Cyber Crime and Geostrategic Clash Over the Internet

Deputizing the Private Sector to Assist

Admiral (Ret.) Dennis C. Blair
William "Bud" Roth

Over the past two decades, global society has shifted significant portions of its social and economic activities online. In the US alone, Internet Association experts estimate that Internet-based commerce accounted for about $2.1 trillion, or 10% of GDP, in 2019. With this rise in economic and social activity, the world has witnessed a dramatic rise in cyber-attacks, mostly by criminal actors seeking to steal assets, defraud victims, and ransom decryption keys. One expert projects that by 2025, worldwide cyber-crime losses will reach a staggering $10.5 trillion, making cyber-crime—were it a country—the world's third largest economy.[1] For victims, the harm includes not only the cost of cleanup, but the loss of tangible assets such as stolen funds and fraudulent credit card charges, as well as harder-to-quantify figures for businesses that shut down operations or lose valuable intellectual property that finds its way into competitors' hands.[2] Thus, the consequences for business owners and everyday citizens are severe. Yet progress in stemming the flow of cyber-attacks in the US seems stymied. The White House's 30-nation meeting on ransomware in October 2021 was a promising initiative, but lacked any mention of private-sector active defense measures.[3] As noted in the 2016 "Into the Gray Zone" report co-authored by ADM Dennis Blair, one of this article's authors, the US must take active steps not only to protect networks, but also to hunt down threat actors. Doing this at scale will require robust private sector participation. This article suggests one way to achieve this.

Currently, amid our inaction, private enterprise and government agency alike have suffered an unbroken string of malicious cyber intrusions that will continue unless we, as a nation, better galvanize and integrate the private sector into the nation's defense. The theft

Views and opinions herein are those of the authors.

Admiral (Ret.) Dennis Blair, Knott Distinguished Visiting Professor of the Practice at the University of North Carolina at Chapel Hill, serves on the Energy Security Leadership Council and chairs the board of Security America's Future Energy. From 2014-18 Admiral Blair was the CEO and Chairman of the Board of the Sasakawa Peace Foundation USA. Previously, he served as Director of National Intelligence, President of the Institute for Defense Analyses, and Commander, U.S. Pacific Command. In addition, Admiral Blair served as Co-Chair for the GW Center for Cyber and Homeland Security 2016 report, "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats." A graduate of the U.S. Naval Academy, Admiral Blair earned a master's degree in history and languages from Oxford Uni-versity as a Rhodes scholar, and authored *Military Engagement: Influencing Armed Forces Worldwide to Support Democratic Transitions.*

of defense-related IP and national security secrets by government-sponsored hackers tangibly contributes to the geopolitical strategies and power of our adversaries. Military analysts point to China's leaps in military technology as, in great part, the result of China's rampant theft of US defense secrets and technology. The Pentagon's 2013 annual report to Congress noted that China uses stolen US defense technology to accelerate development of its weapons systems. A follow-up report leaked to the press identified the Aegis Ballistic Missile Defense System, F-35 Joint Strike Fighter, Littoral Combat Ship, and electromagnetic rail guns as systems whose plans were stolen by Chinese hackers.[4] This theft of defense technology is contributing to China's military confidence in pressuring the US and its allies across an array of tension points in Asia and elsewhere.[5] In short, nation-state hacking of US government (USG) and defense contractor networks has concrete and significant national security consequences.

As China and Russia recognize the strategic value of hacking our networks, they have mobilized hacker teams to identify networks with valuable US intellectual property or national security secrets, penetrate them, and steal the valuable IP or secrets.[6] Every year brings new examples of stolen US secrets, either from government agencies or companies. The OPM hack, Equinox breach, SolarWinds supply chain hack, and recent compromise of Microsoft Exchange systems are just a few major breaches that led to huge losses of national security and defense secrets.[7] Some of the compromised networks such as the Department of Homeland Security (DHS) and Department of Defense (DoD) networks, have implemented the strongest security protocols available, making the hackers' ability to operate undetected for months or even years all the more shocking.[8] Perhaps more disturbing, post-incident forensics confirm that US adversaries are still able to navigate networks freely and exfiltrate sensitive data, while avoiding detection.[9]

William "Bud" Roth, graduate of Dartmouth College, clerked at the Delaware Court of Chancery after law school and then began his federal career as an attorney with the Securities and Exchange Commission's Office of Internet Enforcement. He served on the Department of Justice 9/11 Financial Crimes Task Force before leaving the SEC. Mr. Roth spent almost a decade with the Department of Defense supporting counter-terrorism operations, where he received a Defense of Freedom Medal and Meritorious Service Medal from the Department of the Army. Mr. Roth served as the Non-Resident Fellow for Cybersecurity at Sasakawa Peace Foundation before joining his current employer, the Army's 781st MI Battalion. The authors previously coauthored, *A National Security Strategy for 5G (2020)* (presented at RSA 2020), and *WannaCry's Lesson for the US-Japan Alliance*, The Diplomat (May 23, 2017).

As losses mount, the US has struggled to implement an effective deterrent policy.[10] Attempts to focus on protecting national security assets and critical infrastructure have failed, while leaving firms, agencies, and citizens who are not part of this subset of systems with little recourse to protect their networks.[11] While prioritizing critical infrastructure (and national security assets) is a logical next step in allocating limited resources, policymakers and security experts must be mindful that attacks on high-value targets are interwoven into a broader range of attacks supported at some level by adversaries seeking to disrupt the US economy or otherwise degrade public confidence in US and Western institutions. The onslaught of cyber-attacks our nation faces requires a more robust set of deployable defensive responses that effectively counter all attacks, whether state-sponsored or not, and for all networks, whether deemed critical infrastructure by the government or not. This requires more actors capable of responding. In short, increasing the number of assets available to defend against cyber-attacks is required to address the broader threat this nation faces. Activating private-sector defenders is the best way to do this.

This article takes the 2016 "Into the Gray Zone" report's call for a larger private sector role a step further. We urge that private-sector capabilities be folded into a robust nationwide active defense of all US networks against any cyber-attack. This proposition is premised on the belief that criminal hacking is assisting our adversaries in three important ways:

- Providing noise that conceal sophisticated attacks by adversaries.
- Damaging Western assets and public confidence, consistent with our adversaries' strategic goals.
- Exploiting sensitive networks targeted by adversaries and/or sharing the lead with state actors to exploit.

US adversaries are piggybacking on private sector criminals to compromise our networks and further their strategic goals, it only makes sense for the US to actively engage the private sector in countering these assaults on our nation. As a starting point, the next section examines in detail the ways our adversaries benefit from a criminal cyber threat.

A. Noise that conceals sophisticated adversary attacks

Cyber intrusions by Russian and Chinese military and intelligence sometimes track and other times differ from criminal behavior. For example, nation-state actors that steal national security secrets target federal agencies and government contractors or subcontractors because they hold secrets and defense-related intellectual property. Criminal actors seeking profit pursue a wider variety of targets, including hospitals and smaller firms unconnected to government. Yet, China's hacking blurs this distinction. For example, state-owned enterprises may direct government hackers to target IP and trade secrets of competitors in industries wholly unrelated to national defense.[12] Use of government resources for economic espionage is a longstanding sore point for the US, an issue President Obama stressed with President Xi during his 2015 visit.[13] But the problem does not stop there. Russia and China take it a step further by turning a blind eye to, and in many cases, hosting criminal hackers that target only western networks.[14] These adversaries deliberately provide safe havens and foster a cyber-crime ecosystem that targets US and Western networks. The sheer volume of such hacking attacks provides cover for our adversaries' cyber operations. Reacting to the widespread noise of criminal hackers consumes limited federal resources that could otherwise be available to counter the adversaries' best hackers, hackers who today may go undetected.

B. Damaging Western Interests

Russia and China are permitting—in some instances, encouraging—domestic hackers to attack Western targets.[15] Their permissive attitude may have originated from a belief that it was simply not worth the significant effort to stop criminal activity that only harmed Western economies and citizens.[16] For governments whose priority is domestic political stability and information control, curtailing criminals who target victims only in the West was logically a low priority.[17] Over time, perhaps because of complaints from the West, China and Russia became aware of the presence of these criminal hacker elements, and saw not a threat, but an opportunity.

Invented in the US as an open system outside government control, the Internet, from its beginning, has threatened authoritarian governments bent on strict controls over what the populace sees and thinks. Internet users around the world have always known that the Internet offers simple, hard-to-block ways for private citizens to sidestep censors and propagandists, and exchange news and ideas across borders.[18] Authoritarian governments have taken strong measures to control Internet usage: blocking seditious content, identifying disaffected citizens, and censoring content to favor official views and policies. Russia and China's rulers

see the Internet's explosive growth and free flow of information as not only a domestic threat to authoritarian control, but also as a core component of a Western-imposed, post-Cold War world order.[19] Their efforts to counter this Western threat go well beyond blocking portions of the Internet at the border; they include undermining the integrity of the Internet itself. Both countries leverage the open nature of the Internet to sow political discord and distrust in the West. One of their primary goals is to undermine Western confidence in the utility and safety of the Internet. Our adversaries see the Internet not only as a medium to subvert the West, but also as a symbol of the West that must itself be subverted.[20]

The tactical goal of subverting the Internet fits within our adversaries' overall strategic imperatives, and explains our adversaries' tolerance of criminal hacking activity against US and its allies. Criminal hacks such as the Colonial Pipeline hack or the Equifax credit report hack disrupt US society, create distrust of the Internet, and foster doubt about US abilities to defend American interests. This palpable impact has led adversaries to not just tolerate, but actively facilitate criminal hacking activity against US and Western interests.[21]

C. Acting as Hacker Proxies

Analysis of serious hacks against US interests suggests that criminal hackers operating in China and Russia that target Western networks now receive various levels of state support, ranging from passive tolerance, to refusal to honor law enforcement requests for assistance, to active support and funding.[22] The sophisticated hacker group, Wicked Panda, began attracting US security firms' attention for their profitable targeting of gaming entities in 2013.[23] Beginning in 2015, Wicked Panda started targeting a broader array of industrial targets in the US, Japan, Germany and elsewhere, targeting that was more aligned with economic espionage goals of China's state-owned enterprises.[24] As the group's targets changed, they began using more sophisticated attacks. In 2016, analysts blamed Wicked Panda for a set of supply-chain attacks focused more on targets aligned with Chinese government strategic goals than on profits.[25] The Department of Justice (DOJ) unsealed indictments against five members of Wicked Panda in 2020, charging it with compromising networks of 100 firms, universities and agencies, stealing for profit, and illegally benefiting the Chinese government.[26] As then Deputy Attorney General Jeffrey A. Rosen put it, "The Chinese government has made a deliberate choice to allow its citizens to commit computer intrusions and attacks around the world because these actors will also help the P.R.C."[27]

Russia similarly has demonstrated tolerance of—if not collusion with—criminal hacking from its territories.[28] Indeed, the FBI seeks the arrests of Russia-based Maksim Yakubets and Igor Turashev for bank wire fraud and theft of over $100 million from US banks and non-profits in 21 municipalities.[29] Russia persists in rebuffing arrest and extradition efforts.[30] Russian authorities know of, and authorities suspect at some level may be even complicit in, the criminal hacking activities of these two.[31] Not surprisingly, extradition is deemed highly unlikely as these criminal activities target US and Western countries only, and squarely advance Russia's

national security policy of weakening the US in response to perceived US interference with Russia's pursuit of its foreign-policy interests.[32] In fact, the Atlantic Council reports that Yakubets consults with Russia's Federal Security Service (FSB).[33] Here, the criminal Internet activity advances Russia's foreign-policy interest in weakening the US. It does this by degrading the public's trust in the Internet as a medium to transact business or conduct social activities, as well as degrading confidence in the ability of the US and Western governments to effectively defend their networks.

AN EFFECTIVE US RESPONSE

Chinese hackers ignored President Xi's 2015 promise to President Obama to refrain from cyber-based economic espionage. The lack of follow-through exemplifies our challenge in compelling adversaries to curb criminal hacking against US targets. Policymakers have invoked several measures to dissuade adversaries from attacking US and Western networks. In addition to the Obama-Xi commitment, the US has rolled out the DoD "Defend Forward" strategy, DOJ "name-and-shame" indictments of overseas hackers, and trade sanctions.[34] Yet, cyber-attacks continue, undeterred, if not even greater than before.[35] The next section examines this threat with our view that even a whole-of-government response is not big enough to make a difference, and why we believe the private sector must be engaged in this effort.

A. Historical Precedent For Private Sector Engagement in Enforcement

Even when working collaboratively, the USG collectively lack the manpower to sift through the millions of cyber-attacks on US networks each month, much less flag and focus on the significant ones.[36] Indeed, the federal government is only able to identify and respond to a small handful of cyber incidents at any given moment, and local governments are even less effective. Large cities have recently begun working on a much-needed first-responder capability for cyber-attacks, but this effort focuses primarily on threat intelligence and incident response.[37] State and local law enforcement capabilities are quite limited, especially their Internet investigative capabilities, and their ability to pursue overseas hackers is almost non-existent. In short, the USG responses amount to no more than a drop in the bucket given the magnitude of this growing threat. This explains why US actions to date have come up short in meaningfully impacting the cost/benefit analysis of adversary governments and the criminals they host.

We believe it highly unlikely that the USG can ever develop a cyber investigative and retaliatory mechanism that effectively deters the myriad threat actors operating from *de facto* safe havens in Russia, China, and elsewhere. To build a defense and deterrence mechanism on a scale adequate to the challenge, the USG must leverage the private sector. We propose doing that by deputizing cyber security firms to hunt down the cyber attackers hitting US networks. There is a rich array of historical precedents for doing this.

1. Bounty Hunters

The War of Spanish Succession from 1702-13 and civil unrest in the Bahamas led to flourishing piracy in Caribbean waters.[39] England's King George I responded with naval force and promises of clemency that had the unintended effect of pushing the pirates to new waters off the coast of the Carolinas.[40] British colonial forces lacked the funding and personnel to counter this growing threat, which in the mid-1700's led colonial authorities in Charleston and elsewhere to offer bounties.[41] The idea was to entice commercial ship owners with sufficient weaponry and skilled sailors to hunt down and capture pirates marauding off colonial America's shores. These so-called bounty hunters became a critical part of the English response to piracy in the colonies and the Caribbean. Bounty hunters were responsible for capturing or killing "The Gentleman Pirate," Stede Bonnet, Blackbeard, Calico Jack, and John Roberts.[42] Rewarding private citizens for taking out pirates with a share of the pirates' stolen loot was controversial, but this practice allowed outgunned colonies to quickly build up a maritime force to the scale needed to counter the piracy threat, and provided a critical and timely solution to a crisis.

The effective role of privateers in fighting piracy as well as acting as naval mercenaries in time of war was in the minds of America's revolutionaries when they drafted the US Constitution.[43] Specifically, they added in Article I, Section 8, authority for Congress to "grant Letters of Marque and Reprisal," a clause commonly understood to permit the USG by act of Congress to hire privateers to interdict vessels of a warring state as well as pirates.[44] This authority can be extended to activities in international or foreign seas as well as US waters, leading some to suggest that cybersecurity firms be issued Letters of Marque to pursue criminal hackers,[45] although this suggestion has met much skepticism from legal and foreign policy experts.[46] We do not agree with the critics who fear cybersecurity firms will run amok in overseas networks, taking systems down in ways that the USG would never do and with diplomatic consequences that outweigh the deterrent impact of their actions,[47] and believe that the risks of this approach can be effectively mitigated. Indeed, as the next example demonstrates, private-sector actors can be deputized in ways that preserve judicial oversight and compliance with legal processes designed to protect legal and constitutional rights.

2. Pinkerton Detectives

Railroads in the western territories of the US faced growing lawlessness around the time of the Civil War. Living on the edge, some settlers turned to crime to survive.[48] Train robbery was lucrative, and at one point, a train robbery occurred once every four days.[49] Frontier towns appointed sheriffs to keep the peace, but they had little time or incentive to investigate train robberies taking place far from the outskirts of town, leaving railroads to fend for themselves.[50] In the 1850s, Illinois Central Railroad hired Allen Pinkerton to guard its railways and depots,[51] and fortuitously, hired a young attorney, Abraham Lincoln, to help

manage Pinkerton's efforts. Although on the railroad's payroll, Pinkerton detectives became *de facto* railway police. Unlike state and territorial authorities, they rode the train across borders and arrested bandits wherever caught.[52] In their heyday, Pinkerton detectives were the bane of railway bandits, infiltrating and bringing the Reno gang to justice as well as forcing Butch Cassidy and the Sundance Kid to flee to Argentina.[53] The Pinkerton detectives successfully employed what we now consider to be the inherently governmental authority of police arrest as well as undercover investigations to put in place a law enforcement capability to protect the railroads that the territories could not provide. Without this, the railroads could not adequately protect passengers and freight, or avoid serious operational disruptions.

It is worth noting that President Lincoln later used Pinkerton as his personal security and as an intelligence asset in the Civil War, helping cement Pinkerton's role as a trusted agent for the government and establishing precedent for entrusting private sector firms with highly sensitive government operations.[54] Unfortunately, Pinkerton detectives were later used to spy on and break up unions,[55] a low point in Pinkerton's history,[56] which should serve as a reminder that private firms charged with carrying out inherently government activities must be subject to the same rigorous oversight and judicial processes we require for government authorities.

Ultimately, use of private sector railway police made its way into the nation's national railway charter. Congress authorized Amtrak, a federally created corporation, to hire and deploy its own railway police.[57] Amtrak police officers attend training at the Federal Law Enforcement Training Centers or an equivalent state school. Amtrak police exercise arrest authority[58] and must afford citizens the same constitutional protections that govern normal police officers (Miranda warnings, Fourth Amendment rights, etc.).[59] We believe that private cybersecurity firms can be similarly engaged in the fight against cyber-attacks, armed with those authorities needed to pursue cyber intruders, and legally bound to honor the protections accorded to individuals suspected of hacking or of owning infrastructure wittingly or unwittingly exploited by criminals.

B. Employing Private Security Firms to Hunt Down Hackers

The US cybersecurity industry (with revenue estimated at $54 billion in 2021)[60] is far larger than the USG's cybersecurity detection and incident response assets will ever be. It also possesses network defense talent and skills at a scale that the USG never could achieve. So, while these firms are already operating within private networks to protect them and to conduct forensic investigations into intrusions, they are prohibited from the more proactive elements of active defense. Private sector firms that pursue intruders beyond the client's network enter a murky legal realm. They risk violating Internet Service Provider's terms of service, state, and federal law, as well as the law of foreign states whose networks they traverse.[61] Yet active pursuit is where the government's capability gap hurts the US the most. To correct this, as with Pinkerton and the bounty hunters, the US cybersecurity industry should be authorized and incentivized to actively engage in hunting down malicious cyber

actors. Ability to chase down hackers in real time and identify their operational platforms, infrastructure and identity would be dramatically improved if private-sector hunters have US broader authorities. Private sector real-time tracking capability will greatly enhance the ability of the US to defend networks and deter attacks. As used here, real-time tracking is analogous to police crossing state lines chasing a suspect. This sort of hot pursuit authority would allow private sector defenders can cross borders and penetrate suspects' systems[62] is the USG's best way to build a rapid response mechanism scaled to the magnitude of the threat and with the means to hunt down, thwart, and otherwise deter the many bad actors that threaten the US now.

PRIVATE SECTOR DETECTIVES AND PRIVATEERS

The Internet, fundamentally a creation of the West, promotes the free flow of information and low-cost commercial transactions at a scale never before possible.[63] It is integral to today's world order and acts as a medium for global communications and trade.[64] Protecting it aligns not only the USG's priorities, but also with the priorities and interests of the US private sector. Responsibly incorporating the private sector more actively into the cyber fray will require effective governance to avoid certain dangers. First and foremost is the profit motive, the concern that private firms might abuse their governmental authorities to pursue profits.[65] Secondly, there is the risk that activities legal here in the US would violate the laws of other countries, thereby exposing US firms to overseas law enforcement or civil actions.[66] Third, there is the possibility that a deputized private sector entity could unwittingly cause serious harm to a third-party or third-party network mistakenly suspected of being the criminal. Fourth, there is the need to avoid chaos by deconflicting the sorts of operations proposed here with overlapping actions by government agencies and other licensed private actors[67] Finally, there is the danger inherent in pursuing a network intruder who is part of a state-sponsored group.[68]

A. Profit Motive

Private firms can be aligned with the national interest in several ways. For example, licenses and contracts can be crafted to align profit with national interest. Licenses would delineate required personnel qualifications, authorized and unauthorized activities, activity reporting, and periodic requalification. The licensed private firm could then solicit business with private companies to protect their networks, offering enhanced services not previously possible without the license. The commercial value of providing customers the enhanced services should, in turn, attract more business for licensed cyber security firms and, as with the railways and Pinkerton detectives, drive deployment of a much larger cadre of threat hunters to protect private sector assets. In the aggregate, this would achieve the national goal of protecting US networks. An important component of such a scheme would be the active, ongoing oversight of licensed firms, to ensure effective accountability. Private firms

would be required to obtain, either directly or through a federal partner, judicial and/or executive approvals necessary to fully protect the rights of US citizens and minimize impacts on third parties.[69]

B. Overseas Investigations

Actions by licensed private cyber defenders beyond US borders invariably will implicate other nations' laws. Tracking a hacker across multiple hops often requires logging onto machines in multiple jurisdictions. Understanding, much less abiding by each country's laws, poses a real challenge, and violations raise the specter of civil liability or criminal prosecution.[70] While this risk is real, it can be mitigated by allowing firms to operate under the same authorities that allow the government to do this. It can also be reduced by working with friendly nations to create common rules of the road for active defense by private companies, particularly when defenders are in hot pursuit of a hacker.[71] Legislation that protects defenders in hot pursuit from prosecution overseas may also be desirable. Finally, firms and their employees, like government employees, must accept some risk that their activities may make them targets of overseas investigations and impact their ability to travel freely.[72]

C. Deconfliction and Government Oversight

Private sector firms must not have free rein to hack into any machine suspected of housing a malicious hacker's activities. In the case of active, ongoing intrusions, an immediate hot pursuit authority is much needed, but must be granted with strict limits on authorized behavior and with immediate or almost-immediate reporting requirements to the proper deconfliction authority. In some instances, a private firm's use of a particular law enforcement tool, such as surreptitious entry, would require executive branch or judicial approval. In other words, as with Amtrak police, a private firm invoking special powers would be subject to the same legal restraints that govern federal agents. These controls and the preparation required to obtain judicial or executive branch approvals would reduce the risk of harm to innocent parties by forcing firms to explain themselves to a third party before acting. If the judge or oversight body agrees the proposed activities are justified then, and only then, would they coordinate and deconflict with ongoing operations by other private firms and federal agencies.[73]

D. Active Federal Management

As noted before, there are situations where network intruders breaking into private US networks are state actors.[74] Although in one reported instance, an individual took down North Korea's entire Internet in retaliation for being hacked by North Korean spies, we recognize that most firms lack the resources and risk tolerance to take on a hostile government.[75] Yet, if we deputize private sector firms to pursue threat actors, some of them will inevitably end up chasing state-sponsored actors. When this happens, it is crucial that the government

and licensed private firms be in communication, so that the government can step in and take over pursuit as warranted. The final section of this article proposes a task force designed to do exactly that.

CYBER ACTIVE DEFENSE TASK FORCE

The federal government should create and empower a private-sector cadre with the proper authorities and the proper oversight to conduct active defense of US networks. This Cyber Active Defense Task Force or CADTF should be overseen by the Office of the Director of National Intelligence with representatives from NSA, CISA, DoD and FBI. They would license and oversee private firms authorized to use active defense tools normally reserved to the government. We use the term "license," but the government-private sector relationship can be contractual, with each firm meeting stringent qualifications to be awarded a contract.[76] The end result of using contracts is similar to licensing, but might obviate a need for legislation.

This CADTF, operating from regional offices, would issue licenses (i.e., contracts) to qualified private sector parties authorizing specific permissive active defense measures.[77] To facilitate licensee governance, we envision the CADTF would issue three tiers of licenses:

- **Hot pursuit team:** These licensees would work for commercial (or government clients), protecting their networks as private cybersecurity firms already do, and further authorize pursuit of network attackers into a client's network.
- **Cyber detectives:** These licensees would investigate threat actors, using special tools such as undercover operations and surreptitious entry (with proper executive or judicial approvals, as required).
- **Network operators:** These licensees would assist regional CADTF officers in managing local hot pursuit teams and cyber detectives, sharing intelligence with various private and public sector counterparts, and setting up infrastructure for regional hot pursuit teams and cyber detectives to use.

A core responsibility of CADTF personnel in each region would be to define required skills and capabilities for each tier of licensees, and to assess on a recurring basis whether licensees were maintaining those skills and qualifications.

A. Hot Pursuit Teams

As with the Pinkerton detectives, hot pursuit teams would work for private sector clients, protecting their networks, but would possess the legal authority to pursue cyber-attackers. Hackers currently can break into networks, then flee across a border or into a third-party network, compelling victim companies and even state authorities to cease pursuit.[78] A hot pursuit license would give the private-sector cyber defender an authority analogous to a police chase. When a state trooper chases a suspect across state lines or into a house, the

trooper does not need to give up the chase but may continue, depending on the nature of the suspected crime and other factors so long as a hot pursuit continues. Network defenders must similarly be empowered to traverse networks across the US and the globe to collect evidence while responding to an ongoing intrusion. A hot pursuit team could follow an intruder across the Internet wherever the intruder goes, collecting evidence on the hacker, its machines, tools, and infrastructure. Eventually, the intruder will disappear behind a firewall or secure host for which there is no obvious access, and the chase must stop. In most cases, this is where hot pursuit would end. While some might argue that such a chase is already legal and already undertaken by private firms tracking stolen data, there is some ambiguity in the law when it comes to scanning hosts and looking for vulnerabilities or other unauthorized means of entering a network or logging onto a host. Also unclear is the consequences of violating Internet Service Providers' terms of service, and the laws of any particular nation implicated. Within clearly defined limits, the USG would authorize hot pursuit teams to pursue intruders across third-party networks.

In the rare situations where the hot pursuit team identifies a vulnerability by which to gain access to the intruder's host or secure network,[79] the CADTF would provide rapid consideration of a request by the team to grant immediate access to the intruder's machine and collect useful information. It would be incumbent, however, on the hot pursuit team to communicate with its CADTF point of contact at the outset of the hot pursuit, reporting their progress and seeking guidance on next steps. A CADTF official could then seek judicial or other required approvals needed before the hot pursuit team would be authorized to access to the intruder's machine. Alternatively, the CADTF official could, upon obtaining required approvals, bring in a government team or a cyber detective team (see below) to take operational control. Either way, the goal would be to immediately enter the intruder's machine or network and harvest evidence about keyboard operators, hacker tools, stolen data, and other evidence of wrongdoing. While taking retaliatory action would generally be barred, a hot pursuit team might request approval to delete copies of customer data if the data clearly confirmed theft from a client.

B. Cyber Detectives

As critical as hot pursuit authorities are, intruders rarely can be traced in real time beyond the first secure device.[80] Getting past the intermediate cut outs that hackers use to obfuscate their true origins requires significant fact gathering, analysis, and operational planning. By the time that process concludes, hot pursuit is long past, which gives rise to the need for the private sector to play a detective-like role. Like the Pinkerton detectives, cyber detective licensees would be empowered to use law enforcement authorities in their investigation of suspected criminal hacker groups. These would include undercover operations, running informants, reconnaissance, and surreptitious entry. Cyber detectives would work with various CADTF counterparts to develop or even execute a scheme of maneuver and must be

prepared to follow up on actionable leads generated by hot pursuit teams. Cyber detectives' activities would be subject to the same judicial and executive branch oversight applicable to a federal agent conducting the same activity. For example, with advance authorization, the cyber detective could use hacking tools to penetrate suspects' machines and collect evidence, or undertake undercover sting operations.

These cyber detectives would honor the same legal restrictions and judicial reviews governing government personnel and answer to the CADTF's deconfliction mechanisms. While risk is never totally eliminated, a cyber detective risk exposure should not exceed that of a federal agent doing the same task. Authorizing the private sector via cyber detective licenses to fulfill this role, however, acts as a force multiplier, greatly increasing the US' ability to pursue intruders, collect evidence of crime, and deter future attacks.

C. Network Operators

Finally, we propose a third tier of licensee, the network operator, who would perform an infrastructure and management role. The need to build out a nationwide response would soon out-scale the USG's ability to manage licensees. CADTF should have regional offices that employ network operators to help manage their operational activities. In each region, CADTF government personnel, working in tandem with network operators, would perform the following functions:

- Build an infrastructure from which cyber detectives and, to some extent, hot pursuit teams, would operate.
- Provide a platform by which local licensees could communicate with the CADTF and other licensees.
- Act as a local or specialized analytical hub focusing on specific needs like local infrastructure protection and the regional threat landscape.
- Interact with CADTF teams nationwide, sharing information and operational plans.
- Manage sensitive taskings entrusted to the region's private sector licensees.

To perform these roles, the network operator licensee must be fully cleared and possess the sophistication and professionalism to act impartially towards other licensees and interact with the CADTF at the highest and most sensitive levels. Because network operators would play a regional role, and not only private firms, but state or local law enforcement can also play this role, thereby allowing for a more effective state and local first responder response to cyber-crime. One variation on this would involve National Guard units that, acting on behalf of the unit's home state, use either its inherent federal authorities or a CADTF detailee role, to spearhead local efforts to defend local networks and investigate intruders. Ultimately, such network operators, supporting a regional CADTF presence would permit a more dispersed and robust defensive ecosystem than we have now with only federal resources.

D. Cyber Active Defense Task Force Management

To ensure that licensees maintain the required qualifications and conduct themselves in accordance with the law, government personnel would always lead or oversee CADTF operations. It is essential the government officials perform these four roles:

- Adjudicate license applicant's qualifications and audit them periodically as licensees.
- Monitor licensees' activities to minimize counterintelligence and/or operational risk as well as compliance infractions.
- Share threat information in real time among CADTF agency members, licensees, and other partners to increase situational awareness and build actionable leads for all.
- Deconflict CADTF activities with other government activities.[81]

Under this management scheme, private sector licensees would be subject to proper oversight and could greatly expand our ability to counter the crippling number, size, and sophistication of cyber-attacks faced by the US.

CONCLUDING THOUGHTS

There is strong, bipartisan resolve to thwart our adversaries ever evident ability to intrude upon US networks and steal or destroy our digital assets. This article proposes a way to counter this trend, but its implementation might, for some parts, will require legislation. To remain effective for the long term, such legislation should refrain from rigidly defining either the threat or the solution. Technology evolves at warp speed and many technical, legal, and practical lessons will be learned as private-sector cyber defenders enter the fray. Effective legislation should articulate precise authorities and limits,but leave executive branch personnel with flexibility in managing the public-private active defense partnership proposed here.

Our proposal would dramatically increase the number of active defenders available to fend off cyber-attacks. Across the nation, hot pursuit teams would operate inside client networks, guarding against intrusions, but would be empowered to move outside their defended networks, when attacked, to track intruders as far back as possible. Cyber detectives would engage in the long-term effort to identify and hunt down malicious actors, using law enforcement tools such as undercover operations and surreptitious entry when necessary. Finally, network operators would maintain the regional infrastructure required to house this public private partnership of active cyber defenders across the US. These three tiers of federal licensees would act as a force multiplier, bringing in a larger number of active network defenders than the government could ever provide.

The overriding goal of this article is to advance the operational need for and strategic value of bringing the private sector into a deeper and wider partnership with the government in defending our nation's increasingly imperiled networks. Without robust private sector augmentation, federal resources are simply inadequate to respond effectively and counter the millions of cyber-attacks that take place every month. US networks lie heavily in the private sector. To get this job done right, the private sector must shoulder a greater share of the burden of actively defending these networks. Our adversaries are fully engaged with criminal private sector elements whose activities undermine our citizens' ability to enjoy and rely on the Internet. We must find ways to deputize and otherwise entrust our enormously talented private sector to counter them. The USG needs the private sector as a full partner in hunting down malicious actors and taking them offline.

NOTES

1. Steve Morgan, Editor-in-Chief, Special Report: Cyberwarfare in the C-Suite, Cybersecurity Ventures (Sausalito, CA, November 13, 2020), https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.
2. See, for example, IBM Security, "Cost of a Data Breach Report 2021" (July 2021), Ponemon Institute, November 12, 2021, https://www.ibm.com/security/data-breach?mhsrc=ibmsearch_a&mhq=data%20breach.
3. Briefing Room, White House, "FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware," October 13, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.
4. Sam LaGrone, "Report: China Hacked Two Dozen U.S. Weapon Designs," *USNI News* (May 28, 2013), https://news.usni.org/2013/05/28/report-china-hacked-two-dozen-u-s-weapon-designs.
5. Ibid.
6. See Staff, "Significant Cyber Incidents," Center for Strategic & International Studies, November 13, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
7. Josh Fruhlinger, "The OPM hack explained: Bad security practices meet China's Captain America," CSO Online (February 12, 2020); Josh Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" CSO Online (February 12, 2020); Saheed Oladimeji & Sean Kerner, "SolarWinds hack explained: Everything you need to know," TechTarget (June 16, 2021); and Kate Conger & Sheera Frenkel, "Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China," *The New York Times* (August 26, 2021), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html, https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html, https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know, https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html.
8. Staff, "The Biggest Hacks of 2021 (So Far)," *Gizmodo,* November 13, 2021, https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024/slides/1.
9. David Sanger, Nicole Perlroth, and Eric Schmitt, "Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit," *The New York Times (*December 14, 2020), https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html.
10. COL Timothy M. McKenzie, "Is Cyber Deterrence Possible?" Air Force Research Institute Papers (January 2017), https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF.
11. Adm. Dennis C. Blair, Hon. Michael Chertoff, Frank J. Ciluffo, & Nuala O'Connor, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," 4, Center for Cyber & Homeland Security, George Washington University (October 2016), https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.
12. Department of Justice, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," press release (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
13. Scott W. Harold, "The U.S.-China Cyber Agreement: A Good First Step," RAND blog (August 1, 2016), https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html.
14. Tim Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals," Carnegie Endowment for International Peace (February 2, 2018), https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499.
15. See, for example, Katie Benner & Nicole Periroth, *"China-backed Hackers Broke into 100 Firms and Agencies, U.S. Says," The New York Times (*September 16, 2020), https://www.nytimes.com/2020/09/16/us/politics/china-hackers.html; Bobby Allyn, *"Russian Hacking Group Evil Corp. Charged by Federal Prosecutors in Alleged Bank Fraud," NPR* (December 5, 2019), https://www.npr.org/2019/12/05/785034567/russian-hacking-group-evil-corp-charged-by-federal-prosecutors-in-alleged-bank-f.
16. Tim Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals," Carnegie Endowment for International Peace (February 2, 2018), https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499.
17. Ibid.

NOTES

18. See Shanthi Kalahil, "Internet Freedom: A Background Paper," Aspen Institute (October 2010), https://www.aspeninstitute.org/wp-content/uploads/files/content/images/Internet_Freedom_A_Background_Paper_0.pdf.
19. Scott Jasper, "Assessing Russia's role and responsibility in the Colonial Pipeline attack," Atlantic Council (June 1, 2021), https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/.
20. Ibid.
21. Ibid.
22. Joseph Marks, "The Cybersecurity 202: The U.S. and allies are taking a stand against Chinese hacking. Here are three takeaways," *The Washington Post* (July 19, 2021), https://www.washingtonpost.com/politics/2021/07/19/cybersecurity-202-us-allies-are-taking-stand-against-chinese-hacking-here-are-three-takeaways/.
23. Katie Benner and Nicole Periroth, "China-backed Hackers Broke Into 100 Firms and Agencies, U.S. Says," *The New York Times* (September 16, 2020), https://www.nytimes.com/2020/09/16/us/politics/china-hackers.html.
24. Ibid.
25. Ibid.
26. Ibid.
27. Ibid.
28. Matt Burgess, "Leaked Ransomware Docs Show Conti Helping Putin From the Shadows," *Wired* (March 18, 2022), https://www.wired.com/story/conti-ransomware-russia/.
29. Bobby Allyn, "Russian Hacking Group Evil Corp. Charged by Federal Prosecutors in Alleged Bank Fraud," NPR (December 5, 2019), https://www.npr.org/2019/12/05/785034567/russian-hacking-group-evil-corp-charged-by-federal-prosecutors-in-alleged-bank-f.
30. Ibid.
31. Ibid.
32. Scott Jasper, "Assessing Russia's role and responsibility in the Colonial Pipeline attack," Atlantic Council (June 1, 2021), https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/.
33. Ibid.
34. Scott W. Harold, "The U.S.-China Cyber Agreement: A Good First Step," RAND blog (August 1, 2016); Department of Defense, "DoD Cyber Strategy 2018" (articulating "defend forward" strategy); Derek B. Johnson, "DOJ official says 'name and shame' is one piece of the puzzle" (January 18, 2019); and staff, "US imposes sanctions on Russia over cyber-attacks," BBC (April 16, 2021), https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, https://fcw.com/articles/2019/01/18/demers-doj-cyber-shame.aspx, https://www.bbc.com/news/technology-56755484.
35. COL Timothy M. McKenzie, "Is Cyber Deterrence Possible?" Air Force Research Institute Papers (January 2017), https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF.
36. Zachary Cohen, Vivian Salama, & Brian Fung, "Concern mounts over government cyber agency's struggle to respond to hack fallout," CNN (January 2, 2021), https://www.cnn.com/2021/01/02/politics/hack-goverment-cyber-struggle-respond-fallout/index.html.
37. Maxim Kovalsky, Deputy CISO for NYC Cyber Command, "Overview of NYC Cyber Command," ISSA-NOVA Chapter Meeting (September 23, 2021) (Roth attended online presentation).
38. Maggie Bruner, "Challenges and Opportunities in State and Local Cybercrime Enforcement," *Journal of National Security Law & Policy*, Vol. 10:563, 572, 578.
39. Dr. Nic Butler, "The Pirate Hunting Expeditions of 1718," Charleston County Public Library (November 23, 2018), https://www.ccpl.org/charleston-time-machine/pirate-hunting-expeditions-1718.
40. Ibid.
41. Ibid.
42. Ian Harvey, "Pirate Hunters risked their lives to bring the Golden Age of Piracy to a close," *Vintage News* (February 9, 2017), https://www.thevintagenews.com/2017/02/09/pirate-hunters-risked-their-lives-to-bring-the-golden-age-of-piracy-to-a-close/.

NOTES

43. Ensign Lucian Rombado, "Grant Cyber Letters of Marque to Manage Hack Backs," U.S. Naval Institute (October 2019), https://www.usni.org/magazines/proceedings/2019/october/grant-cyber-letters-marque-manage-hack-backs.
44. William Young, "A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal," 66 *Wash. & Lee L. Rev* 897-898 (2009), https://law2.wlu.edu/deptimages/Law%20Review/66-2Young.pdf.
45. Frank Colon, "Letters of Marque for Private Sector Cyber Defense," Cybersecurity & Information Systems Information Analysis Center (Vol. 7, Issue 4, Spring 2020), https://csiac.org/articles/rebooting-letters-of-marque/.
46. Rombado, "Grant Cyber Letters of Marque to Manage Hack Backs."
47. See, for example, Jen Ellis, "Why hack back is still wack: 5 causes for concern," *Security Magazine* (October 13, 2021), https://www.securitymagazine.com/articles/96295-why-hack-back-is-still-wack-5-causes-for-concern.
48. Staff, "How wild was the Wild West?" History Extra, BBC (July 1, 2019), https://www.historyextra.com/period/victorian/wild-west-how-lawless-was-american-frontier/.
49. Marshall Trimble, "The Train Robbers," *True West Magazine* (November 2018), https://truewestmagazine.com/article/the-train-robbers/.
50. "Pinkerton, Allan," Encyclopedia.com (May 29, 2018), https://www.encyclopedia.com/people/social-sciences-and-law/crime-and-law-enforcement-biographies/allan-pinkerton.
51. Staff, "How wild was the Wild West?" History Extra, BBC (July 1, 2019), https://www.historyextra.com/period/victorian/wild-west-how-lawless-was-american-frontier/.
52. "History," Railroad Police (undated), https://www.therailroadpolice.com/history, https://www.therailroadpolice.com/history.
53. Staff, "How wild was the Wild West?" History Extra, BBC (July 1, 2019), https://www.historyextra.com/period/victorian/wild-west-how-lawless-was-american-frontier/.
54. Ibid.
55. "Pinkertons," *Encyclopedia of Chicago* (undated), http://www.encyclopedia.chicagohistory.org/pages/969.html.
56. Ibid.
57. 49 U.S.C. § 24305(e) (codifying Railroad Passenger Services Act of 1970).
58. Ibid.; Paul Miller, "The Railroad Police – history" (undated), http://www.therailroadpolice.com/history.
59. US v. Tillman, E.D. La (Criminal Docket No 14-041) (circa February 18, 2014), DOJ memo noting that defendant was "Mirandized," https://www.justice.gov/file/339456/download.
60. Staff, "Cybersecurity," Statista (undated), https://www.statista.com/outlook/tmo/cybersecurity/united-states.
61. Adm. Dennis C. Blair, Hon. Michael Chertoff, Frank J. Ciluffo, & Nuala O'Connor, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," Center for Cyber & Homeland Security, George Washington University (October 2016), https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.
62. See, for example, Robert Barnes, "Supreme Court tightens, slightly, rules for police entering a home without a warrant," *The Washington Post* (June 23, 2021); Public, "Hot Pursuit," *Wikipedia* (undated), https://www.cbjlawyers.com/decision-in-hot-pursuit-case-unlikely-to-have-significant-ramifications/, https://en.wikipedia.org/wiki/Hot_pursuit.
63. Jessica Nicholson & Giulia McHenry, "Measuring Cross-Border Data Flows: Data, Literature, and Considerations," Internet Policy Task Force, National Telecommunications and Information Administration, Department of Commerce (May 10, 2016), https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows_pre-roundtable_materials_2016_05_05v2.pdf.
64. Homepage, Internet Policy Task Force, National Telecommunications and Information Administration, U.S. Department of Commerce (May 10, 2016), https://www.ntia.doc.gov/category/internet-policy-task-force.
65. Staff, "Country Case: Inherently governmental and critical functions in the United States", OECD (undated), https://www.oecd.org/governance/procurement/toolbox/search/inherently-governmental-critical-functions-united-states.pdf.
66. See, for example, Peter Singer, "The Dark Truth about Blackwater," Brookings Institution (October 2, 2007), https://www.brookings.edu/articles/the-dark-truth-about-blackwater/.
67. See Police Foundation, "Best Practices in Event Deconfliction," CALEA (October 2016), 1, https://www.calea.org/sites/default/files/2019-02/EventDeconfliction_PoliceFoundation.pdf.

NOTES

68. See, for example, Robert McMillan and Aruna Viswanatha, "North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says," *The Wall Street Journal* (February 17, 2021), https://www.wsj.com/articles/u-s-authorities-charge-north-koreans-in-long-running-hacking-scheme-11613581358; but also see, 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/.
69. Staff, "Country Case: Inherently governmental and critical functions in the United States," OECD (undated), https://www.oecd.org/governance/procurement/toolbox/search/inherently-governmental-critical-functions-united-states.pdf.
70. "An in-depth look at hacking back, active defense, and cyber letters of marque," MalwareTech (November 7, 2021), https://www.malwaretech.com/2021/11/an-in-depth-look-at-hacking-back-active-defense-and-cyber-letters-of-marque.html
71. See, for example, Press Release, "Schengen Area – The Commission proposes to facilitate cross border surveillance and 'hot pursuit' between Member States", European Council, European Union (July 19, 2005), https://ec.europa.eu/commission/presscorner/detail/en/IP_05_970.
72. Gaia Pianigiani, "Italy Jails Ex-Officials for Rendition," *The New York Times* (February 12, 2013), https://www.nytimes.com/2013/02/13/world/europe/former-italian-military-officials-sentenced-in-abduction-of-abu-omar.html.
73. Office of Counterintelligence (DXC), Defense CI & HUMINT Center, Defense Intelligence Agency, "Terms and Definitions of Interest for DoD Counterintelligence Professional," at GL-129 (May 2, 2011).
74. Robert McMillan and Aruna Viswanatha, "North Korea Turning to Cryptocurrency Schemes in Global Heists, U.S. Says," *The Wall Street Journal,* https://www.wsj.com/articles/u-s-authorities-charge-north-koreans-in-long-running-hacking-scheme-11613581358.
75. Andy Greenberg, "North Korea Hacked Him. So He Took Down its Internet," *Wired* (February 2, 2022),
76. See, for example, Federal Acquisition Rules, Subpart 9.104-2, Special Standards:
    " (a) When it is necessary for a particular acquisition or class of acquisitions, the contracting officer shall develop, with the assistance of appropriate specialists, special standards of responsibility," https://www.acquisition.gov/far/part-9#FAR_9_104_2
77. Blair et al., "Into the Gray Zone," 19.
78. Ibid., 8-11.
79. This would include the use of payloads embedded in files on client networks that an intruder might steal and execute from the intruder's machine.
80. Panayotis A. Yannakogeorgos, "Strategies for Resolving the Cyber Attribution Challenge," 12, *Perspectives on Cyber Power,* Air Force Research Institute Papers (December 2013), describing compromised hosts used as cutouts as "botnets," https://media.defense.gov/2017/May/11/2001745613/-1/-1/0/CPP_0001_YANNAKOGEORGOS_CYBER_TTRIBUTION_CHALLENGE.PDF.
81. If the U.S. Department of Justice (DOJ) pursues a prosecution based on a CADTF licensee's report, the CADTF licensee must be prepared to serve as a witness.