Testimony Of

Drew Bagley
CrowdStrike

Before

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland"

January 13th, 2026

Chairman Ogles, Ranking Member Swalwell, members of the subcommittee, thank you for the opportunity to testify today. Throughout my career, I have seen firsthand the challenges and opportunities of improving American cybersecurity from my work in the private sector, government, and academia. For more than a decade at CrowdStrike, a leading cybersecurity company, I have had a front row seat to cybersecurity innovation while building our privacy and public policy programs and advising customers around the globe. Prior to that I worked at the intersection of law and technology in the FBI's Office of the General Counsel. I previously taught at universities in the US and Europe, and currently serve as an adjunct professor in American University's cybersecurity policy program.

As a leading U.S. cybersecurity company, CrowdStrike has a useful and often quite textured vantage point on malicious activities in cyberspace. Protecting organizations with our cybersecurity technology, threat intelligence, professional services offerings and incident response work, we confront a full range of cyber threats. We defend many components of the U.S. Federal government and serve as a commercial cybersecurity provider for major technology companies, 8 of the top 10 financial services firms, and 43 of 50 U.S. states[1]; as well as all manner of critical infrastructure entities and small and medium sized businesses. We defend America.

Nation states are relentless. In parallel, there is a democratization of destruction whereby those perpetrating cyber attacks no longer need the knowledge, resources, or time once required to execute high impact attacks–indeed, adversaries can "vibehack" their way to success. Moreover, because legitimate credentials may be purchased in online criminal forums, along with the tools to deploy ransomware and malware, the means to attack are available for those who merely have the intent. As adversaries evolve, defenders are most successful when they adapt. This holds true for our digital ecosystem in general. As we adopt new technologies, features and abilities, we must

[1] State and Local Governments, CrowdStrike. https://www.crowdstrike.com/en-us/solutions/state-local-government/

adapt how we secure them. Today, this means we must think about how we detect, prevent, and defend an attack surface that now includes AI.

To what extent is America secure from cyberthreats?
America remains vulnerable to cyberattacks, and the scope and severity of which continues to increase.[2] To be clear, some organizations are effectively defending themselves. Bright spots include broader adoption of modern endpoint and managed security solutions in public and private enterprises. Still, organizations face an array of attacks targeting cloud environments, Software as a Service (SaaS) applications, and identities.

Under-resourced public institutions and small and medium sized businesses are particularly vulnerable. But high-profile attacks over the past few years from China, notably the VANGUARD PANDA/Volt Typhoon attacks targeting critical infrastructure and the OPERATOR PANDA/Salt Typhoon attacks targeting telecommunications entities have raised the most acute concerns from a national security perspective. Despite significant investment in cybersecurity measures, the status quo isn’t working.

What’s gone wrong?
Simply put: threat actors are still operating at scale, still operating with limited consequences, and still all-too-often achieving their objectives. They are still seeing a clear return on investment. They are still assessing a risk calculus that shows favorable outcomes. To make durable progress, we must work in a concerted fashion to change each of these conditions. (I describe how below.)

What’s the role for “offense” in confronting cyber threats?
In the cyber context, offense can mean a number of different things. At a high level, from a law enforcement or industry lens, threat actor infrastructure disruptions might include seizing malicious domains, servers, or relay infrastructure; asserting control over hosted malware kits or botnets; or offlining darkweb forums or sites used to anonymously host pilfered information. Importantly, denying an adversary the ability to monetize their efforts is also achievable. At a minimum, these sorts of operations require careful planning, pose coordination challenges, and may raise questions about burden sharing.

Offense from a military or intelligence lens might imply breaching foreign organizations or otherwise attacking them, such as through denial of service or destructive attacks. The latter can focus on deleting data, destroying IT systems, or causing ‘effects’ in the real world, such as by manipulating operational technology (OT) systems and thus associated infrastructure.

At the level of the enterprise, we advocate that defenders threat hunt or work with a partner who can do it on their behalf. This essential practice can be performed on each organizations’ own

[2] America’s technology infrastructure consists of an array of IT, OT, telecommunications, cloud and digital services, cyber-physical systems, and the data and identity layers that connect them all. These systems are managed by organizations large and small, well-resourced and under-resourced.

systems, resources, and data.[3] Therefore, it's mainly a proactive approach–sometimes called active defense–rather than offense per se. But threat hunting is one of the most effective techniques we have as an industry to confront targeted attacks.

Should cyberattack victims or their representatives "hack back"?
When the 'hack back' policy discourse started in earnest about 15 years ago, it was in response to multiple reports of egregious campaigns where adversaries had, for example, breached a series of organizations like National Labs or defense contractors, exfiltrated gigabytes of sensitive data, left that data on a fairly exposed staging server, and collected it later at their convenience. In that type of scenario, particularly where the victim(s) possessed relevant forensic artifacts and telemetry, the inability to legally "do something," often meaning to delete the only copy of the stolen data, caused a great deal of consternation.

Today, attacks are generally far more sophisticated, leveraging compromised accounts of legitimate (e.g., SaaS) applications; transient, ephemeral, or shared cloud environments; and other obfuscation techniques. In this environment, a policy framework that's more conducive to 'hack back' operations carried out by a broad array of actors could yield revictimization, collateral damage, and impacts to innocent victims. Ongoing investigations could be disrupted. Retaliation could lead to waves of escalation, potentially along geopolitically-salient lines. For these reasons, we share the view that offense is best left to professionals with relevant authorities, deconfliction processes, and clear oversight. A democratized regime for hacking back that lacks these attributes probably creates more problems than it solves.

Is defense discredited?
No. Defense is foundational. Even those who wish to increase offense must recognize the value of robust defenses. Even if a city announced an enormous and well-resourced crackdown on crime, homeowners should still, rationally, take the basic steps of shutting and locking their doors at night. New threat actors emerge routinely with different capabilities and motivations. Economic and geopolitical conditions change, often for the worse. Having defenses in place amid this changing terrain is essential. Further, to the extent policy dictates that offensive actions will increase, that should lead to a heightened, rather than reduced, focus on defense.

In the kinetic world, it is not uncommon to categorize 'soft' targets versus 'hard' targets. Simply put, organizations that have hardened themselves with modern approaches are more secure and have drastically reduced the likelihood of suffering a high impact event. Those that haven't remain vulnerable not only to infiltration but to existential impacts in the face of an incident.

It's often said that 'mom-and-pop' operations can't be expected to singlehandedly defeat the People's Liberation Army. That's true. National-level policies and capabilities are needed to create conditions of reduced threats. But, as with other threats, hazards, and risks, all organizations should take reasonable steps to defend themselves.

[3] As a vendor, we facilitate sharing of visibility in threat hunting operations at the sector-level, national-level, and international level through our threat intelligence reporting.

What's the role of deterrence in defeating threats?
Mechanically, deterrence is achieved either through denial (i.e., an adversary realizes an attack won't be effective, so they apply their energies elsewhere) or through a credible threat of retaliation. Retaliation can be intradomain (i.e., also a cyberattack) or crossdomain (e.g., leveraging a law enforcement or conventional military capability).[4]

Cyberattacks are caused by adversaries. Threats themselves aren't deterrable; the people, institutions, and nations behind them often are. The people in question are military or political figures. Or anonymous criminals. They might be rich or poor; empowered or desperate; or seeking fame or seeking to effectuate a radical political or social cause. They might be, in the political science sense, rational or irrational actors. Given that their conditions and motivations vary so widely, there is no singular approach to deterrence that could succeed.

Deterrence is difficult to measure. Clearly, a significant number of adversaries are not presently deterred. As a community, we must strengthen deterrence as part of a holistic approach to cyberdefense.

How should policymakers think about resourcing defense vs. offense?
Unfortunately, a simple 50-50 (or 80-20, or 20-80)-style-answer here is elusive. But several considerations should guide investments:

- With respect to defense, organizations should develop realistic, informed threat models and plan to confront those threats.
- Some amount of investment in security is reasonable. Against today's adversaries, unfortunately, basic hygiene and best practices alone fail. The ability to achieve real-time visibility, detection, and response across federated IT systems is required for protection and threat hunting. For organizations with resource constraints, clear illustrations depicting how investments map to reduced risks are typically most persuasive to planners, be they management, boards, or appropriators.
- Efficacy is often more important than resourcing overall. Unfortunately, in today's public policy debates, there are many false proxies for assessing whether cyber defenses are effective. Simply because the federal government, a particular sector, or an individual organization spends a certain dollar amount on security does not mean it is buying the best technology, deploying it on the most critical assets, or operating it correctly. Similarly, and especially in government, technology with the lowest price tag—or that is included as part of an add-on bundle—is unlikely to deliver the same security outcomes.
- Ultimately, it's probably reasonable to conceive of security investments as a portion of overall IT spending (best practices for which may vary, but are sometimes assessed by reputable technology research advisory firms).

[4] For our part, the core technologies we produce–namely the Falcon platform and associated capabilities–essentially seek to support denial. Our threat intelligence products, among other things, can support threat actor identification, which can strengthen targeting for organizations with enforcement and defense missions.

Similarly, at a national-level, it’s appropriate and realistic for institutions operating under Title 10 and Title 50 authorities to resource offensive missions. But rather than defining resourcing levels for those activities relative to cyber *defense* investments, it’s probably more reasonable for planners to consider cyber offense relative to other *offensive* capabilities (e.g., kinetic options) that might achieve a similar outcome.[5]

What roles, missions, and authorities must change to better confront cyber threats?
Our core prescription is bringing to bear more focused, more persistent, and more tightly-orchestrated campaigns disrupting threat actors and those who support them. This means leveraging more technical operations, erecting more barriers to success, and leveraging all available tools of statecraft (i.e., crossdomain responses) to pressure adversaries, dampen their success, and prevent them from operating at scale.

Consider first financially-motivated attacks, such as ransomware. CISA, probably acting through JCDC, should consult with industry to determine which groups are most problematic (either because of scale, targeting practices, or some other criteria) and establish a “Most Wanted”-style list. CISA should ascertain targeting information about those responsible from stakeholders.[6] They should orchestrate actions with relevant law enforcement partners (or, where appropriate, Intelligence Community partners) to use disruption authorities and, where possible, simultaneous enforcement actions to target those responsible. They should orchestrate actions with partners at Treasury and the private sector financial ecosystems to complicate or prevent cash-outs or monetization of hacking. They should leverage industry partners who can contribute along the way by sharing visibility and better enforcing their own terms of service, given that most firms already contractually prevent criminality and abuse.

Similar coordination must take place focused on nation state actors. In those cases, there might be less focus on disrupting monetization and law enforcement actions,[7] and more on Title 10 and Title 50 actions. Still, particular actions should be prioritized in consultation with relevant stakeholders and executed with great frequency.

[5] Whether other means to attain intelligence or other means to achieve effects.

[6] Our sense is that CISA possesses all relevant authorities to perform these actions. National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1715 (Joint Cyber Planning Office), 134 Stat. 3388 (2021).

[7] Although not in the case of national state actors engaged in cybercrime to fund the regime, such as the DPRK, and/or operating from 3rd party countries where U.S. and allied nations have law enforcement reach.

Everything I've described here does take place–just not nearly enough. It's really a matter of will for decisionmakers to demand that this sort of thing, which happens periodically, takes place routinely,[8] and on the highest impact targets.

How does the advancement of AI impact these considerations?

The advancement of AI does not materially impact threat actor motivations. It does, however, provide threat actors with a new class of systems to target, new infrastructure to leverage, and a new accelerant to automate their own TTPs. We expect this trend to continue as adversaries exploit new tools and adapt to changing conditions.

AI itself is under threat from adversaries, whether its the systems, data, or human and non-human identities or the end user platform. This will only increase as AI becomes more ubiquitous and disappears into the traditional IT stack, becoming a commonplace part of America's digital infrastructure. Much like the need for detection and response for the endpoint, network, cloud and identity, AI Detection and Response (AIDR) detects and prevents direct and indirect prompt injection, jailbreaks, and model manipulation attempts.

At its core, cybersecurity is fundamentally a data problem. Fortunately, AI–and specifically Agentic AI-which takes bounded actions on users' behalf–radically empowers defenders. One of the most immediate areas Agentic AI can improve cybersecurity practices is leveraging agents to eliminate bottlenecks in the Security Operations Center (SOC). By deploying specialized agents to tackle time-intensive tasks, security teams can reclaim a speed advantage, close persistent labor and response gaps, and shift from reactive to proactive defense. Agents can analyze malware, perform certain hunt actions, prioritize exposure remediation, and more.[9]

Recommendations

- **Public and private organizations must take reasonable actions to defend themselves.** Denying cyber threat actors the ability to achieve their objectives is an important ordering principle for investments in cybersecurity capabilities. How to achieve this will continue to evolve over time in line with technological adoption and adversary techniques. Right now, enterprises should view endpoint detection and response (EDR), threat hunting, identity threat detection and response, SaaS security, and cloud security as high-leverage areas of investment to this end.

[8] In July 2017, we called on the cybersecurity community to "*bring more energy to this fight. A serious commitment from law enforcement and the security community to attempt to take down one botnet every week would be a "game changer."... These goals are ambitious relative to the status quo, but not impossible. Ultimately, focusing on such initiatives would provide a powerful organizing principle for decision makers across government and industry, going well beyond botnets and automated threats to catalyze a seismic shift in cybersecurity*." https://www.ntia.gov/files/ntia/publications/crowdstrike-20170713.pdf. Sadly, as a community we've never approached this scale.

[9] Such agents are central to a profound change that's underway now to modernize traditional SOCs for the emerging era of the Agentic SOC. A NextGen SIEM capability will enable organizations to leverage these agents by exposing them to all relevant security data and positioning them to perform workflows like threat hunting and remediation.

- **The cybersecurity community should radically increase the operational tempo of malicious infrastructure disruptions and takedowns** that are carried out by government organizations and aided by private sector support where appropriate (e.g., information sharing and operational collaboration). In some instances, private actors like IT providers or telecommunications companies can leverage legal processes or their own terms of service to disrupt operations themselves.
- **Given its stakeholder engagement functions, CISA should be central to coordinating public and private actors to this end.** This Committee can ensure that CISA[10] is properly focused and resourced to perform this mission. From an oversight perspective, you can ensure it has authorities, talent, and capabilities to maximize its impact.
- **Federal law enforcement, along with Title 10 and Title 50 entities, should work to increase deterrence.** The USG should lead holistic responses to significant adversary actions, leveraging existing authorities in parallel and with speed to deter adversaries and reduce the ROI for their attacks,

Thank you again for the opportunity to testify today, and I look forward to your questions.

###

[10] Organizations operating under Title 10 and Title 50 authorities have a somewhat more complicated resource allocation question,