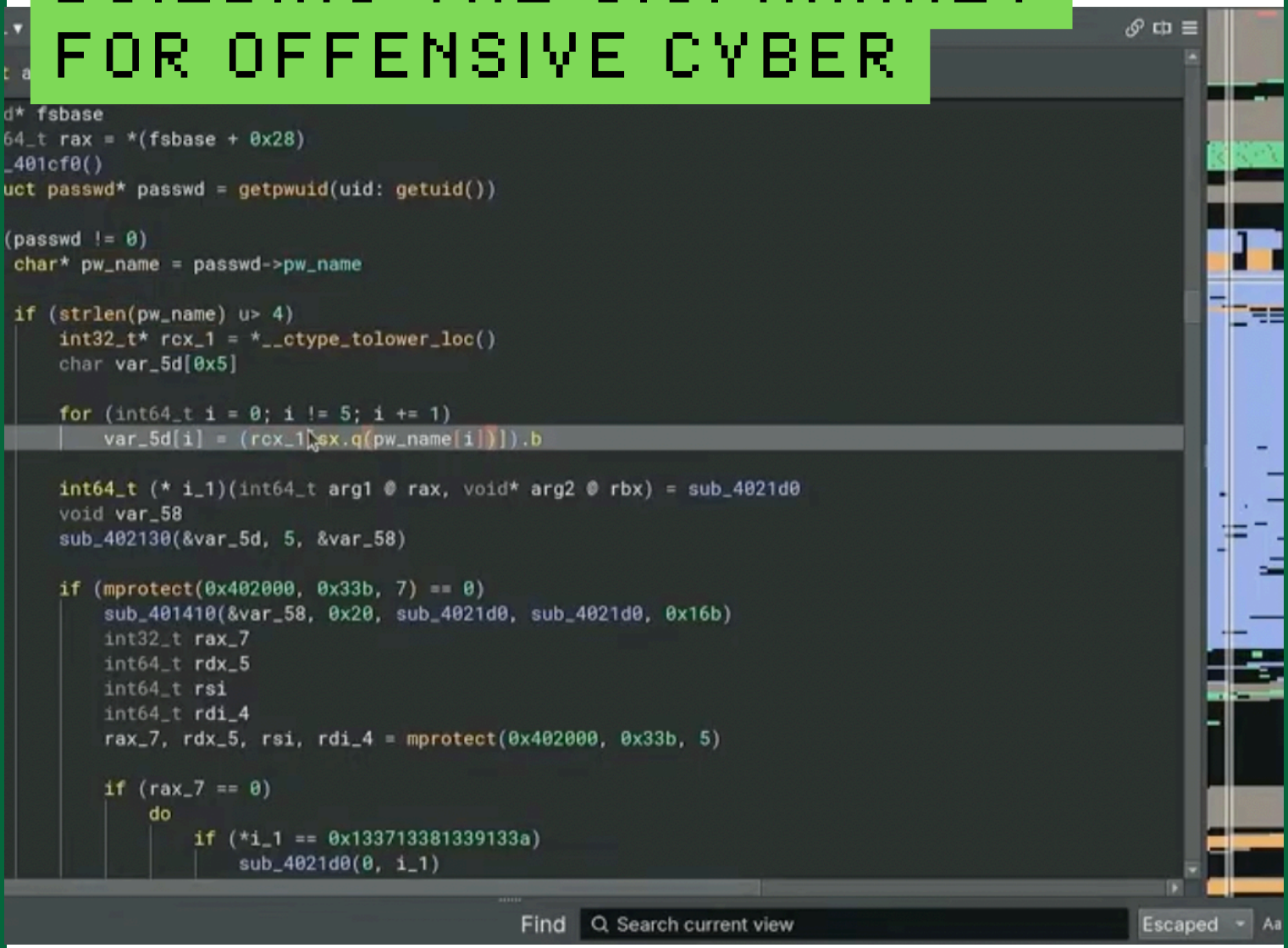
DARTMOUTH

ISTS

FROM CHAOS TO CAPABILITY

BUILDING THE U.S. MARKET FOR OFFENSIVE CYBER



Winnona DeSombre Bernsen
Sergey Bratus

Image Credits: Screenshot of LiveCTF 2025 Finals at DEFCON, https://www.youtube.com/watch?v=YcXgm9zy4Vk

EXECUTIVE SUMMARY

The U.S. government wants to engage with the private sector in cyberspace to tackle threats at scale, but it currently lacks a coherent public framework to do so. If the U.S. government wants to encourage more private sector support in offensive cyber, legal and policy changes must be made to create near-term, realistic opportunities.

In October 2025, Dartmouth's Institute for Security, Technology and Society (ISTS) convened thirty experts from government, industry, academia, and venture capital under Chatham House rules to analyze how private sector actors currently supports the U.S. government in "offensive cyber", and to make recommendations on how to effectively leverage the private sector to scale up such activity. Offensive cyber was broadly defined to include tool development, access, and effect generation for government cyber operations (OCO/CNE and law enforcement operations).

The roundtable identified the following three key findings in the U.S. offensive cyber landscape:

1. **Cyberspace dominance now requires both high- and low-equity capabilities, and opportunistic access at scale**: a large portion of real-world cyber operations do not require novel zero-days (high-equity), but instead require taking opportunistic advantage of adversary errors (low-equity). Organizations can realize outsized gains by detecting those errors quickly and determining which errors can create mission-aligned access.

2. **The U.S. private sector (through government contractors, small companies, and individuals) already actively supports cyber operations on behalf of the U.S. government.** It does so in three primary ways: capabilities support (i.e., providing tooling, training, and infrastructure for cyber operations), providing access (i.e., breaking into a system and passing off access to government), and creating effects themselves.

3. **Domestic private sector growth in offensive cyber tooling and access is currently limited** by how offensive cyber is acquired: while private equity firms invest in well-established offensive cyber firms, early-stage companies likely do not get private investment because venture capital does not normally invest in bespoke research or services. Unfortunately, the U.S. government largely acquires offensive cyber capabilities and access via services contracts and research.

The roundtable identified two gaps and three opportunities in the space:

1. **Gap:** The United States intelligence, military, and law enforcement is optimized for deliberate, tightly scoped, top-down operations in cyberspace. However, this does not create offensive cyber outcomes at the tempo asked for by U.S. policymakers. While the private sector can act on new bottom-up, time-sensitive opportunities created by adversary error, the government's operational tempo likely cannot keep up.

2. **Opportunity:** The U.S. private sector is willing to provide offensive cyber capabilities and access at a larger scale than currently utilized. Companies exist that possess the

technical skill, tooling, and operational experience required to deliver offensive capabilities and access, and are already providing services to the U.S. government.

3. **Opportunity:** Private sector actors are also likely willing to provide rapid cyber effects for the U.S. government against limited, lower-risk targets, but would need additional oversight, as well as liability and safety assurances. Letting the private sector conduct such activity would free up resources for the U.S. to focus on higher-priority targets.

4. **Gap:** The U.S. Government lacks transparency to signal a clear demand for offensive cyber. While the private sector could create more rapid, timely, and at-scale access or effects on the government's behalf, the U.S. government lacks clear avenues to encourage these offerings, and is currently unable to send clear demand signals.

5. **Opportunity:** Offensive cyber is now as much about understanding systems as exploiting them: breakthroughs in software understanding research and offensive systems analysis through "weird machine theory" of cyber exploitation could allow the U.S. to better comprehend how to exploit adversary systems while defending our own.

To effectively leverage the private sector in offensive cyber, the U.S. government must do the following:

1. Develop a public offensive cyber strategy;
2. Create robust capability pipelines through NSA / FBI / Department of War (DOW) pilot programs, Small Business Innovation Research (SBIR) programs, Other Transaction Authorities, and non-contracting instruments;
3. Invest in research on offensive systems analysis both within academic institutions and private cyber innovators; and
4. Authorize a pilot program for private sector operations against low risk actors.

A federal pilot program against foreign cryptocurrency scammers and ransomware operators may be the best initial use case for a legal, operational, and feasibility reasons - particularly given U.S. desire to become the "crypto capital of the world" and the benefit the U.S. could obtain by clawing back assets that leave the country annually in crypto scams. Despite the success of the most recent 15-billion-dollar law enforcement seizure of illicit cryptocurrency in October 2025, current reporting suggests that over 75 billion dollars of cryptocurrency is currently linked to criminal activity.

Offensive cyber power will depend not only on developing the most capabilities and accesses, but also on building legal, financial, and institutional frameworks that can harness innovation responsibly. Moving from chaos to capability requires shifting from ad hoc coordination to a structured ecosystem: one that connects private innovation with public purpose, scales lawful federal offensive operations, and reasserts U.S. leadership in cyberspace.

Introduction: The Future of Offensive Cyber

"Defense and offense are not peers. Defense is offense's child."
- John Lambert

"No modern computing system ends up being only and exactly what it was meant to be."
- Sergey Bratus

Offensive cyber, however defined, is becoming more prevalent as both policy idea and technical reality. However, there are still questions about what "offensive cyber" even entails, and how this will impact U.S. economic and national security.

Under Chatham House Rules, Dartmouth's Institute for Security, Technology and Society (ISTS) gathered a group of thirty cyber experts across the fields of industry, academia, think-tanks, non-profits, venture capital, and government, to discuss the following:

1. How does the U.S. private sector currently support and conduct offensive cyber operations for the U.S. government?

2. What further private sector and investment opportunities exist in offensive cyber?

3. If the U.S. government wishes to encourage more private sector collaboration in "offensive cyber", what policy and legal changes could be made to create near-term and realistic opportunities?

This roundtable started from the assumption that U.S. policymakers are increasingly interested in a private sector-led approach to respond to the rapidly increasing numbers of malicious cyber actors. Recent congressional actions[1] and U.S. government[2] statements[3] clearly show that, despite recognition of both the private and public sectors' hard work, U.S. policymakers believe current cyber options are ultimately inadequate due to lack of speed, flexibility, or scope.[4]

Moreover, cyber policymakers in the U.S.[5], as well as the United Kingdom, the Netherlands, Japan, and Canada[6], have moved towards a strategy of cyber persistence (or persistent engagement) since 2018.[7] Cyber persistence theory prizes continual situational awareness in cyberspace, and "persistently" engaging with one's adversary in the domain. Unlike cyber deterrence, cyber persistence argues that nation states can act in cyberspace without fear of escalation, and that interactions between states, businesses, and citizens continue to be important in the cyber domain, even in war.[8] The shift to more persistent, non-

escalatory cyber activity opens the door for the U.S. government to add offensive cyber as an "additional arrow in the quiver"[9] (i.e., adequately respond to malicious actors in cyberspace) by using a strategy that will likely require greater and broader collaboration with the private sector.

What this Paper Is and Is Not

"Privatized offensive cyber" oftentimes evokes varying definitions, authorities, and horror stories from the cyber policymaking community, alongside wide-ranging risks and trade-offs. This paper does not offer a grand vision for all the ways the private sector could potentially conduct cyber operations. This paper is, simply and pragmatically, the following:

1. An analysis of the current state of play for private sector actors providing offensive cyber tools, accesses, and effects for the U.S. government;

2. A selection of key opportunities and challenges about the current state of play; and

3. Policy recommendations for how the U.S. can expand the private sector's role in offensive cyber activity, to include capability engineering, access development, and effect generation.

The Offensive Cyber Landscape: Current State of Play

A. Cyberspace Dominance Now Requires Both High- and Low-Equity Capabilities, and Opportunistic Access at Scale

Cyberspace as a domain has evolved: the software and devices we rely on are completely different today than 15 years ago. As an example, almost all devices globally in 2010 were desktop computers - now, mobile devices make up 60% of global market share.[10] Moreover, systems and applications continue to get increasingly complex: containerization, cloud environments, and sprawling IT ecosystems make any organization's digital terrain notoriously difficult to map and navigate.[11]

Theories around offensive cyber have also evolved to comport with this new complex reality. This is especially the case for high-end offensive cyber capabilities like zero-day exploits. Zero-day exploitation (i.e. exploiting zero-day vulnerabilities) was historically defined as using crafted inputs to enable the execution of adversary code (or, "bugs") on a victim machine. In this way, exploit development was historically thought of as a search for *primitives* and their reliable compositions, *exploit chains.*[12] However, this understanding assumes that the effects of an exploit primitive or chain stand out, and are therefore easily detectable.[13] Today, large swathes of a target system's own intended logic can be repurposed to create exploit execution

engines - i.e., “weird machines”, which don’t exhibit easily detectable anomalies: such exploit chains have been found in the wild against Google’s Chrome browser[14][15] and Apple’s iMessage.[16] The emerging “weird machine theory” of cyber exploitation, originated at Dartmouth[17], suggests that exploits should be assumed in any sufficiently large system. In other words, instead of considering a program as a machine that may or may not have bugs hidden inside, any sufficiently complex program is actually one intended machine, with endless “weird machines” inside of it, waiting to be unlocked by an attacker.[18]

Some missions will always demand rare, stealthy, high-value exploits and weird machines. Unfortunately, those capabilities are becoming ever more expensive to discover and sustain.[19] A participant at the Dartmouth roundtable with over 25 years of exploit development experience stated that faster updates and complex ecosystems have compressed timelines for developing bespoke tools – for example, a single Apple platform update often requires entire offensive exploit development ecosystems to update their wares.[20] Participants remarked that developments in artificial intelligence may enable exploit development at a cheaper scale, but that the field has not yet exhibited public leaps in this regard.[21]

However, cyberspace is also expanding as a terrain: a new operational space has opened up where speed, scale, and replaceability matters more than singular technical elegance. As systems get more complex and are updated at increasingly faster rates, the number of ephemeral opportunities for access are expanding (ranging from complex “weird machines” to simple misconfigured AWS buckets[22]).

In other words, **a large portion of real-world cyber operations do not require novel zero-days**: multiple roundtable participants across industries attested that credential stuffing, or techniques targeting human error or supply-chains could often produce similar outcomes at minimal cost.[23] This is largely because adversaries (particularly lower-skilled ones) routinely make mistakes: lower-tier attackers fumble command-and-control, misconfigure infrastructure, or accidentally expose sensitive logs. Organizations who can move fast could realize outsized gains simply by detecting as many of those errors as possible, quickly determining which errors can create mission-aligned access, and rapidly exploiting those errors.

There is also growing public recognition that inexpensive and fast approaches have strategic value. The U.S. Department of War (DOW) has begun to realize that not all of their capabilities need to be high-end zero-days, and is determined to acquire more “low-equity capabilities”: U.S. Cyber Command (CYBERCOM) has budgeted for additional “low-equity cyber tooling to meet specific rapid access generation” needs of its Joint Task Force Zero (although this is only a small fraction of its overall budget) in FY2026.[24]

However, while one can strategically task out and acquire lower-equity capabilities from the top-down, much private sector ephemeral access is actioned upon from the bottom-up. The private sector is able to take advantage of many ephemeral, opportunistic accesses, because 1)

they have excellent visibility into customer and open-source environments, 2) receive alerts of anomalies in said environments; and 3) have bottom-up processes that enable an organization to take action on that visibility quickly. For example, in September 2025, defensive cyber security company Huntress published on an e-crime actor's tactics after the actor downloaded Huntress's free trial and conducted enough suspicious activity to raise signals on Huntress's EDR software.[25] This was likely only possible because individual analysts were alerted to the opportunity, elevated this opportunity to management, created a plan for observing and reporting on the threat actor, and got approvals to do so – all in a short period of time.[26]

By contrast, multiple roundtable participants agreed that the U.S. government, without the private sector, cannot operate at the speed required to achieve bottom-up, opportunistic success at the scale necessary to achieve mission objectives.[27] This is likely because the government is 1) slow to hear about the opportunity; 2) slow to authorize taking advantage of the opportunity (particularly due to legal and policy constraints); or 3) slow to act internally or contract out the activity. A roundtable participant in the government contracting space added that the rapidly shifting digital ecosystem can create a problem for government concept-of-operations (CONOP – plan of what is to be accomplished and how) development: regardless of tooling, adapting to a new CONOP within a large, bureaucratic organization (in reaction to the shifting environment) can be slow and operationally costly, because the individuals developing the CONOP may not understand the target well enough to find a new path.[28]

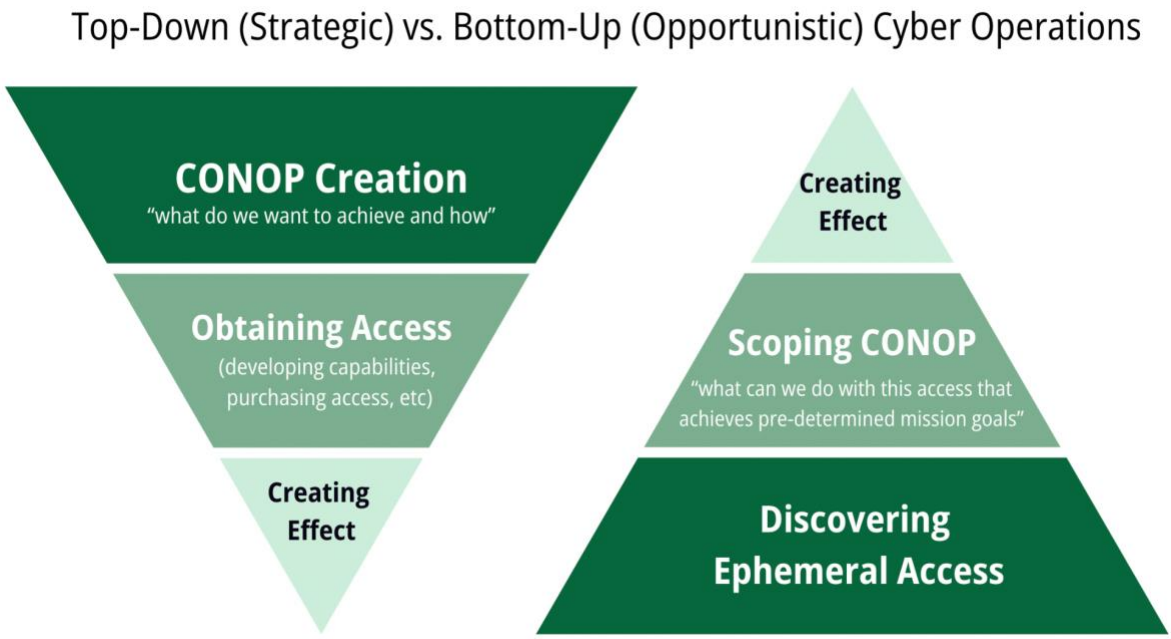


Figure 2: Top-Down (Strategic) vs. Bottom-Up (Opportunistic) Cyber Effects
Source: Winnona DeSombre Bernsen & Sergey Bratus

B. The Private Sector Both Already Supports and Conducts Cyber Operations on Behalf of the U.S. Government

Offensive cyber is a broad term with multiple meanings. For this purpose, offensive cyber is defined as support and execution around Offensive Cyber Operations (OCO). This includes creation of initial access capabilities, tooling, infrastructure, data management and pipelines, as well as providing access and effects for OCO under Title 10 (military), computer network exploitation (CNE) operations under Title 50 (intelligence) or other law enforcement operations.

Make no mistake - U.S. private sector companies already actively support and conduct cyber operations on behalf of the U.S. government. Companies do so in three primary ways: **capabilities** support (i.e., providing tooling, training, and infrastructure for cyber operations), providing **access** (i.e., breaking into a system and passing off access to support further government actions), and creating **effects** themselves. All of these ways currently involve the government contracting process, the recruitment of individual hackers, or ad hoc outreach and conduct by private citizens.

A Caveat: The Private Sector Already Creates "Effects" in Cyberspace Without Offensive Cyber

It is important to note that most of the private sector creates effects (i.e., disrupts adversaries) in cyberspace without offensive cyber.

Some effects can be conducted purely inside one's own infrastructure. Private sector disruption of activities on infrastructure already issued and maintained by that corporation (i.e., termination of accounts that conduct illegal hacking activity[29] or issuing patches for software exploited by adversaries[30]) is common: Google, Microsoft, Apple, Oracle and other large technology companies already do this, either through their trust and safety teams, abuse teams, or cyber security teams. Sharing indicators of compromise and other signatures both publicly and privately is also common, allowing companies to understand what threats other researchers are observing in the wild, and to shut down additional abusive activity on their infrastructure. Indicators (albeit through layers of in-house counsel) are normally shared with the U.S. government, either proactively or via law enforcement request under the Stored Communications Act.[31]

Other effects are created by the private sector outside their own infrastructure, via international court systems and/or in partnership with law enforcement. Here, the private sector either provides additional information to law enforcement during existing takedowns[32]

or seizures[33], or can even obtain a court's permission (via a civil lawsuit) to seize or transfer ownership of infrastructure conducting cybercriminal activity in parallel with law enforcement. Microsoft's activity during the DOJ Lumma Stealer takedown in May 2025 is one of many examples: the U.S. Department of Justice obtained a criminal warrant and coordinated with Europol and Japan's Cybercrime Control Center to seize websites used by cybercriminals to distribute LummaC2, an information stealing malware. In tandem, Microsoft initiated a civil action to take down and block 2,300 domains also used by actors behind LummaC2.[34]

It is important to distinguish that civil seizures are not executed via breaking into adversary infrastructure: in the court order for the LummaC2 case, the U.S. Court effectively directed third party Internet registries, registrars, data centers, and hosting providers with a presence in the United States to reasonably assist in either shutting down LummaC2 domains or transferring their ownership to Microsoft.[35] However, these civil actions are largely inefficient given the timeframe it takes to obtain a court order: the LummaC2 court order was granted 2 days after filing, and likely took multiple days to file after discovery of the malicious domain[36]. While 4-5 days is fast for bureaucracy, many APT groups are known to cycle through malicious domains in far less than a week, with some domains staying up for less than a day.[37] Moreover, this tactic is not effective for the significant portions of adversary infrastructure that are outside a U.S. court's reach.[38]

U.S. technology firms would like private sector disruptive activities to exclude cyber operations generally, because they do not want individuals exploiting flaws in their platforms. U.S. technology firms currently profit greatly from a global system in which they currently dominate data aggregation, routing, and storage. The U.S. private sector still leads in cloud infrastructure and social media, thus controlling the vast majority of the world's data. 1 out of every 4 people in the global population is an average monthly user of Google or Meta, while U.S. cloud infrastructure services (AWS, Microsoft Azure, Google Cloud, Oracle, Salesforce, and IBM) make up 70% of the global market.[3940] Much of this market share (and, by extension, the U.S. economy) is put at risk if they can no longer convince their consumers that their products are safe. For precisely this reason, large technology firms are unlikely to support mechanisms explicitly encouraging private-sector offensive actions, particularly ones that would be exploiting flaws in their platforms to break into target machines.

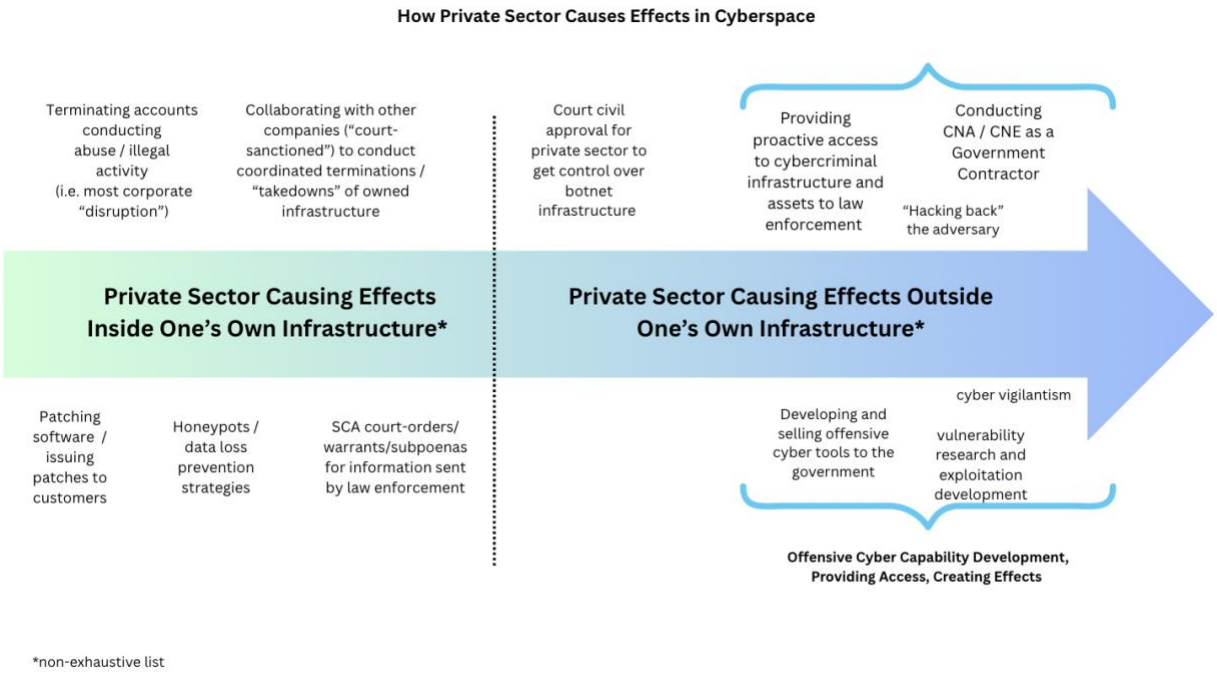


Figure 1: How Private Sector Causes Effects in Cyberspace
Source: Winnona DeSombre Bernsen & Sergey Bratus

Capability Support / Tooling:

Private sector actors in the United States are already heavily involved in providing tools and capabilities for such operations: researchers discover and sell vulnerabilities, implants (i.e., "spyware" or "malware"), and associated infrastructure to domestic law enforcement[41], foreign intelligence, and military organizations[42]; brokers and middlemen set prices and control supply chains; and defense contractors and boutique firms create and maintain tools for government customers.[43]

The U.S. government (intelligence community, military, and law enforcement) purchases cyber capabilities. Some of these government contracts result in the development of single tools or exploits, or even black-box capabilities used by the government: products that are "end-to-end" software suites enabling the user of the software to gain remote access to a target computer.[44] Here, the government has control of the CONOP and actual operation, but with varying levels of technical granularity, as the tooling available limits what is technically feasible, and black-box solutions may not showcase how exactly the target is being broken into. Many of the contract vehicles are services contracts (rather than direct product acquisition), whereby the companies are providing engineering resources to develop and manage a bespoke platform or software suite for the government.

This is backed up by CYBERCOM budget reporting: CYBERCOM's Cyber Weapon Payloads (CWP) budget was 160.75 million dollars between October 1, 2024 and September 30, 2025, with 98.6 million estimated for Fiscal Year 2026.[45] The CYBERCOM budget contains many services contracts, stating within line items the imperative to continuously improve "exquisite cyber capabilities being developed by internal and external agencies".[46] CYBERCOM's Cyber National Mission Force (CNMF), the organization charged with defending the nation in cyberspace through full-spectrum operations, specifically acquires capabilities from "a diverse spectrum of sources to contribute technical solutions, services, and tools".[47]

Providing Access:

Private sector actors also directly provide access (i.e., break into a target computer) to enable U.S. government operations.

Private accesses occur frequently in law enforcement cases: prior to the FBI takedown of Qakbot infrastructure in 2022, the FBI used confidential human sources to infiltrate the e-crime group behind Qakbot.[48] Former and current U.S. government roundtable participants verified that the FBI recruits informants who are directly "hands on keyboard": i.e., private individuals working on behalf of the government, directed by the government. Such FBI informants would likely be authorized to conduct a small number of hacking activities for a finite amount of time via the "Otherwise Illegal Activity" authorization process, which applies to all confidential human sources.[49] Under this policy, the informant still takes on civil and criminal liability risk: the FBI on its own cannot promise or agree to any immunity from prosecution by a Federal or State prosecutor, but can inform the appropriate Court about the informant's assistance to the FBI upon request. Individuals attending the Dartmouth roundtable suggested that the government could purchase "access" to a target[50]: law enforcement purchasing Cellebrite, Magnet Forensics, and other forensic tools is one example of such access: while the product may use particular Android zero-days to unlock phones, the law enforcement is purchasing "access" to the phones through the forensic tool, rather than purchasing the zero-day capability itself.[51]

In such cases, a company is providing access to the government by breaking into a machine on the government's behalf, or providing a tool through which the government can do so. However, the government is still the "trigger-puller"[52], deciding what effect to have on that target machine (i.e., using their access to conduct espionage or create some sort of effect). By providing access, the private sector is widening the options available for the government, but whether that optionality turns into additional trigger-pulling is uncertain: just because a private sector actor provides access to the government does not mean that the government will take action using such access, or take action before the access is no longer available.

Private individuals can also proactively provide access in an ad hoc way, without a formal relationship with the U.S. government. Hacktivists, for example, have proactively broken into criminals' computers to procure evidence for U.S. law enforcement without prompting by the government.[53] In 2000, a Turkish hacker named UnknownUser proactively provided information to the FBI regarding a child pornographer that the hacker had procured by hacking into the individual's computer.[54] In this limited way, private hackers are able to provide some opportunistic accesses to the U.S. government, so long as they continue to act without government direction or supervision. Likewise, the U.S. government can leverage rare instances of private sector visibility that they might otherwise not have.

Creating Effects:

In some circumstances, government contractors are specifically hired by the government to create effects in cyberspace. Roundtable participants stated that government services contracts in offensive cyber can include direct staff augmentation, whereby defense contractors sit co-located with government officials and conduct cyber operations with varying levels of oversight.[55] In this sense, the defense contractors directly staff operations, conduct operations on behalf of the U.S. government, and legally carry the authority of the agency in doing so.

Many government contractors are already open about providing services for offensive cyber operations, although most are reluctant to state whether they actively conduct the operations themselves. As an example, Nightwing[56] is a defense contractor with 2,200 employees[57] that provides "people, products, and processes" for offensive cyber operations, and advertises their ability to "sustain physical and virtual operations in hostile environments".[58] The CYBERCOM budget also corroborates the existence of staff augmentation and expertise. CNMF was budgeted 52 million dollars in 2025 to acquire, deploy and improve "expert contract services" for Joint Task Force ZERO, the organization charged with "rapid access generation" into target devices for CNMF.[59] Because the contractors are embedded as additional staff within government operations, it is highly likely that the government is still creating the CONOP and overall direction of the operation from the top-down.

Separately, some private sector actors have already created effects against threat actors in cyberspace without providing the government notice or enough opportunity to provide guidance. This has resulted in varying U.S. government responses. Hack and leak operations have likely been conducted by private individuals[60] with limited pushback from the U.S. government. Campaigns by researchers to "scambait" cyberscammers through a variety of legal and illegal means have also resulted in no public researcher arrests.[61] However, when a U.S. security researcher took down North Korea's internet for a few days in 2022 (in response to North Korean hackers targeting him individually[62]), the FBI found the researcher responsible, and reprimanded him for doing so.[63]

C. The U.S. Government Conducts Cyber Operations via Intelligence, Military, and Law Enforcement with Private Sector Assistance

The U.S. Government, like the private sector, is not just one monolith - intelligence agencies, military, and law enforcement all leverage the private sector to achieve a variety of goals in cyberspace.

Intelligence

The American public (and, in some senses, the rest of the world) first learned about U.S. cyber operations through leaks of U.S. intelligence operations. Stuxnet in 2010, and the Snowden leaks in 2013 (which were some of the first mentions of NSA's Tailored Access Operations Unit)[64] were some of the first indicators that the U.S. government was conducting operations in cyberspace. The U.S. intelligence community gathers intelligence on foreign threats to the United States, and purchases a wide variety of software[65] and offensive capabilities[66] from the private sector to do so.

To collect intelligence via cyberspace, intelligence officers must obtain access to a target's device and remain undetected. The U.S. intelligence community is excellent at doing this: leaked documents[67] and open industry talks[68] show that the U.S. has conducted highly sophisticated, long-term intelligence operations. Multiple former government, current government and industry participants of the roundtable asserted that this intelligence-focused mission of U.S. cyber decisionmakers may prevent parts of the intelligence community from being more public with cyber operations.[69] Intelligence officers culturally pride themselves on being covert and undetected: so much so that NSA used to be known as "No Such Agency" prior to the Snowden leaks.[70] This culture is likely changing over time, however: the intelligence community has worked more openly and closer with private sector partners in the last decade (particularly the NSA, whose mission encompasses both providing signals intelligence and enabling computer network operations to gain a decisive advantage for the nation).[71]

When the intelligence community has decided to conduct an effect in cyberspace, it does so for cases deemed to have long-term geostrategic value. Stuxnet, the alleged U.S. and Israeli cyber operation to sabotage Iranian nuclear centrifuges, is such an example.[72] This is by design: the intelligence community's covert action authorities (codified in Title 50 U.S.C. § 3093 and executed under presidential findings) govern intelligence operations intended to influence conditions abroad while preserving U.S. deniability. Covert channels enable clandestine cyber effects but are structurally incompatible with private sector collaboration, because statutory secrecy requirements prevent market signaling, liability frameworks, and other transparency necessary for sustained private participation.

The intelligence community is likely reluctant to create effects in cyberspace when conducting that operation may compromise accesses they could use for intelligence gathering.[73] In any intelligence operation, causing disruptions to adversaries requires a cost-benefit trade off vis-a-vis intelligence gain or loss. This is particularly the case if the capability required to gain access was expensive, and the access may be "burned" (i.e. discovered) while conducting the effect.[74] Put simply, if the U.S. government acquires an expensive capability to conduct a cyber operation - like an exploit chain worth ten million dollars, using that exploit chain to create an effect may be less appealing than using the same capability to collect a year's worth of intelligence.[75]

Military

On the military side, the mission of CYBERCOM is to conduct operations that may produce effects.[76] However, while CYBERCOM has been involved in providing cyber support to traditional, kinetic military activities (such as the U.S. strikes on Iran's nuclear facilities in Operation Midnight Hammer[77]), or conducting operations in response to non-cyber activities, there have been few details released. The last public example was Operation Glowing Symphony almost eight years ago - when CYBERCOM took down ISIS's media operations online in 2016-2018 and made it difficult for ISIS to operate on the Web.[78] Instead, most public operations attributed to CYBERCOM are "Hunt Forward Operations" - defensive cyber operations designed to detect malicious activity in partner government networks, at the request of the partner government.[79]

While the Commander of CYBERCOM has both Title 10 (military) and Title 50 (intelligence) authorities through his dual hat, CYBERCOM's platforms and tools used in cyber operations differ from those in the intelligence community.[80] This is not just for legal reasons, but also because the capabilities have differing contract organizations (i.e. private sector companies) and try to not overlap capability.[81] Any "Title 10 vs. Title 50 debate"[82] is important for both determining legal authority (i.e., who within the Department of War will conduct the operation and if the purpose is for intelligence collection or military purposes), and dictating the tooling and platforms used.

Unfortunately, CYBERCOM's Title 10 capabilities and operational abilities may be less developed than those of their Title 50 counterparts. CYBERCOM's "Joint Cyber Warfighting Architecture" (JCWA) platform has been plagued with interoperability and usability issues, some of which are still being fixed.[83] If given the option between two platforms, a roundtable military participant suggested that DOW may easily prefer to use the more developed platform – likely one used for intelligence operations, rather than the military platform designed to produce military effects), which may dictate how they plan their CONOP from the beginning.[84]

Moreover, multiple[85] public reports on the shortage of qualified personnel at CYBERCOM[86] suggest issues with CYBERCOM's ability to "man, train, and equip": in other words, there are not enough individuals in uniform to adequately meet CYBERCOM job requirements (man), not enough effective tooling to break into systems critical to the mission (equip), and current staff is not consistently well-trained enough in the current tools to fulfill the mission (train). This has resulted in calls for a "cyber force" to more formally create a cadre of military cyber operators.

This is a particularly interesting dynamic for the private sector, as the US military has recently received a 1-billion-dollar budget increase for its offensive cyber operations, which could filter into new acquisitions from private sector companies. However, shortage of internal manpower and underdeveloped platforms suggest that any products or services produced by the private sector for this branch of the U.S. government may have limited impact. In fact, a lack of qualified USCYBERCOM acquisition officers could likely result in the acquisition of more expensive products, but poor product-mission fit.

Law Enforcement

The FBI and U.S. Secret Service has dual responsibilities in law enforcement and intelligence. FBI has both purchased and utilized private sector offensive cyber capabilities[87] to further investigations: the FBI acquired an exploit from a private company to unlock the San Bernardino mass shooter's iPhone, and subpoenaed commercial spyware company FlexiSpy to investigate and then arrest El Chapo, a notorious Mexican drug lord.[88] The FBI also purchases hands-on forensics tools, such as Magnet Forensics[89] and Cellebrite[90], that provide access to locked phones.

When the U.S. has decided to create public effects in cyberspace, it has largely decided to do so via federal law enforcement takedowns - although most of them are likely not done via "offensive cyber". The DOJ indicts and arrests individuals that commit computer crime against U.S. targets (which include both e-crime groups[91] and members of foreign intelligence organizations[92]). It also seizes malicious infrastructure and stolen assets: the DOJ has conducted cryptocurrency seizures by serving a seizure warrant to third party cryptocurrency platforms.

It is possible that some crypto-seizures require breaking into foreign criminals' machines. While some seizures of cryptocurrency (domestic or foreign) are possible via serving warrants on a cryptocurrency platform,[93] other seizures of "unhosted" wallets require law enforcement possession of a foreign criminal's private key or seed phrase.[94] Individuals usually write their seed phrases on paper, or save a digital copy (on their laptop or in the cloud). On October 2025, the FBI, in concert with the U.S. Department of Treasury and the UK government, seized

unhosted wallets containing $15 billion U.S. dollars owned by a Cambodia-based online investment scam empire – becoming the largest single amount of cryptocurrency seized by law enforcement. [959697] According to the indictment, Chen personally maintained all the private keys and seed phrases for his unhosted wallets.[98] To obtain possession of these seed phrases, law enforcement would either have needed 1) an informant with physical access to obtain the criminal's private key or seed phrase; or 2) an individual (either in government or an informant) with the ability to break into the criminal's laptop or cloud drive to obtain them. Ergo, while there are no details of how the private keys were obtained, it is possible that the largest cryptocurrency seizure in history involved hacking, although a physical seizure is also equally possible.

Law enforcement seizures[99] and searches[100] of domestic-linked infrastructure are done with a similar process as domestic cryptocurrency seizures – serving warrants on third-party platforms. When infrastructure is not owned by a U.S. company or physically located in the U.S. however, the investigation is often processed through informal requests, or through Mutual Legal Assistance Treaties (MLAT): a notoriously slow and laborious process between U.S. law enforcement and international law enforcement partners.[101] There are some distinct successes from this process when partners are willing to collaborate: U.S. law enforcement has collaborated with private companies and Interpol in Operation Endgame, dismantling key infrastructure behind malware used to launch ransomware attacks.[102] The FBI also worked with the Dutch police to tap into El Chapo's servers (which were transferred to the Netherlands from Canada by a confidential informant at the FBI's request).[103][104]

D. Venture Capital Largely Invests in Defensive over Offensive Cyber, Because Offensive Cyber is Traditionally Research Heavy and Service Contract-based

Offensive cyber companies, like other firms that rely on government contracts, often need assistance and private funding prior to their first sale.[105] While some reports have focused on private equity investment in established offensive cyber companies, very little has been reported on venture capital and initial seed investment for new firms entering the market.[106]

Despite heightened venture capital interest in dual-use and offensive technologies[107], most funding interest in cyber remains relatively concentrated on defensive cyber solutions.[108] Portfolios of venture firms like In-Q-Tel still overwhelmingly favor commercial defensive or dual-use technologies[109].

VCs and industry participants of the Dartmouth roundtable stated this is likely because commercial defensive technologies have clearer market applications and predictable revenue streams than their offensive counterparts.[110] This is particularly the case for vulnerability

research, as one cannot know in advance what vulnerabilities will be found or how long they will remain viable.[111] Pure-services businesses are difficult for venture funds to justify because they don't scale well, rely on a small number of high-value clients, and lack the recurring-revenue predictability required to support a classic VC return model. Companies have also historically struggled to create offensive businesses that mimic a subscription software model with annual recurring revenue because offensive work tends to become services-heavy, where customers pay for expertise and time, not a reproducible platform.[112]

Moreover, offensive firms have added problems of customer concentration risk, which limits potential growth and investor returns. Offensive firms often rely on only a handful of large government or prime-contract customers, whereas defensive firms can sell to most customers, public or private, domestic or international. This concentration of mostly-USG and FVEYs customers means that a single procurement shift, policy reversal, or declassification decision can wipe out revenue overnight.[113] This dependence on only a few government customers also narrows exit options - offensive companies are unlikely to IPO, likely getting purchased instead by a larger defense prime, or by private equity firms: Boldend[114], Azimuth, and Kudu Dynamics[115] are all small to medium-sized offensive firms who were acquired by larger defense companies in the last five years. NSO Group, a large Israeli access-as-a-service company linked to human rights abuses, was purchased by a U.S. private equity firm in both 2014 and in October 2025.[116]

Offensive companies can find broader exit opportunities when they pivot their business to focus largely on defensive use-cases: Endgame, once called the "Blackwater of Hacking"[117], brought in CEO Nathaniel Fick in 2012 to grow the company's commercial and federal offerings[118], and was acquired by Elastic in 2019. By this time, the company had largely pivoted to providing "endpoint protection, detection, and response".[119] This optionality does not necessarily translate into additional profits however (Endgame was acquired for $234 million dollars via Elastic shares and debt payments, while Kudu was acquired in a $300 million all-cash acquisition).[120]

As a sidenote, many investors also enjoy seeing observable results: a roundtable participant remarked that secrecy resulting from often-classified, intelligence-based contracts with the government made showing investors such results difficult.[121]

The Offensive Cyber Industry - Gaps and Opportunities

1. **Gap**: The U.S. Government's Current Avenues to Bring Private Sector into Offensive Cyber Do Not Create Enough Outcomes, Particularly for Bottom-Up Opportunities

The United States intelligence, military, and law enforcement is optimized for deliberate, tightly scoped, top-down operations in cyberspace. However, this does not create offensive cyber outcomes at the tempo asked for by U.S. policymakers. Moreover, while the private sector can act on new bottom-up, time-sensitive opportunities created by adversary error, the government's operational tempo likely cannot keep up.

The intelligence community's structure values long-term clandestine activity, and its culture dislikes creating short term effects, especially if it risks burning an expensive capability. CYBERCOM's ability to deliver effects at scale is limited by persistent issues with tooling and manpower. Finally, law enforcement agencies, primarily the FBI and the Department of Justice (DOJ), are the most visible executors of U.S. cyber operations, but are limited by their very mission and authorities. Taken together, these institutional silos produce a fragmented ecosystem that does not support operations at a scale needed to compete in cyberspace. As a result, when time-sensitive opportunities emerge internally, the U.S. may lack the procedural and legal infrastructure, or even resourcing, to act decisively.

Moreover, the U.S. government's current structure for leveraging private actors (rigid contracting, recruitment, or proactive vigilantism) produces pockets of technical excellence, but this is not a scalable system for rapid, lawful, and repeatable offensive cyber operations, either via top-down tasking or bottom-up opportunity. Much of the nation's offensive tooling remains locked behind bespoke service contracts instead of scalable, interoperable platforms. Confidential human sourcing relationships are highly individualized, time-bound, and fraught with legal ambiguity. Private sector effects are either strictly overseen by the government in a top-down manner, or take the government by surprise outside government channels. This shows a clear gap: there is a distinct desire by policymakers to scale our cyber offenses, but no large-scale channels for the U.S. government to work with private entities to do so.

2. **Opportunity**: Private Sector is Capable and Willing to Provide Offensive Cyber Capabilities and Access at a Larger Scale than Currently Utilized

Fortunately, the private sector already possesses the technical skill, tooling, and operational experience required to deliver both exquisite and low-equity offensive capabilities, as well as rapid, timely, and at-scale access, and is willing to provide more capability and access to the government.

Capabilities / Tools

Multiple venture capital and industry roundtable participants agreed that there is an opportunity in the U.S. market to build a handful of private sector firms to disrupt the services and defense-prime heavy model of offensive cyber tooling: shifting away from bespoke services to something that's more product focused, which can also be a better business model for private funding.[122]

Companies have already recast defense technology as a product in other spaces. For example, Anduril has become the darling of the defense technology space by making a single but substantive change to the defense prime business model: they did not rely on services contracts to do research. Instead, Anduril conducted private research and development investment upfront, and delivered ready-made systems to bypass slow procurement cycles.[123]

The private sector's capacity to field offensive cyber effects is already real and multifaceted: firms can simultaneously pursue low-equity, high-volume capabilities (leaked credentials, logging misconfigured buckets, etc) as well as exquisite, tailored zero-days that require deeper research and engineering. In practice, these are not mutually exclusive, particularly if AI becomes an enable of scale in this space. Multiple roundtable participants agreed that automation and AI will also likely become central enablers of that scale.[124] Industry has already begun to integrate LLMs and fuzzing into offensive R&D workflows and security contests.[125]

This duality of high and low-equity capability is important because not every mission requires the same fidelity or risk posture; what matters is matching capability to objective, having "things on the shelf" that are expressly designed for the mission they will be asked to accomplish, or being able to quickly create a tool when an operation takes an unexpected turn.

Access

The private sector is also likely willing to create additional companies who have the trust and ability to provide actual "access" to the government, via breaking into systems on the government's behalf.

Some of this can be trivially combined with the low-equity capabilities provided above: if

one has a breached credential, for example, it is easy to see whether or not the credentials actually work (thus obtaining unauthorized access to a target machine). Success at scale requires an in-depth understanding of adversary systems and defensive processes: in practice, that means opportunistically targeting low-level accesses at a high enough quantity to achieve mission impact, while building pipelines that integrate data and capability acquisition, safe testing, and rapid deployment.

The economics would be incredibly compelling to firms entering the market if the right procurement and incentive structures are put in place. For one, smaller firms who productize offensive cyber accesses could potentially disrupt services contracts largely only obtainable by prime contractors - thereby making a profit, reducing inefficiencies in procurement, and passing on cost savings to the government.[126] By creating access platforms rather than services, the companies would also likely be more attractive for VC investment.

Providing access could also unlock additional, albeit more unconventional, value pools. For example, creating a bounty model for crypto asset seizure and recovery could be an enormous moneymaking opportunity for upcoming firms if properly authorized and governed. Because these accesses could be conducted through a product and have more regular payouts, venture capital and other investors would be far more interested in investing.

Of course, there are a number of legal risks in this business model. For private firms, the Computer Fraud and Abuse Act (CFAA) is the primary legal barrier against accessing target devices, as the statute criminalizes unauthorized access to computer systems. From deploying an exploit to taking advantage of cloud misconfigurations, all are illegal hacking under the CFAA if done without authorization.[127] This means that gaining access creates criminal and civil liability exposure, both domestically or internationally. While the CFAA provides an exception for "lawfully authorized investigative, protective, or intelligence activity of U.S. law enforcement or intelligence agencies," this has never been openly defined or tested in a court of law.[128] Moreover, authorization likely occurs under classified circumstances, upping concerns around greymail and preventing firms from talking more openly with lawyers or investors in the market.[129]

However, many organizations are already living with this legal exposure - as stated previously, both individuals and firms are already providing accesses to the U.S. government. Even more firms in the defensive cyber security industry, like the bug bounty industry, conduct security research in a way that exceeds authorized access. DOJ likely does not prosecute such private firms simply because doing so currently "does not serve U.S. government interests."[130] Multiple roundtable participants also remarked that juries are unlikely to want to convict an individual or organization who went after a cybercriminal actor - but this could change if unintended harm was to result from such private sector access.[131]

Roundtable participants remarked that concerns about escalation[132] and reputational risk, and security concerns for both government and private sector are often overstated in policy discussions.[133] For example, while the risk of reputational harm and security concerns are still high, many defense contractors and security firms already operate in contested environments and accept certain operational risks: for example, North Korea and other state actors already routinely target offensive security researchers for their tools alone, and companies have altered their OPSEC stances accordingly.[134]

In short, both the technology and the capital exist; what remains is creating policy and legal protections, oversight mechanisms, demand signals, and procurement vehicles so that private firms can build credible, investible offensive cyber platforms that deliver predictable national-security outcomes.

3. **Opportunity**: The Private Sector is Capable and Willing to Provide Additional Effects against Lower-Tier Targets if Provided with Adequate Civil Liability, Oversight, and Other Protections

Private sector actors are also likely willing to provide rapid effects for the U.S. government against limited, lower-risk targets, but would need additional liability and safety assurances, as well as oversight mechanisms. Letting the private sector conduct such activity would free up government resources for the U.S. to focus on more high-priority targets. Dartmouth roundtable participants largely showed very little enthusiasm for private sector operations independent of direct government tasking.[135]

Despite certain policymakers' insistence that private sector effects would 'unleash the private sector' against China, the private sector may demur from targeting actors that are perceived as higher risk, either to individual researcher safety or to geopolitics writ large. Industry participants noted that the risk to physical safety differs based on the actor: while targeting North Korea, lower-tier China-affiliated actors, and ransomware actors would likely not create a threat to a researcher's life (and be safe for companies to go after), some cartels (and certain other China-based organizations[136]) may have the resources to retaliate with direct physical violence, therefore bringing too great of a risk.[137]

However, roundtable participants seemed encouraged by a program whereby private sector actors could opportunistically target threat actors that are lower risk to researcher safety and geopolitics. Private sector participants also stressed the need for some oversight and optional approval mechanism, to ensure that they were 1) not interfering with ongoing government operations; 2) not accidentally violating other federal laws (like the Wiretap Act or ECPA), or even 3) conducting their operation in an otherwise safe and tailored manner.[138] Although, as seen in the law enforcement deputation case re: FISA above, there are likely mechanisms through which government can provide that oversight. Government participants

suggested that these targets may be of low interest to the U.S. government, especially given resources that could be required to oversee private actors.

Regardless of program or target, civil liability would likely remain the heaviest deterrent for private companies. Creating an effect on a machine can count as "damage" under the CFAA and creates further exposure to criminal and civil liability - particularly if the effect has unintended consequences. Third-party infrastructure operators, cloud providers, or foreign entities can already easily sue firms that are found exploiting Western technology systems under the law.[139] Many such cases already exist in the bug bounty industry, where software vendors have issued coercive cease and desists against individual bug-hunters conducting defensive research.[140] Despite DOJ efforts to create a "good faith security research" non-prosecution policy, researchers reported that the threat of lawsuit creates a chilling effect that persists, as the policy does not provide the same cover as full statutory protection. As several noted, "it's a policy, not a law".[141]

Roundtable participants disagreed on how much liability protection the private sector would need, however - particularly if the private sector makes a mistake. One participant captured the sentiment clearly: "I'm not going to sign a contract for a company of mine that says if they do something related to the U.S. government, the U.S. government has carte blanche to sue them if they hit the wrong target."[142]

Thus, the U.S. government has an opportunity to create a legal and/or regulatory oversight and approval model that would allow for the private sector to act more opportunistically in cyberspace against lower-risk actors, while giving the U.S. government enough control over the process to ensure minimal collateral damage.

4. **Gap**: The U.S. Government Lacks Transparency to Signal Clear Demand for Offensive Cyber

The U.S. government is capable at recruiting highly skilled individuals and signing contracts with large prime contractors.[143] However, it has not yet produced a strong enough demand signal in offensive cyber for funding and capital to flow to effective teams.

There is currently no public U.S. government-led, programmatic commitment that tells investors and entrepreneurs, "build an offering in offensive cyber, and we will buy and sustain it." The result is that capital flows toward defensive, productizable technologies while offensive work remains underfunded and ad hoc.

For investors and businesses to increasingly enter the space, they need clearer policy signals to know what the government needs, in order to decide what to fund or build. Without crisp mission descriptions and outcome metrics, even sophisticated participants struggle to see

how their efforts contribute to national objectives. When government strategy and requirements are opaque, only seasoned insiders can parse the signal—most investors are not seasoned insiders, and will not commit capital in the face of such ambiguity.[144]

That weak demand signal is compounded by complexity and secrecy. Offensive cyber work by necessity blends capabilities, authorities, and agencies, and much of that activity is classified. That secrecy is antithetical to what private-market investors require: VCs want to understand what a company builds, which public-policy problems it addresses, and what repeatable revenue model supports an exit.[145]

5. **Opportunity**: Research Institutions on Software Understanding and Offensive Security Can Fast Track New Research to create Emerging Solutions

Weird machine theory suggests that 1) the complexity of an attacked program works in favor of the attacker;[146] and 2) understanding any program to build secure systems requires an understanding of the very system's exploitability.[147] Despite the centrality of software understanding to both national security and technological competitiveness, academic and government R&D programs still prioritize applied IT and defensive cybersecurity over offensive research, or even dual-use analysis of how modern software systems actually behave and fail.[148] Currently, only a few American universities, like Dartmouth, teach software understanding techniques, which encourage study of protocol interaction, execution flow, timing, and logic errors that adversaries themselves rely on. This opens the door to active cyber countermeasures: deliberately constructing environments that absorb, study, and neutralize hostile activity without escalation or attribution risk.

In an era where offensive advantage depends on speed, automation, and creative improvisation, only institutions that understand how systems work (via weird machine theory, or software understanding) will be able to anticipate and exploit those emergent properties before adversaries do. Prioritizing this field within universities and research centers ensures that future operators, analysts, and policymakers can move from reacting to intrusions toward designing resilient, adaptive systems—and, when necessary, using that understanding to shape adversary behavior in ways that protect national interests. Understanding wider systems (not just software itself) could also lead to additional discovery of ephemeral accesses, or even additional opportunities to affect the environment that do not require offensive cyber at all.

Recommendations - Leveraging the Future of Offensive Cyber in the Private Sector

The next phase of offensive cyber power will depend not on finding the next zero-day, but on finding a model (legal, financial, and cultural) that can harness all forms of offensive cyber at scale. Thus, the following recommendations are offered based on the Dartmouth roundtable's key findings:

1. Develop a Public Offensive Cyber Strategy

Overall, the United States has reached a strategic inflection point in offensive cyber operations. The current approach, driven by ad hoc relationships, bespoke contracting, and opaque processes, cannot scale to meet the demands of modern conflict and persistent engagement. The White House must unify these ad hoc approaches under a single, public offensive cyber strategy.

Calls for a national offensive cyber strategy have been made for the last two decades: such an effort could transform this patchwork into a publicly declared, organized ecosystem, aligning private innovation, cooperation with international allies, and government capability development under a shared vision and clear demand signal.[149]

By articulating a vision for offensive cyber, the government can clarify boundaries between lawful, strategic operations and reckless disruption, while also distinguishing U.S. practice from that of adversaries such as China, North Korea, or Russia, whose private sector offensive approaches often introduce systemic risk to global networks.[150] Clear strategic outcomes could include: enhanced and scaled US offensive-cyber supply chains, a long-term and strengthened offensive cyber talent pipeline derived from the private sector, clear operational divisions of responsibility between government and the private sector in cyberspace, and long-term degradation of adversary capability.

A mature strategy must also expand the policy imagination of what offensive cyber is for. Cyber operations should not be conceived solely as counter-cyber measures. The U.K. has already acknowledged that it uses cyber "for a range of foreign, military, and public objectives," not just in retaliation for digital incidents.[151] Likewise, U.S. doctrine should view cyber as a proactive instrument of statecraft, applicable across domains. That requires better pairing of capabilities to goals—a recognition that high-value targets like Natanz merit billions in investment and covert authorities, while other objectives require faster, noisier private sector effects.

Being more transparent would also enable better coordination, policy alignment, and targeting across international partners and the Five Eyes alliance. This is particularly timely as

Australia invests more into its offensive cyber capabilities[152], and the UK considers the future direction of its National Cyber Force. The UK's National Cyber Force has deliberately published its principles of responsible cyber power in practice, framing offense not as a rogue instrument but as a calibrated tool of statecraft, designed to be accountable, precise, and calibrated.[153] The U.S. can do the same - as a policy roundtable participant quipped: "we have to stop pretending we don't do things."

This is not a call to increase offensive cyber while ignoring defense - quite the opposite. Currently, the U.S. cyber market favors defensive activity overall[154]: any offensive cyber strategy must naturally work hand-in-hand with defensive efforts. Creating an offensive cyber strategy would enable more explicit conversations with the defensive community, including some of the very same companies responsible for securing US networks, and create clear coordination efforts to ensure that U.S. offensive cyber efforts do not risk undermining our own national security.

In a similar vein, the United States intelligence community and military could also adopt a calibrated policy for taking public credit for certain offensive cyber operations. Law enforcement operations aside, the public record for intelligence and military cyber operations sits at two extremes: high-profile leaks (like Vault 7[155] and the Snowden Leaks), and public announcements of USCYBERCOM activity with little public detail. Thoughtful, evidence-backed transparency would 1) improve deterrent signaling, 2) clarify government responsibility and oversight over such operations; 3) signal to international allies and partners that the government will admit to operations in cyberspace (especially important if an authorized private actor makes a mistake in the future), and 4) create a clearer demand signal to the private sector and allied partners about what capabilities are valued and why. As one participant captured, "if there's a willingness to talk more publicly about [offensive cyber], and a willingness to use it more frequently, you'll actually see much more of a market response."[156]

2. Create a Robust Offensive Cyber Capability Pipeline through Pilot Programs and Accelerators

The United States struggles to obtain capabilities from skilled smaller firms, relying on prime contractors with burdensome overhead costs or bespoke service contracts. Creating accelerators and funding programs specifically for offensive cyber (in all forms) would shift providers of technology towards providing platforms over tailored services.

For more traditional, exquisite offensive cyber capabilities, Vulnerability Research Accelerators (VRAs) through the Defense Innovation Unit (DIU) could significantly bolster the supply of zero-day exploits, particularly if the accelerators are encouraging the use of artificial intelligence and automation throughout the process. Creating additional DOW policies to get

away from multi-year service contracts and towards more Other Transaction Authorities will be essential here.

For more low-equity, platform-oriented approaches, the U.S. government should apply the Anduril model to offensive cyber. Anduril got its first contract through government pilot programs developed by CBP's innovation team.[157] On the funding side, the company was both VC-backed and utilized Small Business Innovation Research programs to grow its business.[158] In this vein, the FBI Operational Technology Division, NSA's IDEAS Program and Small Business Program[159], and DIU should each separately create pilot programs to work with small businesses on the forefront of offensive cyber. Creating additional DARPA SBIR (Small Business Innovation Research)[160] programs for offensive cyber will also be crucial to ensuring platforms are built to meet mission needs.[161]

Applied to offensive cyber, the Anduril model creates an opportunity to incubate a small number of durable, product-first companies that can scale operational tempo to meet government needs. This also makes the market more appealing to investors: VCs will be more comfortable where there is a product with recurring revenue and a scalable platform.

3. Invest in Research on Software Understanding

To ensure long-term national competitiveness in offensive and defensive cyber operations, the U.S. government should prioritize sustained investment in "software understanding" research. Software understanding, derived from weird machine theory, is not just about identifying vulnerabilities; it is about comprehending how systems behave under unexpected inputs and how emergent computational states can be controlled, disrupted, or defended against. This field underpins both exploit development and advanced defensive analysis, yet U.S. research institutions remain chronically underfunded and underdeveloped in this area.

To address this, the U.S. should establish a coalition model for funding and coordination, linking DARPA, NSF, NIST and leading academic institutions in a joint offensive-cyber research consortium. This model would fast-track emerging research from theory to prototype through a combination of rapid prototyping grants, open collaboration frameworks, and DARPA-style microgrants for independent researchers and smaller labs. The program should emphasize low-overhead, high-velocity awards to support unconventional, creative work in areas such as automated exploit discovery, binary analysis tooling, large language model (LLM)-assisted vulnerability research, and behavior analysis of complex systems.

This coalition should also incentivize research that imposes costs on adversaries without crossing into illegal intrusion, such as utilizing LLM-enabled scambaiting[162], programmatically analyzing international standards and attempts to circumvent safety through standards bodies,

as well as other methodologies for analyzing adversary ecosystems at scale.

4. Authorize a Pilot Program for Private Sector Access Operations Against Low-Risk Actors

Finally, for both the U.S. government to move forward into scalable, offensive cyber accesses, the ecosystem needs some balanced allocation of liability between government and private actors, backed by indemnities and defined safe harbors that allow limited, auditable risk-taking, while minimizing collateral damage. For private sector companies to grow in this space, such demands must be public enough to provide company and investor confidence and regulated enough to ensure market stability.

While some programs could be conducted via unilateral executive action, Congress has the opportunity to pass new laws to create the requisite new authorities, shared liability models, and a path for sanctioned cooperation.[163] One option on how an initial program could work is as follows:

Public Bounties for Access (Rewards for Justice with Teeth)

The U.S. should create narrowly scoped pilot programs within the NSA and DOJ/FBI that carves out a legal and operational space for vetted private-sector cyber operations. These operations would be against low risk actors: a limited set of actors that currently evade law enforcement, are hard to combat at scale, but that don't impact long term intelligence or military operations (e.g., pig-butchering scams, e-crime wallets, ransomware infrastructure, clearly illicit crypto-money-laundering firms operating in China, and certain foreign terrorist media operations[164]). The program must be unclassified and public to truly take advantage of the scale of the private sector.

Operational scope must be tightly bounded - this pilot would restrict private action to low-risk foreign criminal or national security targets. Participants noted that cyber actors with civil judgments or indictments against them could already form the start of an initial list.[165] The pilot program would also need links to law enforcement for safety assistance, particularly if certain actors try to retaliate against the private participants. This risk would also be minimized by deliberately choosing targets with low ability to cause physical harm to individuals operating in the United States.

After providing initial access and enough evidence for the government to validate that the access is to a specified target, the private operator's role would end, preserving U.S. government "trigger-pulling". Upon successful validation of access, the government can provide a grant or payout to the private actor. For the U.S. government to effectively be "trigger-pullers", however, NSA and FBI would need additional capacity to be able to take action on accesses

and coordinate with partners in a timely manner: both organizations would need to be staffed accordingly and could create a task force structure to do so. Moreover, standardized contracting templates, evidentiary chains, and handoff playbooks would need to be made so the model can scale without recreating ad hoc legal work every time.

Critics may argue that a program for access (let alone effects, as mentioned below) will be a departure from international norms or a violation of sovereignty. However, this is misleading - for one, access is already purchased and created by private actors globally. Moreover, the harm already occurring to U.S. sovereignty is real: tens of thousands of civilians and businesses are victimized daily by transnational cybercrime, let alone becoming victims to nation-state cyber activity. Doing nothing because the legal tools are slow or because political risk is uncomfortable imposes real, measurable harm.

Two additional issues arise with any pilot program for access: first, the private sector would need some civil and criminal liability protection against other statutory regimes beyond that of an illegal activity waiver, as currently written. Second, the executive branch risks tasking the private sector to violate the law on their behalf, accidentally or otherwise, and private-sector contribution to offensive activity must have clear oversight and reconcile statutory conflicts—between ECPA (which limits data sharing by service providers), FISA (which imposes surveillance oversight), warrant requirements for searches conducted on U.S. soil, and MLAT treaty obligations (if applicable).

Creating safeguards against these issues is already likely possible via unilateral executive action: for liability safeguards, the FBI and NSA could announce that the pilot program is an authorized intelligence activity under the CFAA (thereby publicly sheltering all participants under 1030(f)). However, this likely would not protect the private sector from third party DMCA or other civil claims. Safeguards against accidental violations can be partially resolved through pilot program design: proper target selection by the executive branch, attestation by the private actor that they are abiding with all federal laws in conducting this activity, or ability for the private actor to request for CONOP review prior to obtaining access.

Roundtable participants disagreed as to whether Congressional action would be necessary for a successful pilot program - however, Congress has the ability to create additional liability protection for the private sector, while ensuring adequate oversight and transparency. Reviving past statutes, like CISA 2015, could be another way to protect the private sector from third-party claims: the CISA 2015 information-sharing framework (sunsetted in 2025) included a “no cause of action” clause (i.e. immunity from suits of any kind, civil or criminal) for entities sharing cyber-threat indicators.[166] The term “Cyber-threat indicator” was defined so broadly (even including vulnerabilities) that it could have been possible to utilize the law to protect private-sector offensive capability (or even access) providers.[167] A requirement that the FBI and NSA also publish a public, redacted evaluation of the pilot annually, including lessons learned

and recommended statutory changes, could also be an effective mechanism for Congress, industry, and allies to assess whether to broaden the program.

Crypto-Seizure Accesses - An Initial Case

A law enforcement pilot "access" program against foreign cryptocurrency scammers or thieves may be the best initial use case for five reasons:

First, the legal landscape is more permissive for foreign cryptocurrency seizures than other cases: seizures of foreign assets like cryptocurrency are possible unilaterally, but require either 1) cryptocurrency platform assistance[168] or 2) pre-existing possession of the foreign asset's private key.[169] While some instances will require probable cause that the assets are traceable to proceeds of a crime,[170] the Fourth Amendment does not apply to the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country.[171]

Second, there is already ample private sector appetite to do this. "Scambaiting" communities are already prevalent online, where security researchers "scam the scammers" through a variety of methods.[172] When scambaiters cross the line into illegal activity by hacking into web cameras or scam facilities, there has been a historical lack of law enforcement appetite to go after these individuals.[173] Juries too, are also unlikely to want to convict an individual or organization who goes after a cybercriminal actor.[174]

Third, this case is most in line with current U.S. economic and national security policies.[175] As the U.S. is attempting to become the "crypto capital of the world", actors who are hindering the stability of digital assets by conducting large-scale heists and scams threaten the stability of the crypto market when doing so.[176] The DOJ has had incredible success in seizing foreign assets so far - however, as the cybercrime continues to rise, the number of cyber criminal groups will continue to use cryptocurrency (and in particular, unhosted wallets) that may make seizure at-scale more difficult without private sector assistance, either because there are too many criminals or wallets[177], or because the wallets themselves are difficult to break into.[178] The largest crypto-seizure to date targeted only 6 unhosted wallets (landing a record-breaking seizure of 15 billion dollars). However, FBI reports show that 10-16 billion dollars leave the U.S. every year in crypto scams, tied to a dizzying number of wallets.[179] Current reporting suggests that there are over 75 billion dollars of cryptocurrency on-chain that are linked to criminal activity, with over 40 billion linked to dark web market operators and vendors.[180]

Fourth, private capital and companies are likely to more easily ascertain how to build the

market around such a law enforcement program, because law enforcement is the least secretive of the organizations currently conducting cyber operations.

Finally, organizations that would normally be against private sector cyber action are more aligned when it comes to crypto-theft: unlike traditional Big Tech firms, cryptocurrency platforms have been more aggressive in soliciting private sector assistance to shut down e-crime actors, even providing bounties to do so.[181] Venture capital firms have also invested heavily into cryptocurrency and would likely fund ventures that further protect their investments.[182]

Creating a program whereby an actor could receive 33% of a wallet's contents after a successful seizure would return much of that lost crypto back into the U.S. economy, while creating a new successful cottage industry. Where private operators obtain provable control over criminal proceeds (e.g., crypto wallet seed phrase or private key access), the DOJ must have streamlined processes to secure seizures or mutual legal assistance where necessary. According to a former government roundtable participant, the DOJ has obtained seizure warrants within 24 hours of getting the seed phrase of a wallet[183] - ensuring this kind of tempo continues to be met when the number of accesses expand are key to a program's success.

Because any access program with a bounty could create perverse incentives (i.e., stealing crypto with one wallet to then report it to law enforcement to guarantee a 5% payout), the DOJ would also need to ensure that the unclassified and public program still has an application process, whereby the applicant consents to monitoring of their spending habits and assets.

Creating such an access program could also galvanize private sector and governments worldwide to disrupt criminal activity, simply because they would not want the United States to utilize such a program on its systems or companies. Much of the cyberscam domain relies on friendly government jurisdictions and big technology infrastructure (where scam farms are already violating technology company terms and conditions). Creating the public program could, in of itself, apply pressure to currently obstinate platforms and governments.

Direct, Public Deputization of Trusted Parties

A public deputation regime that creates a small roster of vetted companies to perform limited, government-authorized disruptive actions could allow scaling of offensive cyber while

embedding accountability, auditability, and oversight. This is not a permissive "hack-back" solution: roundtable participants agreed that open-ended, unregulated retaliation would be dangerous and counterproductive. Instead, the pilot would deputize a small roster of trusted companies (that have likely already developed the necessary trust through prior operations, or through the above pilot program) against a government-determined series of targets. The government would provide explicit protections and liability-sharing arrangements so those firms can perform limited, legally authorized disruption activities in support of law enforcement or national security objectives.

From a program perspective, the U.S. government would need to create enough oversight to ensure that each private sector effect is generated in a targeted and defensible way. Because trust is central to the model, deputized entities would face rigorous vetting (security clearances, background checks, and contractual commitments to non-disclosure and controlled handling of tradecraft), rather than the public marketplace displayed above. Private actors who pass vetting should be able to opportunistically propose effects for approval.

Roundtable participants suggested two ways that such deputation or licensing could occur:

1) **Presidential Directive / Military Deputization:**
   A Presidential directive could be created requesting that CYBERCOM deputize private actors to target lower-risk APT groups that are a threat to the DODIN. This could behave as a stop-gap or supplement for cyber force initiatives as CYBERCOM builds its own capacity, while also integrating private actors into CYBERCOM processes, and interagency or international coordination. To keep domestic and foreign activities separate, such a program would have to involve passing off domestic accesses and information sharing to federal law enforcement where appropriate. However, public oversight over such actors would likely be limited with such authorities.

2) **Cyber Letters of Marque or Other Statutory Licensing Regimes**
   Congress could authorize a licensing framework—drawing on Section 1030(f)/CFAA principles or a new standalone statute—that explicitly permits specified classes of otherwise-illegal computer access and disruption when performed under a government-approved mission and rules of engagement. Roundtable participants were most divided over whether new Congressional action in this way would be either beneficial or realistic. However, legislation crafted by Congress would be one method of providing the balance of transparency and oversight advocated for by private sector actors, while also creating a new framework not tied down by covert intelligence cultures, underdeveloped military platforms, or law enforcement's limited authority.

Conclusion

The United States has an opportunity to move from ad hoc to architecture in offensive cyber, by building a coherent framework that transforms ad hoc, personality-driven coordination into an enduring system of national capacity. The gaps are clear: the U.S.'s underdeveloped, opaque legal architecture chills private-sector initiative, its fractured government ecosystem cannot move at the pace of emerging threats, and its research environment undervalues software understanding — the very foundation of offensive and defensive innovation alike.

Yet the opportunities are equally clear. The United States has an unparalleled combination of private-sector expertise, technical talent, and free-flowing capital. A national offensive cyber strategy that defines acceptable behavior, signals consistent demand, strengthens allied coordination, and establishes lawful channels for private participation would enable the government to act quickly and proportionally while maintaining accountability and oversight. By investing in pilot programs, accelerating research on software comprehension, and pursuing statutory or executive mechanisms to safely deputize trusted private partners in access (or even effects), the U.S. can operationalize a new model for responsible offense.

Ultimately, America has capability, it just needs to remove the chaos that surrounds it. The challenge before policymakers is not to invent new talent or technology, but to create the legal, institutional, and market infrastructure that enables growth. Building that framework will enable a more agile, ethical, and scalable approach to offensive cyber power - one that reflects democratic values while securing national interests. In short: build the framework, and the capacity will follow.

About the Authors

Winnona DeSombre Bernsen is nonresident fellow at the Atlantic Council, and the founder of offensive security conference DistrictCon. She holds a Master of Public Policy from Harvard Kennedy School and a Juris Doctor from Georgetown Law. Winnona was formerly a security engineer at Google's Threat Analysis Group, tracking targeted threats against Google users. In recent years, Winnona has organized content at hacker conferences (including being a presenter for the Pwnie Awards) and has authored multiple pieces on offensive cyber capability proliferation.

Sergey Bratus is the Dartmouth College Distinguished Professor in Cyber Security, Technology, and Society and an Associate Professor of Computer Science. In 2018--2024 He served as a Program Manager at DARPA's Information Innovation Office (I2O), where he created multiple fundamental research programs in cybersecurity, resilience, and sustainment of critical software. Sergey is interested in identifying and eliminating the root causes of software vulnerabilities, and believes that this requires connecting state-of-the-art hacking with fundamental concepts of computer science. He believes that edge-of-the-art hacking has developed into a distinct discipline of computer science, even though not formally recognized as such, and that studying it is indispensable for building future computing systems we can finally trust.

Acknowledgements

The authors would like to thank Dartmouth ISTS for hosting the roundtable, and the participants who came to the Dartmouth roundtable, provided valuable insights, and provided feedback on subsequent paper drafts. Particularly special thanks to Mary Brooks: without her editing and moderating assistance prior to, during, and after the roundtable, this paper would not have materialized.

Endnotes

[1] John Sakellariadis, *Republicans want US companies to hack back against China*. POLITICO Pro, June 9, 2025. https://subscriber.politicopro.com/article/2025/06/republicans-want-u-s-companies-to-hack-back-against-china-00394646

[2]David Dimolfetta. *Contractors could hack back against adversaries, top cyber Democrat says.* Nextgov/FCW, April 2, 2025. https://www.nextgov.com/cybersecurity/2025/04/contractors-could-hack-back-against-adversaries-top-cyber-democrat-says/404233/

[3] Greg Otto*. National Security Council cyber lead wants to 'normalize' offensive operations*. CyberScoop, May 1, 2025. https://cyberscoop.com/alexei-bulazel-white-house-national-security-councial-destigmatize-offensive-cyber-rsac-2025/

[4] Sezaneh Seymour, Brandon Wales. *Partners or Provocateurs? Private-Sector Involvement in Offensive Cyber Operations.* Lawfare, July 16, 2025. https://www.lawfaremedia.org/article/partners-or-provocateurs--private-sector-involvement-in-offensive-cyber-operations

[5] Matt Seldon. *Emily Goldman Set to Join National Security Council's Cyber Office.* HSToday, March 10, 2025. https://www.hstoday.us/subject-matter-areas/cybersecurity/emily-goldman-set-to-join-national-security-councils-cyber-office/

[6]Cyber Persistence Theory, coined by Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett in 2022, states that the key to security in cyberspace is to proactively engage in operations and campaigns that identify vulnerabilities, preclude exploitation, and enable mitigation. Greg Otto. *America's allies are shifting: Cyberspace is about persistence, not deterrence.* CyberScoop, October 2, 2024. https://cyberscoop.com/cybersecurity-deterrence-persistence-richard-harknett-dod-strategy/

[7] "In 2018, U.S. strategic guidance in the National Security Strategy of the United States of America (NSS) shifted to emphasize the significance of this competitive space, and USCYBERCOM prescribed a strategic approach of persistent engagement." Michael P. Fischerkeller et. al, *Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.* The Cyber Defense Review. 2019. Accessed October 14, 2024, https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf

[8]USCYBERCOM's strategy of persistent engagement (announced prior to Cyber Persistence Theory but which applies many of the same concepts), led to hunt forward operations in Ukraine, in which cyber operators constantly work to intercept and halt cyber threats, while degrading capabilities of adversaries. Michael Fischerkeller, Emily Goldman, Richard Harknett. *Cyber Persistence Theory in the Russo-Ukrainian war.* Binding Hook. November 7, 2023. https://bindinghook.com/cyber-persistence-theory-in-the-russo-ukrainian-war/. U.S. Cyber Command PAO. *CYBER 101—Defend Forward and Persistent Engagement.* U.S. Cyber Command, Oct. 25, 2022. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

[9] Greg Otto. *National Security Council cyber lead wants to 'normalize' offensive operations.* CyberScoop, May 1, 2025. https://cyberscoop.com/alexei-bulazel-white-house-national-security-councial-destigmatize-offensive-cyber-rsac-2025/

[10]*Desktop vs Mobile Market Share Worldwide.* StatCounter Global Stats. Retrieved October 7, 2025, from https://gs.statcounter.com/platform-market-share/desktop-mobile/worldwide/2010

[11] *Complexity is killing software developers*. InfoWorld. Retrieved October 7, 2025, from https://www.infoworld.com/article/2270714/complexity-is-killing-software-developers.html

[12] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace.* Atlantic Council, June 25, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

[13] Sergey Bratus et al. *Exploit Programming: From Buffer Overflows to "Weird Machines" and Theory of Computation.* Langsec, December 2011. Retrieved October 7, 2025 from https://langsec.org/papers/Bratus.pdf

[14] Ian Beer. *Blasting Past Webp: An analysis of the NSO BLASTPASS iMessage exploit*. Google Project Zero Mar. 26, 2025. https://googleprojectzero.blogspot.com/2025/03/blasting-past-webp.html
[15]Ben Hawkes. *The WebP 0day*. Icosceles, Sep 21, 2023. https://blog.isosceles.com/the-webp-0day/
[16] Ian Beer & Samuel Groß. *A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution*. Project Zero, December 15, 2021. https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html
[17] Sergey Bratus et al. *Exploit Programming: From Buffer Overflows to "Weird Machines" and Theory of Computation.* Langsec, December 2011. Retrieved October 7, 2025 from https://langsec.org/papers/Bratus.pdf
[18] Sergey Bratus. *What hacker research taught me.* Dartmouth College. Retrieved October 7, 2025 from https://www.cs.dartmouth.edu/~sergey/hc/rss-hacker-research.pdf
[19] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace.* Atlantic Council, June 25, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/. Corroborated by Dartmouth ISTS Offensive Cyber Roundtable, remark from current industry participant, October 3, 2025.
[20] Dartmouth ISTS Offensive Cyber Roundtable, remark from current industry participant, October 3, 2025.
[21] DARPA has invested heavily on AI-enabled creation of exploit chains, as well as automated identification and patching of vulnerabilities. While defensive in focus, the DARPA AIxCC competition showcased multiple teams that were able to create valuable bug reports and patches using AI systems, submitting patches in an average of 45 minutes with an average cost of $152 per task. While submitting patches is clearly a defensive activity, identifying vulnerabilities is dual-use and could be applied to more offensive pursuits. *AI Cyber Challenge marks pivotal inflection point for cyber defense.* DARPA, August 8, 2025). Retrieved October 7, 2025, from https://www.darpa.mil/news/2025/aixcc-results
[22] Mark Ellzey. *Using Censys to Find Misconfigured S3*. Censys, Jan 3, 2023. Retrieved October 7, 2025, from https://censys.com/blog/using-censys-to-find-misconfigured-s3
[23] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry, academic, former government, and current government participants, October 3, 2025.
[24] Department of Defense Fiscal Year (FY) 2026 Budget Estimates. U.S. Cyber Command. Retrieved Oct 6, 2025, from https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf
[25] Jamie Levy, Lindsey O'Donnell-Welch, Michael Tigges. *An Attacker's Blunder Gave Us a Look Into Their Operations*. Huntress, September 9, 2025. https://www.huntress.com/blog/rare-look-inside-attacker-operation
[26] It is important to note that Huntress was largely operating on the basis of their software license terms and conditions. However, such a quick process could be made externally to software license regimes if the private sector was given adequate legal cover.
[27] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry and current government participants, October 3, 2025.
[28] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry participant, October 3, 2025.
[29] Google Threat Analysis Group. *Iranian backed group steps up phishing campaigns against Israel, U.S.* Google, August 14, 2024. https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us/
[30] Microsoft Threat Intelligence. *Disrupting active exploitation of on-premises SharePoint vulnerabilities.* Microsoft Security Blog, July 22, 2025. https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

[31] Congressional Research Services. August 3, 2022. *Overview of Governmental Action Under the Stored Communications Act (SCA)*. CRS Report Number LSB10801. https://www.congress.gov/crs-product/LSB10801

[32] DOJ Office of Public Affairs. *"LockerGoga," "MegaCortex," and "Nefilim" Ransomware Administrator Charged with Ransomware Attacks.* United States Department of Justice, September 9, 2025. https://www.justice.gov/opa/pr/lockergoga-megacortex-and-nefilim-ransomware-administrator-charged-ransomware-attacks

[33] *"United States v. Approximately 225,364,961 USDT",* Civil Action No. 25-cv-1907. United States District Court for the District of Columbia. June 18, 2025. https://www.justice.gov/usao-dc/media/1403996/dl?inline

[34] Steven Masada. *Disrupting Lumma Stealer: Microsoft leads global action against favored cybercrime tool.* Microsoft On the Issues, May 21, 2025. https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

[35] *Microsoft Corporation v. DOES 1-10.* Case No. 1:25-CV-2695-MHC. United States District Court for the Northern District of Georgia, May 15, 2025. https://www.noticeofpleadings.net/lumma/files/06_CourtOrders/01_TRO%20Order%20and%20Order%20to%20Show%20Cause.pdf

[36] *Microsoft Corporation v. Does 1-10*. Case No. 1:2025cv02695. U.S. District Court for the Northern District of Georgia, May 13, 2025. https://dockets.justia.com/docket/georgia/gandce/1:2025cv02695/343822

[37] Will Strafach. *Tycoon 2FA Infrastructure Expansion: A DNS Perspective*. DNSFilter, July 8, 2025. https://www.dnsfilter.com/blog/tycoon-2fa-infrastructure-expansion

[38] Sezaneh Seymour, Brandon Wales. *Partners or Provocateurs? Private-Sector Involvement in Offensive Cyber Operations.* Lawfare, July 16, 2025. https://www.lawfaremedia.org/article/partners-or-provocateurs--private-sector-involvement-in-offensive-cyber-operations

[39] *Biggest social media platforms by users 2025*. Statista, March 25, 2025. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[40] Felix Richter. *Infographic: The Big Three Stay Ahead in Ever-Growing Cloud Market*. Statista Daily Data, August 21, 2025. https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers

[41]*Senator Ron Wyden.* Letter to Christopher A. Wray, Director of the FBI. Senator Ron Wyden's Office, Dec 20, 2022. https://www.wyden.senate.gov/imo/media/doc/FBI%20Hacking%20Letter%20Signed%2012.20.22.pdf

[42]David DiMolfetta, *DOD gets millions for cyber capabilities under GOP reconciliation package.* Nextgov/FCW, July 7, 2025. https://www.nextgov.com/cybersecurity/2025/07/dod-gets-millions-cyber-capabilities-under-gop-reconciliation-package/406540/

[43] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace.* Atlantic Council, June 25, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/

[44] Executive Order 14093: *Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security*. 88 FR 18957. Federal Register, March 30, 2023. https://www.federalregister.gov/documents/2023/03/30/2023-06730/prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to

[45] Department of Defense Fiscal Year (FY) 2026 Budget Estimates. U.S. Cyber Command. Retrieved Oct 6, 2025, from https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[46] Department of Defense Fiscal Year (FY) 2026 Budget Estimates. U.S. Cyber Command. Retrieved Oct 6, 2025, from

https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[47] Department of Defense Fiscal Year (FY) 2026 Budget Estimates. U.S. Cyber Command. Retrieved Oct 6, 2025, from https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[48] APPLICATION AND AFFIDAVIT FOR A SEIZURE WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS. Case Number 2:23-MJ-4251. United States District Court, Central District of California, Aug. 23, 2023. https://www.justice.gov/usao-cdca/file/1312086/dl?inline

[49] THE ATTORNEY GENERAL'S GUIDELINES REGARDING THE USE OF FBI CONFIDENTIAL HUMAN SOURCES. Department of Justice. Retrieved October 6, 2025, from https://www.justice.gov/oip/foia-library/foia-processed/general_topics/ag_guidelines_FBI_human_confidential_sources_2/dl, verified by Dartmouth ISTS Roudtable by industry participant, October 3, 2025.

[50] Dartmouth ISTS Offensive Cyber Roundtable, remark by participant, October 3, 2025.

[51] Amnesty International Security Lab. *Cellebrite zero-day exploit used to target phone of Serbian student activist*. Amnesty International. February 28, 2025. *Amnesty International Security Lab*. https://securitylab.amnesty.org/latest/2025/02/cellebrite-zero-day-exploit-used-to-target-phone-of-serbian-student-activist/

[52] Remarks by Leonard Bailey, Panel on Offensive Cyber during Center for Cybersecurity Policy and Law (Director). October 8, 2025. CyberNext DC 2025 [Video recording]. https://www.youtube.com/watch?v=VxtE68RcqXs

[53] *United States of America, Plaintiff-appellant, v. William Adderson Jarrett, Defendant-appellee, 338 F.3d 339 (4th Cir. 2003)*. Justia Law. Retrieved October 6, 2025, from https://law.justia.com/cases/federal/appellate-courts/F3/338/339/549971/

[54] *United States of America, Plaintiff-appellant, v. William Adderson Jarrett, Defendant-appellee, 338 F.3d 339 (4th Cir. 2003)*. Justia Law. Retrieved October 6, 2025, from https://law.justia.com/cases/federal/appellate-courts/F3/338/339/549971/

[55] Dartmouth ISTS Offensive Cyber Roundtable, remarks from multiple former and current government participants, October 3, 2025.

[56] Colin Demarest. *RTX cyber and intel business becomes Nightwing following sale*. C4ISRNET via Yahoo News, April 1, 2024. https://www.yahoo.com/news/rtx-cyber-intel-business-becomes-190451924.html

[57] *Nightwing Group 2025 Company Profile: Valuation, Funding & Investors.* PitchBook. Retrieved October 6, 2025, from https://pitchbook.com/profiles/company/539011-72

[58] *Solutions – Nightwing*. Nightwing. Retrieved October 6, 2025, from https://www.nightwing.com/solutions/index.html

[59] Department of Defense Fiscal Year (FY) 2026 Budget Estimates. U.S. Cyber Command. Retrieved Oct 6, 2025, from https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf

[60] Saber + cyb0rg. *APT Down—The North Korea Files*. Phrack. Retrieved October 9, 2025, from https://phrack.org/issues/72/7.html

[61] Clement Njoki. *Ethical Scambaiting: Understanding Strategies, Challenges, and Global Solutions*. GASA, May 21, 2024. https://www.gasa.org/post/ethical-scambaiting-understanding-strategies-challenges-and-global-solutions

[62] Andy Greenberg. *North Korea Hacked Him. So He Took Down Its Internet.* WIRED, February 2, 2022. https://www.wired.com/story/north-korea-hacker-internet-outage/

[63] Remarks from Meredith Burkardt, Panel on Offensive Cyber during Center for Cybersecurity Policy and Law (Director). October 8, 2025. CyberNext DC 2025 [Video recording].

[64] Evan Wexler, Elias Mallette. *How the NSA's Secret Elite Hacking Unit Works*. FRONTLINE, May 29, 2014. https://www.pbs.org/wgbh/frontline/article/how-the-nsas-secret-elite-hacking-unit-works/
[65] Sam Biddle. *U.S. Spy Agencies Are Getting a One-Stop Shop to Buy Your Most Sensitive Personal Data*. The Intercept, May 22, 2025. https://theintercept.com/2025/05/22/intel-agencies-buying-data-portal-privacy/
[66] Nicole Perlroth. *The Untold History of America's Zero-Day Market.* WIRED, Feb 14, 2021. https://www.wired.com/story/untold-history-americas-zero-day-market/
[67] Matan Mimran. *The Long-Term Threats Posed by the Vault 7 Leaks*. Retrieved October 8, 2025, from https://www.cybereason.com/blog/vault-7-leaks-long-term-threats
[68] *Head of NSA's Elite Hacking Unit: How We Hack*. ABC News, January 28, 2016. https://abcnews.go.com/International/head-nsas-elite-hacking-unit-hack/story?id=36573676
[69] Dartmouth ISTS Offensive Cyber Roundtable, remarks from multiple former and current government participants, October 3, 2025.
[70] Ellen Nakashima. *'No Such Agency' spies on the communications of the world*. The Washington Post, June 7, 2013. https://web.archive.org/web/20130607162318/https://www.washingtonpost.com/world/national-security/no-such-agency-spies-on-the-communications-of-the-world/2013/06/06/5bcd46a6-ceb9-11e2-8845-d970ccb04497_story.html
[71] *Cybersecurity Collaboration Center*. Retrieved October 9, 2025, from https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/. *About NSA Mission*. National Security Agency. Retrieved October 9, 2025, from https://www.nsa.gov/about/
[72] Kim Zetter. *Countdown to Zero Day.* Pentagon Library. Retrieved October 7, 2025, from https://pentagonlib.overdrive.com/media/1397159
[73] Dartmouth ISTS Offensive Cyber Roundtable, remarks from multiple former and current government participants, October 3, 2025.
[74] Dartmouth ISTS Offensive Cyber Roundtable, remarks from multiple former and current government participants, October 3, 2025.
[75] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace.* Atlantic Council, June 25, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/
[76] CYBER 101—U.S. Cyber Command Mission. U.S. Cyber Command. Retrieved March 16, 2025, from https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-command-mission/https%3A%2F%2Fwww.cybercom.mil%2FMedia%2FNews%2FArticle%2F3192016%2Fcyber-101-us-cyber-command-mission%2F
[77] Mark Pomerleau. *Cyber Command supports strikes on Iran's nuclear facilities, but officials keep details under wraps*. DefenseScoop, June 23, 2025. https://defensescoop.com/2025/06/23/cyber-command-supports-attack-iran-nuclear-facilities-midnight-hammer/
[78] Dina Temple-Raston. *How The U.S. Hacked ISIS.* NPR, September 26, 2019. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis. Alisa Chang, *Newly Released Government Documents Detail U.S. Cyberoffensive On ISIS*. NPR. January 23, 2020. https://www.npr.org/2020/01/23/799004239/newly-released-government-documents-detail-u-s-cyberoffensive-on-isis
[79] Department of Defense Fiscal Year (FY) 2026 Budget Estimates. U.S. Cyber Command. Retrieved Oct 6, 2025, from https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/03_RDT_and_E/RDTE_CYBERCOM_PB_2026.pdf
[80] Dartmouth ISTS Offensive Cyber Roundtable, remark from current military participant, October 3, 2025.
[81] Robert Chesney, *Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries.* Lawfare, April 12, 2018. https://www.lawfaremedia.org/article/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries.

[82] Remarks by Mieke Eoyang, Panel on Offensive Cyber during Center for Cybersecurity Policy and Law (Director). October 8, 2025. CyberNext DC 2025 [Video recording]. https://www.youtube.com/watch?v=VxtE68RcqXs

[83] United States Government Accountability Office (2022, March). *DEFENSE ACQUISITIONS: Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities.* https://www.gao.gov/assets/gao-22-104695.pdf; United States Government Accountability Office (2020, Nov 19). *Defense Acquisitions: Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance | U.S. GAO*. Retrieved March 16, 2025, from https://www.gao.gov/products/gao-21-68 ; Carley Welch. *Cyber Command wants to unify Army and Air Force software factories under JCWA, plans for new PEO*. Breaking Defense, June 6, 2024. https://breakingdefense.com/2024/06/cyber-command-wants-to-unify-army-and-air-force-software-factories-under-jcwa-plans-for-new-peo/. Corroborated by Dartmouth ISTS Offensive Cyber Roundtable, remark from former government and current industry participant, October 3, 2025.

[84] Dartmouth ISTS Offensive Cyber Roundtable, remark from former government participant, October 3, 2025.

[85] Suzanne Smalley. *Cyber Command's rotation "problem" exacerbates talent shortage amid growing digital threat.* CyberScoop, August 18 2022. https://cyberscoop.com/military-rotation-norms-challenge-cyber-command/

[86]Erica Lonergan, et al. Building the Future U.S. Cyber Force. FDD, September 9, 2025. https://www.fdd.org/analysis/2025/09/09/building-the-future-us-cyber-force/

[87] *FBI Equity Discussion, Use of Zero-Days & Policy, Vulnerability Equity Policy and Process.* FBI, April 24, 2014. https://www.aclu.org/sites/default/files/field_document/zero_days_policy_foia_-_fbi_response.pdf

[88] Sidney Fussell. *The Spyware That Brought Down El Chapo's Drug Empire.* The Atlantic, January 15, 2019. https://www.theatlantic.com/technology/archive/2019/01/fbi-used-el-chapos-own-spies-against-him/580324/

[89] *Magnet Forensics Part 01 (Final)*. (n.d.). [File]. FBI. Retrieved October 15, 2025, from https://vault.fbi.gov/magnet-forensics/magnet-forensics-part-01-final

[90] Gaby Del Valle. *The FBI got into the Trump rally shooter's phone in just 40 minutes*. The Verge, July 19, 2024. https://www.theverge.com/2024/7/19/24201935/fbi-trump-rally-shooter-phone-thomas-matthew-crooks-cellebrite

[91] DOJ Office of Public Affairs. *United Kingdom National Charged in Connection with Multiple Cyber Attacks, Including on Critical Infrastructure.* United States Department of Justice, September 18, 2025. https://www.justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical

[92] DOJ Office of Public Affairs. *Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government.* United States Department of Justice, September 5, 2024. https://www.justice.gov/archives/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government

[93]*In the Matter of the Seizure of All Funds from One Cryptocurrency Account pursuant to 18 U.S.C. 981, 982, and 28 U.S.C. 2461(c), Application for a Warrant to Seize Property Subject to Forfeiture.* Case No. 24-sz-27, United States District Court for the District of Columbia Court, June 21, 2024. https://www.justice.gov/usao-dc/media/1410771/dl?inline

[94] *UNITED STATES OF AMERICA v. APPROXIMATELY 127,271 BITCOIN ("BTC") PREVIOUSLY STORED AT THE VIRTUAL CURRENCY ADDRESSES LISTED IN ATTACHMENT A, AND ALL PROCEEDS TRACEABLE THERETO.* United States District Court Eastern District of New York. Case 1:25-cv-05745. October 14, 2025. https://www.justice.gov/usao-edny/media/1416266/dl

[95] Matt Burgess, Andy Greenberg. *Feds Seize Record-Breaking $15 Billion in Bitcoin From Alleged Scam Empire.* Wired, October 14, 2025. *https://www.wired.com/story/feds-seize-record-breaking-15-billion-in-bitcoin-from-alleged-scam-empire/*

[96] *Press Release: U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia*. U.S. Department of the Treasury, 2025, October 14. https://home.treasury.gov/news/press-releases/sb0278.
FBI Internet Crime Report, 2024. FBI Internet Crime Complaint Center (IC3). Retrieved October 7, 2025 from https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf .
[97] U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia. (2025, October 14). U.S. Department of the Treasury. https://home.treasury.gov/news/press-releases/sb0278.
[98] *UNITED STATES OF AMERICA v. APPROXIMATELY 127,271 BITCOIN ("BTC") PREVIOUSLY STORED AT THE VIRTUAL CURRENCY ADDRESSES LISTED IN ATTACHMENT A, AND ALL PROCEEDS TRACEABLE THERETO.* United States District Court Eastern District of New York. Case 1:25-cv-05745. October 14, 2025. https://www.justice.gov/usao-edny/media/1416266/dl
[99] *9.7.10 International Seizures and Forfeitures.* Internal Revenue Service. Retrieved October 7, 2025, from https://www.irs.gov/irm/part9/irm_09-007-010
[100] *FREQUENTLY ASKED QUESTIONS REGARDING LEGAL ASSISTANCE IN CRIMINAL MATTERS.* United States Department of Justice Office of International Affairs (Apr. 2022). https://www.justice.gov/criminal/criminal-oia/file/1498811/dl?inline=
[101] Richard Salgado. *First Insights Into the U.S.-U.K. CLOUD Act Agreement.* Lawfare, March 10, 2025. https://www.lawfaremedia.org/article/first-insights-into-the-u.s.-u.k.-cloud-act-agreement
[102] *Operation Endgame*. Retrieved October 9, 2025, from https://operation-endgame.com/
[103] Sidney Fussell. *The Spyware That Brought Down El Chapo's Drug Empire.* The Atlantic, January 15, 2019. https://www.theatlantic.com/technology/archive/2019/01/fbi-used-el-chapos-own-spies-against-him/580324/
[104] Moreover, not all partners are as friendly: when 12 Russian intelligence officers were indicted for hacking the Democratic National Committee in 2016, Vladimir Putin indicated that the DOJ should request assistance via the MLAT between Russia and the U.S., signed in 1999. Congressional Research Service. *Mutual Legal Assistance Treaty with the Russian Federation: A Sketch*. Product Number LSB10176, Jul. 24, 2018. https://www.congress.gov/crs-product/LSB10176
[105] James Landreth, P.E..*Through DoD's Valley of Death—A Data-Intensive Startup's Journey.* Defense Acquisition Magazine, Jan-Feb 2022. Retrieved October 15, 2025, from https://www.dau.edu/library/damag/january-february2022/valley-death
[106] Jen Roberts. *Mythical Beasts: Diving into the depths of the global spyware market.* Atlantic Council, September 10, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/
[107] Chris Metinko *Defense Tech Venture Funding Gains Traction.* Crunchbase News, February 12, 2025. https://news.crunchbase.com/venture/defense-tech-funding-growth-yir-2024/
[108] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current venture capital and industry participants, October 3, 2025.
[109] *IQT | Portfolio*. In-Q-Tel. Retrieved October 7, 2025, from https://www.iqt.org/portfolio?category=Cyber
[110] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current venture capital and industry participants, October 3, 2025.
[111] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace.* Atlantic Council, June 25, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/
[112] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current venture capital and industry participants, October 3, 2025.
[113] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current venture capital and industry participants, October 3, 2025.
[114] Thomas Brewster. *Peter Thiel-Backed Cyber Warfare Contractor Boldend Gets Acquired*. Forbes, August 6,2024. https://www.forbes.com/sites/thomasbrewster/2024/08/06/boldend-a-peter-thiel-backed-hacking-startup-acquired-by-sixgen/

[115] *Leidos acquires Kudu Dynamics, advancing AI capabilities for cyber warfighters.* Leidos. Retrieved October 7, 2025, from https://www.leidos.com/insights/leidos-acquires-kudu-dynamics-advancing-ai-capabilities-cyber-warfighters
[116] Lorenzo Franceschi-Bicchierai. *Spyware maker NSO Group confirms acquisition by US investors*. TechCrunch, October 10, 2025. https://techcrunch.com/2025/10/10/spyware-maker-nso-group-confirms-acquisition-by-us-investors/
[117] Andy Greenberg. *Inside Endgame: A Second Act For The Blackwater Of Hacking*. Forbes, February 12, 2024. https://www.forbes.com/sites/andygreenberg/2014/02/12/inside-endgame-a-new-direction-for-the-blackwater-of-hacking/
[118] *CNAS CEO Nathaniel Fick to Lead Cyber Security Software Company Endgame Inc.* CNAS, November 7, 2012. https://www.cnas.org/press/press-release/cnas-ceo-nathaniel-fick-to-lead-cyber-security-software-company-endgame-inc
[119] *Elastic Completes the Acquisition of Endgame, a Leader in Endpoint Protection*. Elastic, October 8, 2019. https://www.elastic.co/en-us/about/press/elastic-completes-the-acquisition-of-endgame-a-leader-in-endpoint-protection
[120] *Elastic Completes the Acquisition of Endgame, a Leader in Endpoint Protection*. Elastic, October 8, 2019. https://www.elastic.co/en-us/about/press/elastic-completes-the-acquisition-of-endgame-a-leader-in-endpoint-protection. *Leidos acquires Kudu Dynamics, advancing AI capabilities for cyber warfighters.* Leidos. Retrieved October 7, 2025, from https://www.leidos.com/insights/leidos-acquires-kudu-dynamics-advancing-ai-capabilities-cyber-warfighters.
[121] Dartmouth ISTS Offensive Cyber Roundtable, remark from current industry participant, October 3, 2025.
[122] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry and venture capital participants, October 3, 2025.
[123] Pat Host, *How Anduril Is Driving National Security Innovation*. GovCon Wire, October 1, 2025. https://www.govconwire.com/articles/anduril-uav-uuv-lattice-homeland-security
[124] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry and current government participants, October 3, 2025.
[125] *westonbrown/Cyber-AutoAgent: AI agent for autonomous cyber operations*. GitHub. Retrieved October 9, 2025, from https://github.com/westonbrown/Cyber-AutoAgent
[126] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry and venture capital participants, October 3, 2025.
[127] *Justice Manual | 9-48.000—Computer Fraud and Abuse Act.* United States Department of Justice, February 19, 2025. https://www.justice.gov/jm/jm-9-48000-computer-fraud
[128] *18 U.S. Code § 1030—Fraud and related activity in connection with computers*. LII / Legal Information Institute. Retrieved October 6, 2025, from https://www.law.cornell.edu/uscode/text/18/1030
[129] Dartmouth ISTS Offensive Cyber Roundtable, remark from current industry participant, October 3, 2025.
[130] *Justice Manual | 9-48.000—Computer Fraud and Abuse Act.* United States Department of Justice, February 19, 2025. https://www.justice.gov/jm/jm-9-48000-computer-fraud
[131] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry participants, October 3, 2025.
[132]Erica D. Borghard, Shawn W. Lonergan. *What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?.* Council on Foreign Relations. September 10, 2018. https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations
[133] Stacy H. O'Mara. *To Hack Back, or Not Hack Back? That is the Question … or is it?*. Center for Cybersecurity Policy and Law, May 28, 2025. https://www.centerforcybersecuritypolicy.org/insights-and-research/to-hack-back-or-not-hack-back-that-is-the-question-or-is-it

[134] Clement Lecigne, Maddie Stone. *Active North Korean campaign targeting security researchers*. Google, September 7, 2023. https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/
[135] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry participants, October 3, 2025.
[136] DOJ Office of Public Affairs. *New York Resident Pleads Guilty to Operating Secret Police Station of the Chinese Government in Lower Manhattan.* United States Department of Justice, December 18, 2024. https://www.justice.gov/archives/opa/pr/new-york-resident-pleads-guilty-operating-secret-police-station-chinese-government-lower
[137]Stephen Smith. *Notorious cartel hired hacker to use surveillance cameras, phone data to track and kill FBI informants, U.S. says*. CBS News, June 30, 2025. https://www.cbsnews.com/news/sinaloa-cartel-hacker-phone-data-cameras-track-kill-fbi-informants-doj. Corroborated by Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry participants, October 3, 2025.
[138] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry participants, October 3, 2025.
[139] Asaf Lubin. Unpacking WhatsApp's Legal Triumph Over NSO Group. Lawfare, January 7, 2025. https://www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group
[140] *Research Threats: Legal Threats Against Security Researchers*. Security Research Threats. Retrieved October 8, 2025, from http://threats.disclose.io/
[141]Dartmouth ISTS Offensive Cyber Roundtable, remark from current industry participant, October 3, 2025.
[142]Dartmouth ISTS Offensive Cyber Roundtable, remark from current industry participant, October 3, 2025.
[143] Dartmouth roundtable participants in government attested that prime contractors may lack or have trouble retaining highly skilled individuals, so these two avenues do not have identical results. Dartmouth ISTS Offensive Cyber Roundtable, remarks from current government participants, October 3, 2025.
[144] Dartmouth ISTS Offensive Cyber Roundtable, remark from venture capital participant, October 3, 2025.
[145] Dartmouth ISTS Offensive Cyber Roundtable, remarks from venture capital participants, October 3, 2025.
[146]T. Dullien. *Weird Machines, Exploitability, and Provable Unexploitability.* IEEE Transactions on Emerging Topics in Computing, vol. 8, no. 2, pp. 391-403, 1 April-June 2020, doi: 10.1109/TETC.2017.2785299. http://www.dullien.net/thomas/weird-machines-exploitability.pdf .
[147] Sergey Bratus. *Technical Perspective: How Exploits Impact Computer Science Theory.* Communications of the ACM, November 22, 2024. https://cacm.acm.org/research-highlights/technical-perspective-how-exploits-impact-computer-science-theory/
[148] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace.* Atlantic Council, June 25, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/. Corroborated by Dartmouth ISTS Offensive Cyber Roundtable, remark from current academic participant, October 3, 2025.
[149] Perri Adams, Dave Aitel, George Perkovich, J.D. Work. *Responsible Cyber Offense*. Lawfare, August 2, 2021. https://www.lawfaremedia.org/article/responsible-cyber-offense
[150] Perri Adams, Dave Aitel, George Perkovich, J.D. Work. *Responsible Cyber Offense*. Lawfare, August 2, 2021. https://www.lawfaremedia.org/article/responsible-cyber-offense
[151] *Responsible Cyber Power in Practice*. GOV.UK. Retrieved October 8, 2025, from https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html. Corroborated by Dartmouth ISTS Offensive Cyber Roundtable, remark from current UK government participant, October 3, 2025.
[152] *REDSPICE.* Australian Signals Directorate. Retrieved October 15, 2025, from https://www.asd.gov.au/about/what-we-do/redspice

[153] *Responsible Cyber Power in Practice*. GOV.UK. Retrieved October 8, 2025, from https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html
[154] Winnona DeSombre Bernsen. *Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace.* Atlantic Council, June 25, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/
[155] Matan Mimran. *The Long-Term Threats Posed by the Vault 7 Leaks*. Retrieved October 8, 2025, from https://www.cybereason.com/blog/vault-7-leaks-long-term-threats
[156] Dartmouth ISTS Offensive Cyber Roundtable, remark from current industry participant, October 3, 2025.
[157] *Anduril Deploys 300th Autonomous Surveillance Tower (AST), Advancing Capability for Border Security*. Anduril, September 26, 2024. https://www.anduril.com/anduril-deploys-300th-autonomous-surveillance-tower-ast-advancing-capability-for-border-security/
[158] *How the Government Can Use the SBIR Program to Scale Innovation.* Anduril, Jul. 15, 2021. https://www.anduril.com/how-the-government-can-use-the-sbir-program-to-scale-innovation/
[159] *Programs for Innovation*. NSA. Retrieved October 13, 2025, from https://www.nsa.gov/business/programs/programs-for-innovation/
[160] Note: as of this writing during the government shut down on October 13, 2025, all SBIR program authorization has expired. Congress must ensure that, in passing the budget, SBIR program authorization is renewed.
[161] *Topics and Topic Search (SITIS)*. DOD SBIR Program. Retrieved October 13, 2025, from https://www.dodsbirsttr.mil/topics-app/
[162] Hossein Siadati, Haadi Jafarian, Sima Jafarikhah. *Send to which account? Evaluation of an LLM-based Scambaiting System* (No. arXiv:2509.08493). arXiv. September 10, 2025. https://doi.org/10.48550/arXiv.2509.08493
[163] Sezaneh Seymour, Brandon Wales. *Partners or Provocateurs? Private-Sector Involvement in Offensive Cyber Operations.* Lawfare, July 16, 2025. https://www.lawfaremedia.org/article/partners-or-provocateurs--private-sector-involvement-in-offensive-cyber-operations
[164] Cyber Lunarium Commission. *CLC #002: Cyber Letters of Marque for Counter-ISIL Cyber Operations*. Cyber Lunarium Commission, June 9, 2020. https://www.cyberlunarium.org/2020/06/clc-002-cyber-letters-of-marque-for.html
[165] Dartmouth ISTS Offensive Cyber Roundtable, remark from current government participant, October 3, 2025.
[166] Dartmouth ISTS Offensive Cyber Roundtable, remark from former government participant, October 3, 2025.
[167] Dartmouth ISTS Offensive Cyber Roundtable, remark from former government participant, October 3, 2025.
[168] *In the Matter of the Seizure of All Funds from One Cryptocurrency Account pursuant to 18 U.S.C. 981, 982, and 28 U.S.C. 2461(c), Application for a Warrant to Seize Property Subject to Forfeiture.* Case No. 24-sz-27, United States District Court for the District of Columbia Court, June 21, 2024. https://www.justice.gov/usao-dc/media/1410771/dl?inline
[169] AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEIZURE WARRANT. Case 3:21-mj-70945-LB. U.S. District Court Northern District of California – San Francisco, June 7, 2021. https://www.justice.gov/archives/opa/press-release/file/1402056/dl
[170] 18 U.S. Code § 981—Civil forfeiture. LII / Legal Information Institute. Retrieved October 16, 2025, from https://www.law.cornell.edu/uscode/text/18/981
[171] *Foreigners, Foreign Property, and the Fourth Amendment: United States v. Verdugo-Urquidez, 110 S. Ct. 1056 (1990)* | Office of Justice Programs. Retrieved October 13, 2025, from https://www.ojp.gov/ncjrs/virtual-library/abstracts/foreigners-foreign-property-and-fourth-amendment-united-states-v

[172] Clement Njoki. *Ethical Scambaiting: Understanding Strategies, Challenges, and Global Solutions*. GASA, May 21, 2024. https://www.gasa.org/post/ethical-scambaiting-understanding-strategies-challenges-and-global-solutions
[173] CBC News. *Infiltrating scammer networks with the world's top fraud fighters | Marketplace* [Video recording]. March 21, 2025. https://www.youtube.com/watch?v=MSa7i92o6ho,
[174] Dartmouth ISTS Offensive Cyber Roundtable, remarks from current industry participants, October 3, 2025.
[175] *FBI Internet Crime Report, 2024.* FBI Internet Crime Complaint Center (IC3). Retrieved October 7, 2025 from https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
[176] *Fact Sheet: President Donald J. Trump Signs GENIUS Act into Law*. The White House, July 18, 2025. https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-president-donald-j-trump-signs-genius-act-into-law/
[177] *FBI Internet Crime Report, 2024.* FBI Internet Crime Complaint Center (IC3). Retrieved October 7, 2025 from https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf .
[178] *SAM.gov*. IRS proposal for "'Development of Exploitation Techniques Against Cryptowallets". Retrieved October 15, 2025, from https://sam.gov/opp/2b4b9384655e4237862484106c16e581/view
[179] Matt Burgess, Andy Greenberg. *Feds Seize Record-Breaking $15 Billion in Bitcoin From Alleged Scam Empire.* Wired, October 14, 2025. *https://www.wired.com/story/feds-seize-record-breaking-15-billion-in-bitcoin-from-alleged-scam-empire/*
[180] Chainalysis Team. *The Landscape of Seizable Crypto Assets in 2025.* Chainalysis, October 9, 2025. https://www.chainalysis.com/blog/landscape-of-seizable-crypto-assets-2025/
[181] *FAQ — LazarusBounty*. Bybit. Retrieved October 13, 2025, from https://www.bybit.com/en/help-center/article/www.bybit.com/en/help-center/article/FAQ-LazarusBounty
[182] Vicky Ge Huang. *Crypto Stockpiling Craze Cools After Red-Hot Summer.* Wall Street Journal, October 1, 2025. https://www.wsj.com/finance/currencies/crypto-stockpiling-craze-cools-after-red-hot-summer-d1b6dce2
[183]Chainalysis Team. *Asset Seizure and Cryptocurrency: How Chainalysis Creates Opportunities for Self-Sustaining Law Enforcement.* Chainalysis Blog, March 26, 2025. Retrieved October 13, 2025, from https://www.chainalysis.com/blog/cryptocurrency-asset-seizure/

The Institute for Security Technology Studies (ISTS) was founded at Dartmouth College in 2000 as a national center of security research and development. The Institute conducts interdisciplinary research and development projects addressing the challenges of cyber and homeland security, to protect the integrity of the Internet, computer networks, and other interdependent information infrastructures. ISTS also develops technology for providing the information and tools necessary to assist communities and first responders with the evolving, complex security landscape.