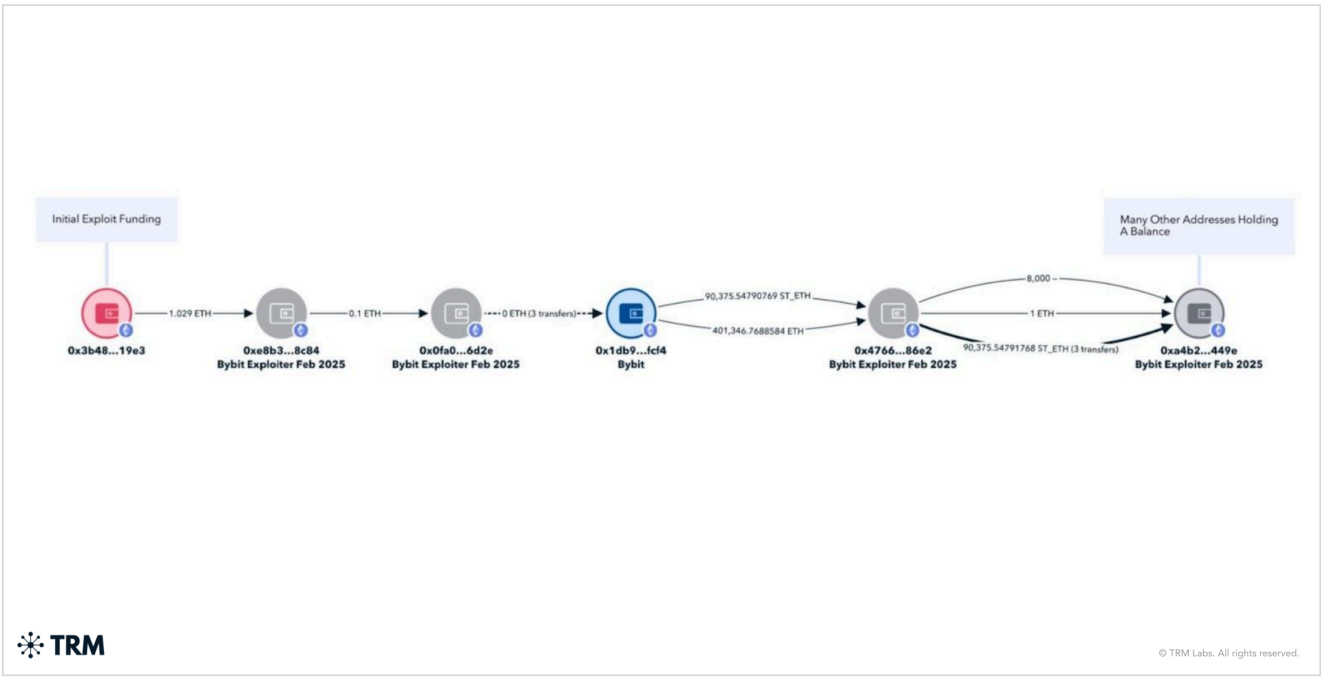
North Korea: A national security imperative

North Korea stole approximately USD 1.92 billion in cryptocurrency in 2025, including the February 2025 hack of Bybit, where USD 1.46 billion was taken in what stands as the largest single cryptocurrency theft in history.

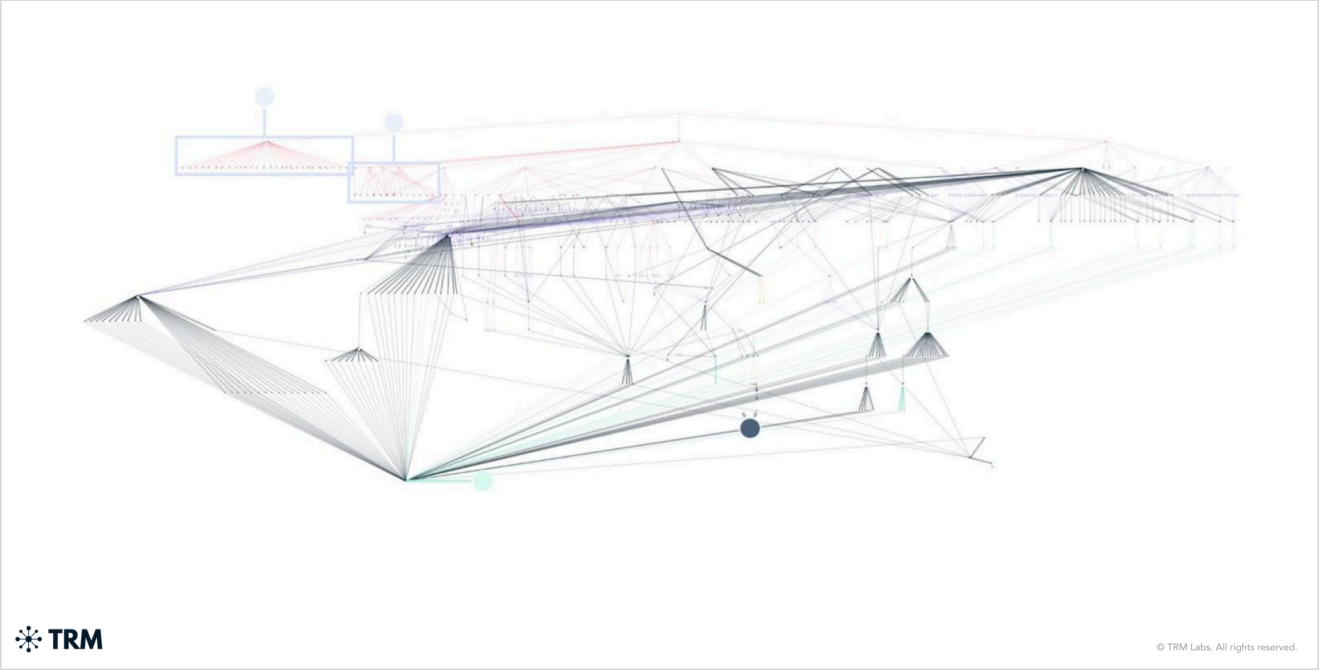
The scale of the theft is matched by the speed and sophistication of the laundering that followed. Within days, nearly all stolen Ether was bridged into Bitcoin using decentralized protocols, reflecting what TRM identified as an unprecedented level of operational efficiency. The funds were then funneled through mixers, cross-chain bridges, and decentralized exchanges, creating rapid layers of obfuscation designed to frustrate tracing and delay interdiction.

Such rapid layering suggests an expansion of North Korea's laundering infrastructure — likely with greater support from underground networks in China to absorb and process the funds. Indeed, once the initial obfuscation was done, a large portion of the assets sat idle, presumably awaiting liquidation through OTC channels that can handle converting tens of millions without detection.





Funds moving off of ByBit after the initial hack, as shown in TRM Graph Visualizer.



The rapid laundering process, as of February 26, 2025, includes transfers through multiple intermediary wallets, conversion into different cryptocurrencies, and the use of DEXs and cross-chain bridges to obfuscate the trail.

This activity reflects a broader evolution in North Korea's laundering playbook. Rather than relying on slower, linear laundering techniques, these actors now move assets through complex, multi-chain transaction paths almost immediately after a hack. The goal is clear: maximize speed, fragment the trail, and position funds for eventual off-ramping. Following the initial laundering phase, a significant portion of the Bitcoin sat idle, likely staged for liquidation through over-the-counter brokers capable of handling large volumes without triggering compliance controls.

Those OTC networks are central to the ecosystem. North Korea's Foreign Trade Bank representative Sim Hyon-sop has been linked to coordination with China- and Hong Kong-based brokers who facilitate the conversion of stolen crypto into fiat currency through exchanges and shell companies. These networks provide the critical bridge between illicit on-chain activity and the traditional financial system, enabling the regime to operationalize stolen digital assets at scale.

At the same time, Russia-based exchanges have continued to play a key role as downstream laundering venues. Garantex, long associated with illicit finance, rebranded as Grinex within days of an OFAC enforcement action, underscoring how quickly these platforms adapt to sanctions pressure. These exchanges remain preferred destinations for both North Korean and Russian criminal actors, reinforcing the interconnected nature of these illicit financial ecosystems and the challenges of disruption.

This is a state-directed financial strategy — not opportunistic crime. The proceeds from these operations directly support North Korea's nuclear and ballistic missile programs. A single operation yielding USD 1.46 billion represents a meaningful contribution to a weapons of mass destruction program. Disrupting these flows is therefore not simply a matter of financial crime enforcement — it is a national security imperative, requiring coordinated, whole-of-government action at the same level of urgency applied to other systemic threats.

The Russia-China-North Korea nexus

What TRM's data reveals is not a collection of separate criminal threats but an interconnected illicit finance ecosystem in which state sponsors, criminal networks, and technical infrastructure are deeply intertwined. North Korea supplies the hackers and cyber capabilities. Russia provides the criminal marketplace infrastructure and technical tools. China furnishes the financial plumbing through underground banking networks and OTC brokers. Scam center operators in Southeast Asia generate the fraud proceeds that flow through the same networks that launder cartel drug money and North Korean stolen cryptocurrency.

The A7 sanctions evasion platform, operated from Russia, processed at least USD 56 billion in 2025. Nearly 95% of sanctioned entity inflows used stablecoins, meaning that dollar-denominated digital assets are serving as the reserve currency of the global illicit finance system. Blockchain data tells us this.

Artificial intelligence as a force multiplier for criminal organizations

Artificial intelligence has transformed the operational capabilities of criminal enterprises at a pace that demands the most urgent policy response this committee can deliver.

In testimony before the House Judiciary Subcommittee on Crime and Federal Government Surveillance in July 2025, I described how the early adoption of AI by TCOs from scammers to ransomware gangs, poses a civilization level threat.

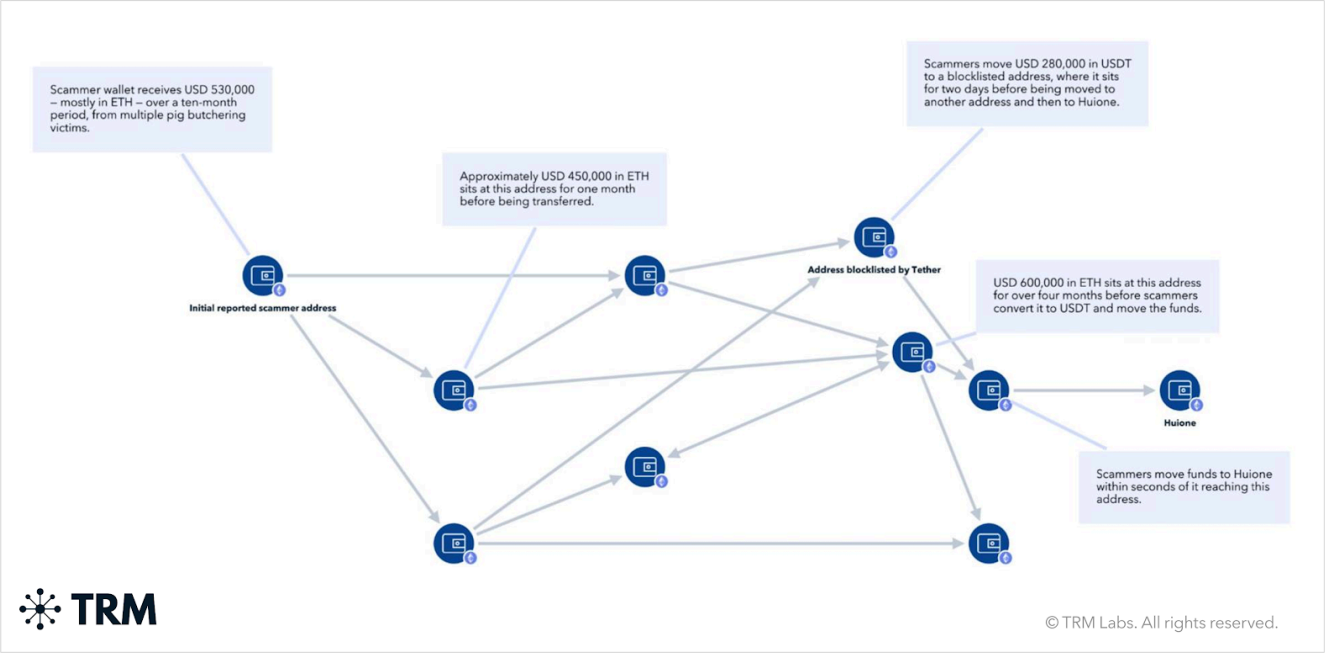
Generative AI-enabled scam activity rose 500% over the last year, according to data from Chainabuse, TRM's open-source scam reporting platform. Deepfake technology now enables real-time face and voice swapping during live video calls, allowing criminals to impersonate financial professionals, family members, government officials, and even romantic partners with sufficient fidelity to deceive careful, intelligent people.

A Hong Kong company lost millions of dollars when employees participated in a board meeting that appeared to include legitimate company executives, all of whom were AI-generated impersonations. Romance scam operators are now deploying AI systems that conduct initial outreach, maintain ongoing emotional engagement across dozens of simultaneous victim relationships, and adapt their communication style in real time based on victim responses, all without a human operator being involved in the conversation.

AI-generated synthetic identity documents are available on criminal marketplaces for as little as USD 15 per document, enabling fraudsters to open accounts at regulated cryptocurrency exchanges and bypass Know Your Customer (KYC) controls at a scale that manual document forgery could never achieve. AI allows criminal networks to operate multilingual outreach campaigns simultaneously, removing the language barrier that previously limited the geographic reach of individual fraud operations. AI-powered ransomware creates polymorphic malware that evades detection systems by constantly rewriting its own code, and identifies high-value targets based on financial data scraped from public sources.

Deepfake tool used in a scam center in Cambodia and Thailand (Source: UNODC).

AI's impact is visible not just in outreach and engagement, but also in laundering tactics. AI accelerates the rotation of infrastructure, the creation of synthetic identities, and the spread of fraudulent domains and social media personas, enabling scam networks to iterate rapidly across platforms and choke off investigative visibility before responses can materialize. In practical terms, what once required teams of human actors now often requires only the right prompt engineering and an AI engine capable of consistent execution.



TRM graph showing typical scam laundering pattern.

Blockchain data confirms this speed acceleration: average wallet holding periods for scam proceeds have decreased significantly. Funds now move across multiple wallets and chains within 24 to 48 hours of receipt, dramatically narrowing the window for meaningful interdiction and recovery.

Fraud, and the laundering of illicit proceeds, has evolved into a coordinated, AI-assisted industry operating at global scale.

Our response must reflect that reality.

The response to this acceleration in AI cannot be the restriction of AI technology or an attempt to slow innovation. It has to be ensuring that the tools of safety evolve just as quickly as the tools of harm. At TRM, that means pairing advanced AI with human expertise—using AI to map illicit networks in real time, identify patterns, triage risk, and surface early warning signs, while enabling analysts and investigators to act faster and make more informed decisions. AI brings speed and scale, but it is the human judgment layered on top that turns insight into action and drives effective disruption.

These systems operate with guardrails that ensure every action is auditable, every output is traceable, and human analysts remain in the decision-making loop for consequential actions. The private sector has built these capabilities. The question for this committee is whether law enforcement will have the resources, training, and legal authority to deploy them at the speed the threat demands.

The Executive Order: A critical and historic framework

On March 6, 2026, President Trump signed an Executive Order on Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens. This order represents the most important federal policy development on cyber-enabled fraud. Its implementation will determine whether the victims I described at the outset of this testimony see a meaningful change in their protection.

The order begins from the correct diagnosis: that transnational criminal organizations are conducting coordinated campaigns of cybercrime, fraud, and predatory schemes against American citizens, that these campaigns are draining American families of their life savings, and that they constitute a national security threat as well as a financial crime problem.

That framing matters because it determines which tools are available in response. A financial crime problem is handled by financial regulators and law enforcement. A national security threat commands the full toolkit of American power, including diplomatic pressure, targeted sanctions, visa restrictions, trade consequences, military and intelligence resources, and whole-of-government coordination.

The EO creates an operational cell within the National Coordination Center to coordinate federal efforts to detect, disrupt, dismantle, and deter cyber-enabled criminal activity. It directs the Secretary of State to engage with foreign governments to demand enforcement actions against TCOs operating on their soil. And it explicitly contemplates consequences for nations that tolerate predatory activity targeting American citizens, including targeted sanctions, visa restrictions, trade penalties, and limitation of foreign assistance.

The order also directs the Attorney General to submit recommendations for a Victims Restoration Program that would provide restitution to victims of cyber-enabled fraud schemes from funds seized from criminal networks. This provision matters enormously to the people I described at the outset of this testimony. The grandmother who lost her retirement account, the veteran who lost his home equity, the family whose savings were gone in 72 hours — they need to know that law enforcement success means something tangible for them, not just a press release about an indictment.

The reason this order is historically significant is not just its content but its accountability structure. For years, the US government's response to cyber-enabled fraud against Americans was fragmented across dozens of agencies, reactive rather than proactive, and consistently under-resourced relative to the scale of the threat.

Scam center operators in Myanmar, Cambodia, and Laos operated with effective impunity because no single agency had both the authority and the mandate to coordinate a comprehensive response. Every agency involved in this space holds a piece of the puzzle. The FBI handles cyber crime investigations. OFAC handles sanctions designations. DEA handles narcotics trafficking. HSI handles human trafficking and money laundering. The State Department handles foreign policy. FinCEN handles financial intelligence. But without a coordination mandate and a clear accountability chain, those pieces rarely come together into a coherent strategy.

The EO creates that accountability. It names responsible officials, sets deadlines, and signals at the highest levels of government that the full toolkit of American power will be brought to bear on the organizations running these schemes. TRM is committed to working with executive branch agencies and this committee to ensure that the EO has a lasting impact on the victims of these criminal networks.

The Scam Center Strike Force and law enforcement efforts

Beyond the EO, the US government is responding to the global threat of transnational criminal networks that have industrialized fraud. In November 2025, the US Department of Justice launched the Scam Center Strike Force to coordinate efforts to dismantle these networks, disrupt their infrastructure, and recover stolen funds.

What distinguishes the Strike Force is its whole-of-government approach, bringing together law enforcement, financial regulators, and national security agencies to address a threat that spans jurisdictions and financial systems. In addition, the Strike Force leverages the Beacon Network and other private sector initiatives in order to bring every resource to bear.

The DOJ leads prosecutions and asset seizures, while agencies like the FBI, HSI, DEA, IRS-CI and US Secret Service conduct investigations and blockchain tracing. Treasury components, including OFAC and FinCEN, apply sanctions and financial intelligence tools to target the laundering networks that move illicit proceeds, while the State Department supports

international coordination. This integrated model reflects the reality that these fraud networks operate across borders and rely on both crypto and traditional financial rails.

More broadly, the initiative signals a shift in how governments are approaching crypto-enabled fraud — treating it as a systemic national security threat that demands sustained, coordinated action across law enforcement, financial, and diplomatic channels.

There are also other efforts. Law enforcement agencies and private sector partners across the US, Asia, and Europe have launched specialized task forces to respond to pig butchering scams, including Operation Shamrock, the FBI's Operation Level Up, and Europol's European Financial and Economic Crime Centre (EFECC).

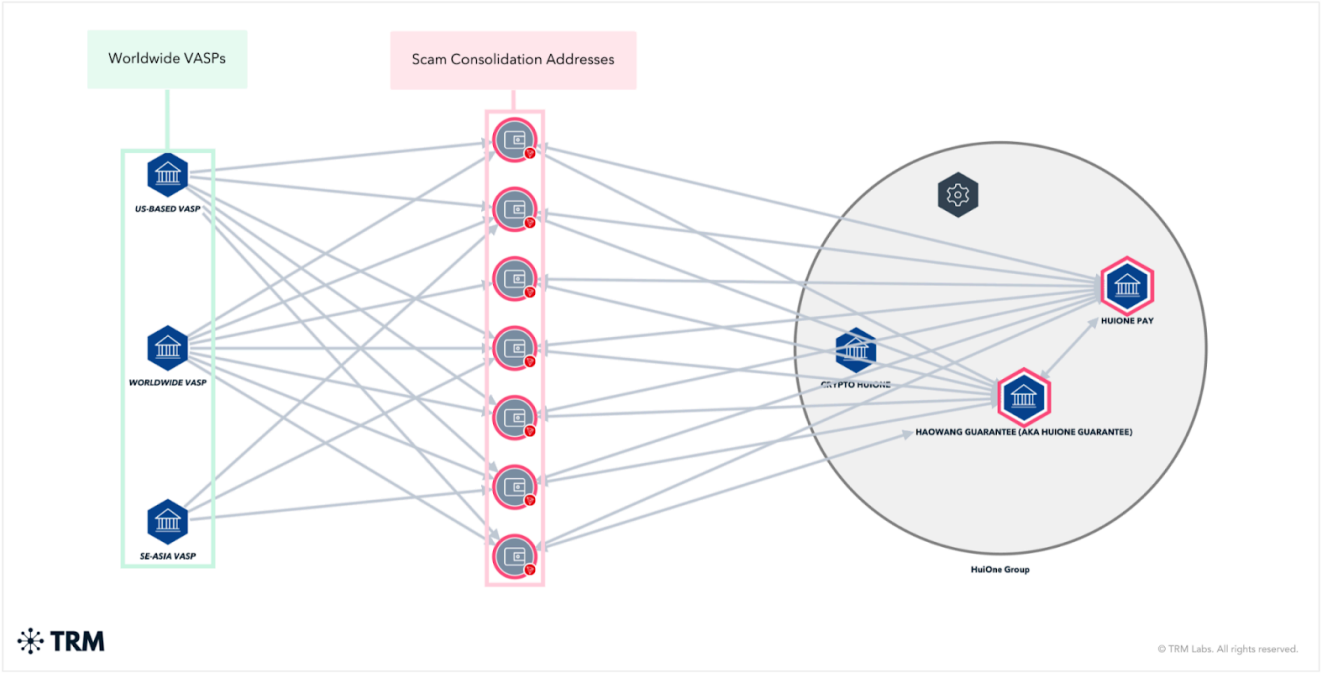
The Homeland Security Task Force (HSTF), announced in early 2025, represents a whole-of-government response to transnational criminal organizations operating within the United States. Co-led by the FBI and Homeland Security Investigations, the task force integrates federal, state, and local law enforcement into a single operational framework designed to identify, target, and dismantle cartels, foreign gangs, human trafficking networks, and financial crime infrastructure. With more than 8,500 federal agents and analysts working alongside over 440 state and local agencies across all 52 states and territories, the model embeds intelligence, personnel, and operational coordination nationwide to break down silos and enable unified, intelligence-driven action.

In just its first year, HSTF has delivered results at scale, including more than 3,200 arrests, over 200,000 pounds of drugs seized, more than 1,000 illegal firearms recovered, and hundreds of coordinated operations in a concentrated enforcement period.

Over the last few years, US authorities have seized billions of illicit proceeds from hacks, ransomware groups, scam networks, and other threat actors. For example, in October 2025, the US Department of Justice announced the indictment of Cambodian national Chen Zhi, founder and chairman of Prince Holding Group, a multinational conglomerate based in Cambodia. Zhi was charged with wire fraud conspiracy and money laundering conspiracy for directing Prince Group's operation of forced-labor scam compounds across the country.

In a parallel action, the DOJ filed a civil forfeiture complaint for 127,271 bitcoin — valued at more than USD 15 billion — now in the custody of the US government. The filing marks the largest forfeiture action in US history, underscoring both the scale of the criminal network and the unprecedented reach of law enforcement's response.

Concurrently, OFAC is working with the UK Foreign, Commonwealth, and Development Office (FCDO), which sanctioned 146 targets linked to the Prince Group. In addition, FinCEN finalized its Section 311 order against the Huione Group, cutting the organization — and any intermediary bank — off from the US dollar system.



As shown in TRM Graph Visualizer Huione Group was involved in laundering illicit funds such as cybercrime, cyberfraud, and DPRK-controlled assets.

At its core, Operation Prince shows how governments are evolving to confront industrial-scale crypto-enabled fraud — aligning prosecutions, financial intelligence, sanctions, and international coordination to disrupt networks, seize assets, and hold leadership accountable. It underscores that tackling transnational scam networks requires a sustained, integrated approach targeting both on-chain activity and the off-chain enablers that allow these ecosystems to scale.

While the Prince Group takedown is a significant win for global security, similar networks continue to operate worldwide.

The Beacon Network

The private sector has built infrastructure that is ready to support the whole-of-government approach outlined in the Executive Order.

TRM's Beacon Network is the first real-time, global intelligence-sharing system for illicit cryptocurrency activity, built in collaboration with leading platforms including Coinbase, Binance, Kraken, PayPal, Ripple, Stripe, Robinhood, Crypto.com, and Zodia Custody. The network connects verified participants across the public and private sectors — including approximately 70 law enforcement agencies worldwide, many within the United States — enabling them to flag illicit wallets and transactions as activity unfolds. By sharing actionable intelligence in real time, Beacon allows investigators and compliance teams to move at the speed of the threat — freezing funds, seizing assets, and disrupting transnational criminal networks before illicit proceeds can be laundered beyond reach.

The network operates through four steps: verified investigators flag illicit wallet addresses in TRM's system; flagged funds are automatically tracked across the blockchain in real time; when those funds reach a participating exchange or financial institution, Beacon sends an immediate alert; and the institution reviews the risk level and coordinates with law enforcement before processing any withdrawal.

The network currently covers approximately 85% of centralized cryptocurrency transaction volume, meaning that when scam proceeds hit a major exchange, there is a high probability that a Beacon alert will fire before the criminal can cash out.

The Scam Center Strike Force and the HSTF — combined with the EO, legal authority to compel holds, diplomatic leverage to pressure host nations, and operational access to Beacon's alerting capability — could represent a fundamentally different kind of enforcement infrastructure than anything the US government has previously fielded against this threat.

Solutions: What Congress can do

The Executive Order creates the framework. Congress must now provide the legal authorities, tools, and resources to make that framework operational and durable.

Enact a digital assets "hold law"

Congress should enact a digital assets "hold law," which would create a legal safe harbor allowing cryptocurrency exchanges to temporarily freeze funds linked to suspected illicit activity, pending legal process from law enforcement. The language for such a law exists today in the Senate Banking Committee's draft of the "Digital Asset Market Clarity Act."

Traditional banks have had this authority for decades. When a bank compliance officer identifies a suspicious wire transfer, they can place a hold while the matter is reviewed. Cryptocurrency exchanges operating under current law lack that clear authority. Every hour of legal uncertainty is an hour that criminal networks use to move funds to the next wallet and beyond recovery. Closing this gap would transform the speed at which the private sector can act on law enforcement intelligence.

Fund and scale real-time intelligence sharing

Real-time disruption and interdiction should be codified as a core pillar of US digital asset policy — embedding networks like Beacon into the regulatory framework as a standard capability across the ecosystem.

These models demonstrate how the private sector's real-time visibility can be paired with government authorities to freeze funds, seize assets, and disrupt illicit activity before it scales. The Senate Banking Committee's market structure discussion draft already moves in this direction, emphasizing enhanced public-private coordination and anti-money laundering obligations as part of a broader effort to address illicit finance risks in digital assets.

To operationalize this, Congress should prioritize policies that scale participation and remove friction. That includes dedicated federal funding to expand real-time intelligence-sharing networks — especially for smaller platforms that are often targeted as compliance weak points — and a formal legal framework that provides liability protection for firms acting on law enforcement intelligence. Illicit actors deliberately migrate to the edges of the ecosystem; closing those gaps requires both resources and clear rules that enable rapid, coordinated action across platforms and jurisdictions.

More broadly, this should be treated as a best practice across the industry. Digital asset firms should be expected to participate in real-time intelligence networks, integrate rapid response capabilities into compliance programs, and act immediately on high-confidence illicit indicators. The future of effective enforcement is not retrospective analysis — it is coordinated, real-time disruption powered by public-private collaboration.

Deploy AI investigative capacity at scale across federal agencies

Congress should fund the development and deployment of AI-powered investigative tools across IRS Criminal Investigation, FinCEN, OFAC, the FBI, DEA, Secret Service, HSI, national security, and defense agencies. The criminal networks before this committee are deploying AI autonomously and at scale. Responding with 20th century investigative tools against 21st century criminal infrastructure is not a viable strategy. Federal agencies need the funding, the procurement authority, and the legal frameworks to acquire and deploy these capabilities at the speed the threat demands.

Explore cyber "letters of marque"

We live in a moment where the private sector holds much of the critical data and the public sector holds the authorities — but success depends on fusing the two in real time.

Effective disruption requires ensuring government has access to actionable intelligence while enabling trusted private sector actors to move quickly, within clear legal frameworks, to freeze funds, identify bad actors, and dismantle criminal networks as activity unfolds. That reality should drive a more forward-leaning policy approach: granting narrowly scoped, government-authorized authorities for vetted private actors to take targeted action against the technical infrastructure of transnational criminal organizations.

There is a strong conceptual foundation for this model. Historically, governments have extended limited authorities to private actors to address threats that outpaced traditional state capacity. In the digital context, this could take the form of what might be called "cyber letters of marque," "authorized disruption authorities," or a structured "white hat intervention" framework — mechanisms that allow approved entities, operating under strict oversight and accountability, to intervene in real time to disrupt illicit infrastructure, block transactions, or degrade criminal networks.

Today's threat environment — particularly scam center networks that blend state sponsorship, criminal enterprise, and advanced technology — demands this kind of adaptation. These networks move at machine speed, exploit jurisdictional seams, and leverage both crypto and traditional finance. Matching that threat requires a system where intelligence, authority, and action are aligned — and where public-private collaboration is not just information-sharing, but coordinated, real-time disruption.

Provide tools and training to state and local law enforcement

When a victim of pig butchering walks into a police station, the officer taking the report is often the only law enforcement contact that victim will ever have. That officer needs to know how to capture blockchain identifiers from the transaction confirmations and wallet addresses the victim can provide, how to preserve digital evidence in forms that support subsequent federal investigation, and how to connect the case to FBI, HSI, or Secret Service task forces with cryptocurrency investigative capability. Too many reports taken today result in no actionable investigation because the frontline officer does not have the training to recognize what they have received.

Mandatory blockchain intelligence training and access to tools for federal, state, and local law enforcement would meaningfully increase the proportion of cases that develop into actionable investigations rather than dead-end reports.

Create a victim compensation fund

Congress should create a DOJ-administered victim compensation or restoration fund to ensure that victims of cryptocurrency-enabled scams are made whole to the greatest extent possible. In today's threat environment, law enforcement can often trace and seize illicit proceeds, but the speed, scale, and fragmentation of these transactions make it difficult to tie specific recovered funds back to individual victims. A centralized fund would solve this problem by pooling recovered assets and distributing them equitably across victims, ensuring that relief reaches constituents even when precise attribution is not possible.

This approach is already contemplated in the Executive Order and should be codified into law. All funds recovered through seizures and forfeitures tied to scam activity should first be directed to victim compensation, with any remaining funds used to administer the program and support continued enforcement efforts. This creates a victim-first model that reflects the realities of modern financial crime while establishing a durable framework for recovery in complex, cross-border cases where traditional restitution mechanisms fall short.

Conclusion

The threat before this committee is real, it is growing, and it is hitting American families with a precision and scale that demands a response equal to the challenge. In my career I have never seen anything like what blockchain intelligence reveals about the operational sophistication and financial resources of the criminal networks I have described today. But I want to leave this committee with something beyond the weight of the problem, because the weight of the problem, while real, is not the whole story.

We can follow the money. The blockchain is a public, permanent, immutable ledger, and the tools to read that ledger and identify the actors behind the transactions exist today. The private sector has built intelligence-sharing infrastructure, real-time alerting systems, and AI-powered investigative tools that are already producing results.

The Executive Order signed in March creates, for the first time, a whole-of-government mandate to bring the full toolkit of American power to bear on the organizations running these schemes. What the grandmother in Ohio, the veteran in Texas, and the family in New York need from this committee is the legal authority, resources, and sustained institutional commitment to deploy these capabilities at the speed and scale the threat demands. I am grateful for the attention this joint hearing brings to these issues and welcome your questions.

Prepared Testimony of Joshua M. Bercu
Executive Director, Industry Traceback Group
Senior Vice President, Policy, USTelecom — The Broadband Association
Before the House Committee on Homeland Security
Subcommittees on Border Security and Enforcement and Cybersecurity and Infrastructure Protection
Joint Hearing: "Online Scams, Crypto Fraud, and Digital Extortion:
An Examination of How Transnational Criminal Networks Target Americans"
April 21, 2026

I. Introduction

Chairman Garbarino, Ranking Member Thompson, Chairman Guest, Ranking Member Correa, Chairman Ogles, and Members of the Subcommittees:

Thank you for the opportunity to testify today and for your leadership on this critical issue. Your continued partnership is vital to sustaining the vigilance, innovation, and coordination we need to fight the transnational criminal networks exploiting the American people we all serve.

I'm Josh Bercu, Executive Director of the Industry Traceback Group, or ITG, and Senior Vice President of Policy at USTelecom—The Broadband Association. For over ten years, USTelecom has led the Traceback Group, which serves as the entity designated by the Federal Communications Commission to trace back suspected unlawful robocalls. I also have served in leadership roles on the Federal Trade Commission's Scams Against Older Adults Advisory Group and the Aspen Institute Financial Services Program's National Task Force for Fraud & Scam Prevention.

The telecom industry has been making real and meaningful progress to protect American consumers by confronting illegal calls, including both illegal robocalls and scams. Communications providers have developed and deployed powerful tools and mechanisms like call blocking and labeling, call authentication, and industry-led traceback — all complemented by a strengthened accountability regime at the FCC and aggressive enforcement by government partners at the federal and state level.

My testimony focuses on the telecom infrastructure that transnational criminal organizations, or TCOs, abuse and misuse to reach American victims and on the industry tools, enforcement partnerships, and policy frameworks we need to disrupt them. The Traceback Group's work sits at an important intersection: we trace the illegal calls that the same criminal networks you are examining today often are behind. And the intelligence we develop supports a myriad of government enforcement actions against these groups and the in-on-the-scheme entities they rely on.

From this work, we've seen both what's possible and what's still urgently needed to protect consumers. The bottom line: we have built and deployed the right tools and anti-scam infrastructure. The foundation is strong. Now we need to keep building on it, deepening collaboration across industry sectors and with government to ensure those tools deliver real accountability for the criminals behind these scams.

II. Disrupting Scam Infrastructure Through Traceback and Enforcement

Traceback is one of the tools we have adapted to disrupt call-based scam operations. It used to take law enforcement agencies months to determine who made an illegal call — we now often find those criminals within hours. That speed and scalability allow us to keep pace with today's fast-moving fraud.

By rapidly tracing the path of illegal calls back through the network, the Traceback Group helps identify the multiple providers that carry the call and actors enabling or originating fraud. We work closely with federal and state law enforcement, routinely tracing calls referred to us – including scams impersonating the Department of Homeland Security, IRS, Social Security Administration and other federal agencies – and providing actionable information to support enforcement. Over the past several years, traceback has contributed to dozens of civil and criminal actions. We also have begun to work with international law enforcement partners.

We know the combination of identifying the bad actors responsible, including through traceback, and then holding them accountable works:

- Raids of illegal calling operations in India led to an 85% drop in robocalls impersonating the IRS in 2016, and a similar joint effort by Canadian and Indian authorities in 2018 drove a 77% decline in calls impersonating the Canadian Revenue Agency.

- Enforcement targeting those responsible for unsolicited vacation and timeshare robocalls led to those calls dropping by half in 2017.

- FTC enforcement led to a 60% decline in unlawful health insurance robocalls in 2019, and FCC and state attorneys general action led to the virtual elimination of the illegal auto warranty robocall campaign between 2021 and 2022.

Today, thanks to coordinated action by industry and government, many of the most disruptive, high-volume scam calls — like those impersonating the IRS or Social Security Administration — no longer reach vulnerable Americans at the same scale. Data from YouMail shows scam robocall volume is about 50% lower than at the March 2021 peak.

In recent years, industry collaboration has expanded beyond the communications sector and the public sector. The Traceback Group, for example, now works with banks, major tech companies, the hospitality industry, and others to identify the criminals behind illegal calls and feed that information to law enforcement. In one recent instance, some of our data was shared through the National Cyber-Forensics Training Alliance to support takedowns by the Department of Homeland Security's Homeland Security Investigations. These burgeoning partnerships are one of the most promising developments to protect consumers.

III. How Criminal Networks Abuse U.S. Telecom Infrastructure

The progress is real, but so is the evolution of the threat. Today's fraudsters aren't blasting millions of robocalls impersonating the Social Security Administration. They're shifting from high volume to high impact, and the criminal networks behind these schemes are sophisticated, organized, and global. From a telecom perspective, this evolution is defined by how these

organized crime groups abuse and misuse U.S. communications infrastructure to reach consumers.

A decade ago, the dominant illegal calling threat to U.S. consumers was concentrated in South Asia, principally India and to a lesser degree Pakistan and Bangladesh. Operators ran tech-support, IRS-impersonation, and bank-fraud scripts out of illegal calling operations. That threat persists, but the center of gravity has shifted. As has been well-documented, the most consequential development is the rise of industrial-scale "scam compounds" in Southeast Asia, principally in Myanmar, Cambodia, and Laos. In parallel, Mexican drug cartels have built their own illegal calling operation networks targeting American consumers.

One important point for Congress' consideration, however, is structural. What was once a regionally bounded set of criminal enterprises has become a globalized, industrialized fraud-as-a-service marketplace. Criminal fraudsters' toolsets are bought, sold, and shared across these ecosystems. Playbooks, scripts, and even trafficked labor move through Telegram channels, dark-web forums, and overlapping financial infrastructure. The practical consequence is that successful techniques are copied, traded, and operationalized across regions on a timeline measured in weeks, not years.

While the threat of foreign actors abusing U.S. networks is not new, their tactics are evolving. Increasingly, we trace calls back to entities posing as U.S.-based providers: forming shell LLCs, using disposable domains, and in some cases impersonating real telecom companies — tactics designed to evade know-your-customer requirements and regulatory scrutiny. Beyond this, we see growing instances where legitimate callers and calling platforms — a hospital, a school broadcast service, tools used for get-out-the-vote calls, and more — are compromised and used to deliver scam impersonation calls, leveraging stolen credentials and deployed at scale using AI and automation. At the same time, SIMBoxes add another layer of complexity, enabling scammers to simulate thousands of unique mobile identities and making high-volume activity look like individual callers — and generate calls from within the United States, even if the callers themselves are located abroad.

These evolutions are not accidental. Traceback and enforcement have systematically eliminated the low-hanging fruit. Enforcement actions have shut down or driven out the VoIP providers that once turned a blind eye to bad traffic or built their business on bringing it into the country. Gone are the days of blasting millions of calls through permissive internet-based voice providers. Instead, criminals have adapted, hijacking or deploying domestic infrastructure.

These trends underscore a central reality: while industry protections are essential and civil enforcement can be highly impactful, they are not sufficient on their own to deter the transnational criminal organizations orchestrating these schemes.

IV. Turning Progress into Lasting Impact

America's telecom providers have been moving aggressively to respond in the face of these evolving threats. But we cannot make arrests or prosecute the criminals — even when we identify them.

When I testified before the House Energy & Commerce Committee, Oversight and Investigations Subcommittee and the Senate Judiciary Committee nine months ago, I outlined three areas where federal action could make a meaningful difference: establishing a coordinated national anti-scam strategy, enabling greater cross-sector data sharing through a safe harbor, and scaling tools and partnerships that are already delivering results.

The Administration's March 2026 Executive Order makes important progress on that first priority and advances elements of the others. It reflects exactly the kind of whole-of-government approach this problem demands and treats scams as what they are: crimes.

The EO establishes a dedicated operational cell within the National Coordination Center to coordinate federal efforts to detect, disrupt, dismantle, and deter TCOs explicitly including private sector engagement. It also directs action to hold foreign governments accountable and to return seized assets to victims. Taken together, it signals that the Administration views transnational fraud as a national security priority, not merely a consumer protection matter.

The EO is exactly what we needed – and it could not have come at a more critical moment. Now the focus must be on ensuring that this momentum translates into sustained impact.

There are three areas where Congress can help:

- **Resource implementation and sustain pressure on cross-border criminal enforcement.** The EO rightly emphasizes enforcement and accountability, particularly for actors operating overseas. Congress can reinforce the EO and its mandate by supporting investigative capacity, prosecution, and cross-border coordination. We need prosecutors and investigators fully resourced so that they can move with urgency and work with willing partners abroad. Communications providers, including through the Traceback Group, stand ready in support.

- **Provide a safe harbor for improved fraud prevention and detection.** Emerging partnerships between telecom providers, financial institutions, tech platforms, and other stakeholders are showing real promise in identifying and disrupting scams. A well-scoped safe harbor could unlock even deeper collaboration across the internet ecosystem to accelerate threat detection and better prevent consumer harm. Right now, however, privacy regulation and other legal concerns can inhibit companies from using and, where appropriate, sharing data that could help identify and stop fraud.

- **Support and scale what works, including proven tools like traceback.** As scams evolve, we must double down on proven tools and partnerships that have shown real results. Traceback is one such tool: it can help drive criminal prosecutions, civil enforcement actions, and real-world disruption of scam networks, and increasingly serves as a model of effective cross-sector collaboration. But like many effective solutions, it requires sustained support and legal clarity to remain viable. Congress should reinforce frameworks that work like traceback, ensuring stability for the program and protecting it from efforts designed to undermine the process and its mission.

V. Conclusion

While we've made progress together, fraud continues to take a toll on American consumers. Scam robocalls are down, enforcement actions are up, and industry tools like traceback are evolving with the threat. The Administration's March Executive Order represents real momentum toward the kind of coordinated, enforcement-first approach this problem demands, and communications providers are committed to being a constructive partner in its implementation.

But the progress in reducing illegal call volume does not mean the threat is gone. Criminal fraudsters are adapting quickly, targeting individuals, impersonating trusted institutions, and operating from beyond what they perceive as the reach of U.S. enforcement. Transnational criminal networks are abusing U.S. telecom infrastructure as one component of a broader, multi-vector attack on American consumers — encompassing crypto fraud, digital extortion, human trafficking, and more.

Our next phase of work must focus on converting intelligence into impact — using traceback and cross-sector collaboration not just to detect fraud, but to deter, disrupt, and penalize it, and prevent perpetrators from targeting another victim.

Strengthening partnerships – particularly around coordinated criminal enforcement and the legal frameworks that enable deeper collaboration – is one of the most important ways the federal government can help turn progress into lasting impact, drive real accountability, and deliver meaningful protection for the American public.

Thank you for your time, and I look forward to your questions.

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.

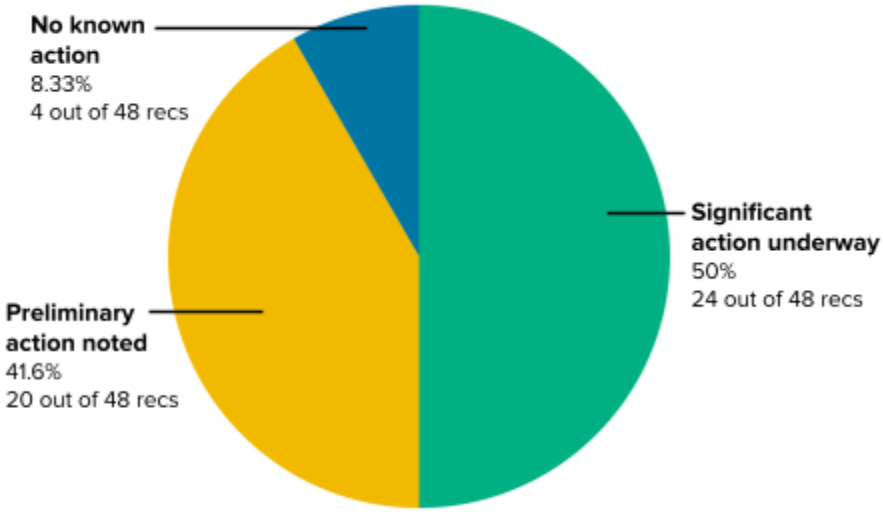
Policymakers should bear in mind that even though AI presents new offensive capabilities, it also creates opportunities for defensive applications. Over time, defensive uses of these technologies may end up dominating, driving down cybercrime. At the same time, even if the defensive uses wind up being 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/