Implementing the Paris Call Principles

Principle #8: No Private Hack Back

NO HACKING BACK: VIGILANTE JUSTICE VS. GOOD SECURITY ONLINE

A POLICYMAKER'S GUIDE TO KNOWING THE DIFFERENCE

EXECUTIVE SUMMARY

In 2018, the Paris Call for Trust and Security in Cyberspace became the largest ever global multistakeholder commitment to principles for responsible behavior in cyberspace. Among the agreement's nine principles is a commitment to prevent private sector hack back. This term, "hack back," is generally accepted as referring to offensive actions that private sector organizations might take, independent of governments, in response to a cyberattack in order to either steal back from, or otherwise cause harm to, the computer systems or networks of attackers. In other words, retaliatory hacking, often violating criminal and civil legal obligations in the process. The Paris Call principle discouraging such behaviors is essential to a rules-based international order in cyberspace where, just as in the physical realm, governments must play a leading role in enforcing laws and holding criminals accountable.

Unfortunately, however, hack back is not as simple to define as the above might led you to believe. In order to respond to an ever-changing threat environment, the private sector, especially the technology industry, needs to continuously innovate to create more effective security measures, some of which are more intrusive than others. Such measures are increasingly important for keeping users and customers everywhere safe and also require companies to pay close attention to the legal obligations that exist in this space, as those duties persist even amid a changing threat landscape.

As the majority of cyberspace is owned, operated and maintained by private industry, many of the actions taken by government agencies and law enforcement groups against malicious actors online inevitably require private sector to comply with legal demands and process. In a limited number of cases, there may be also be coordination to disrupt malicious activity. As a result, policymakers considering how best to approach the subject of hack back should be careful to do so with a scalpel, as opposed to a hammer – to avoid encouraging dangerous hack back activities, while at the same time not inadvertently prohibiting measures that have become important in maintaining good security, and leaving space for continued innovation in security practices by the private sector. If any government is considering a revision of its criminal or civil laws to further enable private sector organizations to take action against attackers, it is essential to engage private sector groups in a dialogue before doing so. Such policies should be based on where the private sector may need to have more latitude to respond to an incident while not creating loopholes that allow for bad actors to flourish, or enable other unintended consequences to occur.

The Cybersecurity Tech Accord, the largest industry commitment to cybersecurity principles and an early supporter of the Paris Call, has produced this report to share its perspective and further advance this discussion. As an organization that includes over 140 technology firms from across the globe, the Cybersecurity Tech Accord has unique insights into what is – and importantly, what isn't – "hacking back". The report seeks to clarify where and how these lines should be drawn in order to support the implementation of this key principle of the Paris Call in the spirit of the agreement itself – collaborating across stakeholder groups to advance trust and security in cyberspace. In addition, the report also includes at the end brief case studies as examples of the kinds of active defense practices, and coordinated activities with governments, that the companies who have signed the Cybersecurity Tech Accord employ in the interests of keeping users and customers safe.

If you have any questions about the contents of the report or would like to discuss the topic further, please feel free contact the Cybersecurity Tech Accord Secretariat: **info@cybertechaccord.org.**

Contents

Terms Used

Private Hack Back:

Unauthorized access to a protected computer or network by individuals or organizations, following an attack, in order to steal data or otherwise harm an attacker.

Active defense:

Proactive security measures, taken by organizations, in their own computer systems or by consent of customers, to identify or thwart potential threats or attempted/ ongoing cyberattacks in a manner consistent with criminal and civil laws.

Passive defense:

Good practices intended to strengthen a digital security environment to ensure that a successful cyberattack is less likely.

The Paris Call for Trust and Security in Cyberspace

In 2018, French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace. This landmark agreement set a new standard for multistakeholder cooperation in promoting stability, security, and resilience in the online world.

As cyberspace is an inherently shared domain, the Paris Call is based on a belief that governments, along with civil society and private industry, all have unique and overlapping roles and responsibilities when it comes to cybersecurity and promoting a rules-based international order online. In this multistakeholder community, the technology industry in particular, as the owners and operators of the majority of what we consider "cyberspace," has unique responsibilities for its security.

Paris Call Principle #8

"No private hack back: Take steps to prevent non-state actors, including the private sector, from hacking-back, for their own purposes or those of other non-state actors."

The Cybersecurity Tech Accord

Also founded in 2018, the Cybersecurity Tech Accord is a coalition over 140 global technology firms committed to advancing trust and security in cyberspace based on four foundational cybersecurity principles.

By combining the resources and expertise of the global technology industry, the Cybersecurity Tech Accord creates a starting point for dialogue, discovery and decisive action. Through a shared commitment and collective action, signatories aim to more effectively:

- Provide their customers, users and the developer ecosystem with information and tools that enable them to understand current and future threats and better protect themselves.
- Protect their customers and users everywhere by designing, developing and delivering products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability and severity of vulnerabilities.
- Work with each other and likeminded groups to enhance cybersecurity best practices, such as improving technical collaboration, coordinated vulnerability disclosure and threat sharing, as well as ensuring flexible responses for the wider global technology ecosystem.
- Oppose efforts to attack citizens and enterprises by protecting against exploitation of technology products and services during their development, design, distribution and use.

I. Introduction

Much ink has previously been spilt calling attention to cyberspace emerging as a new domain of conflict – the proverbial "fifth domain", where nation states are developing military capacities and strategically positioning themselves vis-à-vis adversaries. However, underlying this discussion is a broader reality that cyberspace has emerged a significant domain of human activity. In advanced economies, it is not uncommon for individuals to spend as much as 8 hours each day online, doing everything from banking, to gaming, and working.

This new reality has only been accelerated during the COVID-19 pandemic, as many around the world have transitioned to working, learning, and socializing entirely remotely. While almost half of the globe's population still does not have access to the internet, this digital divide is also closing rapidly.[1] And just like any other domain of human activity – in our communities, on the seas, even in the air – there needs to be clarity around what the rules are, who enforces them when they are broken, and how. This applies to all actors – whether they are governments, private industry, or individuals – and this is why action needs to be taken on both domestic and international levels to set and enforce expectations.

An emerging patchwork of laws and the "hack back" principle

Unfortunately, national legislative and technical infrastructures are generally outpaced by an escalating and evolving threat landscape online. While national cybercrime laws and other laws extending protections to digital environments are becoming increasingly common, there are still countries that have yet to pass such legislation. Even when these laws are in place, however, there is still the need to build the necessary infrastructure to enable law enforcement in a digital environment, where criminal activities frequently take place instantaneously and across multiple jurisdictions. Moreover, as technology develops and we continue to discover all the different ways humans can interact online, these legal frameworks and capacities need to be continually revisited and updated to stay current with the threat landscape. Finally, a growing cybersecurity skills gap often leaves governments short-handed and struggling to retain the necessary personnel to implement even well-designed legal frameworks.

Internationally, there have been valuable, if insufficient, efforts to set expectations and improve cooperation in cyberspace to combat increasing numbers of cyberattacks. This includes the Budapest Convention on Cybercrime[2], and the norms for responsible state behavior in cyberspace established by the UN Group of Governmental Experts on information security in 2013[3] and 2015 [4]. Most recently, in 2018, the Paris Call for Trust and Security in Cyberspace became the largest multistakeholder international agreement to promote long-term stability and responsible behavior in cyberspace. While its nine voluntary principles largely mirror commitments and norms that have been included in previous agreements between nation states, the Paris Call sets itself apart by featuring expectations for other stakeholders as well. This includes principle number eight, which highlights a clear boundary for behavior on the part of the private sector:

[1] *Report of the Secretary-General: Roadmap for Digital Cooperation. United Nations. June, 2020.* https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

[2] *The Convention on Cybercrime. Council of Europe. Strasbourg Cedex, France. 2020.* https://www.coe.int/en/web/cybercrime/the-budapest-convention

[3] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations. June 24, 2013.* https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf

[4] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations. July 22, 2015.* https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

> ### "Principle #8: No private hack back"
>
> *[Supporters will] Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.*[5]

"Hack back" here refers to certain retaliatory actions taken in response to cyberattacks, and the principle speaks to an important question about enforcing rules in cyberspace: who is supposed to respond when things go wrong and when rules are broken? According to this principle, in the wake of a cyberattack which steals data or harms computer systems, the private sector and other non-state actors should refrain from unilaterally trying to steal back stolen data or otherwise harming the attackers in response.

Why "No private hack back?"

On the surface, this principle may seem counterintuitive, as we might logically want to empower individuals and organizations to defend themselves, if possible, by retrieving their own stolen materials and preventing bad actors from harming others. This may even seem expeditious, as private sector actors often have more advanced capabilities, compared to government counterparts, for tracking and tracing those responsible for illegal activity online and for taking action. As mentioned earlier, in many countries the legal, diplomatic and technological infrastructure for government law enforcement to protect cyberspace is still developing and may inevitably lag behind an escalating and constantly changing threat landscape.

Despite this dynamic, however, it is nevertheless essential that the private sector is not independently responsible for, or empowered to, hack back to hold criminals and other malicious actors accountable. In most countries, hacking back would constitute a criminal act. In addition, such action carries with it unique risks, including potentially provoking further escalation with a sophisticated actor, even a nation state; retaliating against the wrong individual(s) altogether and causing further damage; or failing to anticipate unintended consequences of the response and causing further harm – potentially on a global scale. Private hack back might also create a false sense of one's ability to mitigate an attack, which is not possible without law enforcement's legal authorities to investigate, collect information, and hold individuals accountable according to the law. Instead, what is needed is for law enforcement to be trained and resourced in such a way that enables a more effective response to incidents, and for the private sector to be able to engage in collaborative activities with law enforcement in new and non-traditional ways that help address the asymmetric reality we currently face – while bad actors attack with relative ease, and without significant risk of consequence, private organizations and individuals require traditional law enforcement in response to all cyberattacks.

The following sections of the report will seek to explain where private sector security responsibilities end and where government responsibilities begin, and what should and should not be considered "hack back" This begins with drawing a comparison to security and law enforcement responsibilities in the physical world that should extend to the digital domain as well. From there, the report explains the different kinds of defensive security activities the private sector should continue to pursue, and what kinds of actions should only be done in cooperation with law enforcement or with other government authorization. The report then includes specific guidance and recommendations for policymakers to help reinforce cooperation between the public and private sector, maintain high security standards, and discourage hacking back. Finally, the report concludes with several case study examples of forward-leaning security practices led by Cybersecurity Tech Accord companies that help illustrate the difference between active defense measures, cooperating with governments to uphold rules and expectations in cyberspace, and hacking back.

Section II, below, considers how the Paris Call principle eight, "No Private Hack Back," relates to a scenario in the physical world where someone's personal information or belongings are stolen or harmed in an attack.

[5] *The Paris Call For Trust and Security in Cyberspace. Ministry for Europe and Foreign Affairs, France. November 12, 2018.* https://pariscall.international/en/principles.

II. Physical world example: The safe deposit box

Gary keeps a safe deposit box at the local branch of a national bank, where he stores cash and other personal valuables. In doing so, Gary and the bank assume certain responsibilities, governed by a contract between Gary and the bank, and through business processes of the bank. Gary will protect and keep confidential his access credentials, such as a key or combination to the safe deposit box, as well as his methods of personal identification. Meanwhile, the bank will ensure that the safe deposit box is kept secure on their premises via security staff and physical barriers. The bank may even take additional precautions, such as placing a tracking device on the safe deposit box so it can be recovered if stolen, or setting the contents of the box to destruct if they are improperly opened. However, despite all precautions there is always the risk that a sufficiently sophisticated attacker will find a way around these protections and steal the contents of the safe deposit box.

In the event of a successful theft, in which the Gary's possessions are compromised and the robbers manage to escape, responsibilities would generally then shift to the police or other government agencies responsible for law enforcement – to recover stolen property and punish those responsible. In most cases, we would not want Gary or the bank to take matters into their own hands and independently track down those responsible for the robbery in order to either steal back stolen property or otherwise seek retribution/retaliation. Supporting such activity would be to encourage lawlessness and vigilante justice in enforcing the law and would run the risk of causing further harm and inviting further violations of the law. In addition, such expectations would dramatically increase the responsibilities and costs of operating a bank or any business to begin with, if every time there was a robbery the victim organization was responsible for law enforcement actions. Gary may protect his legal rights, as governed by the contract between Gary and the bank, so he does have recourse to protect himself and his interests. But independent action by Gary to "steal back" his property would be a crime, subjecting Gary to legal risk.

This is not to say that law enforcement agencies wouldn't leverage additional support from private third parties in fulfilling their duties. In fact, the police would most certainly want to work with Gary and the bank to better understand the incident and who might be responsible for stealing the safe deposit box. The police may also seek the expertise or assistance of outside groups with specific technical or subject-matter expertise related to bank robberies or the area where the attack took place. The police can engage with experts, victims, third parties, and collect information – consistent with their legal authorities. However, none of this would shift the basic responsibility for investigating the crime or enforcing the law as an exclusive province of government authority, fundamental to its sovereignty.

While there is more nuance (see section III), the basic dynamics at play in this example should hold true in cyberspace as well and help illustrate why a prohibition on private "hack back" is important in reinforcing a rules-based order in cyberspace. As in the example, private organizations have responsibilities for the cybersecurity of the data they own and house, for themselves and their customers. However, these responsibilities do not extend beyond securing and protecting one's own systems and networks, and direct actions against attacker networks must largely be the responsibility of governments and law enforcement agencies.

III. Passive Defense, Active Defense, and Hack Back

Parallels between the physical world and cyberspace, as in the scenario described above with the safe deposit box, have limitations. As compared to physical domains, threats in cyberspace are more rapidly and constantly evolving alongside each new innovation. In addition, there are fewer geographic limitations in cyberspace, meaning that everyone can be exposed to the most advanced threats anywhere in the world. This dynamic requires the private sector, and technology companies in particular, to be continually developing and deploying new and forward-leaning security tools and techniques to counter the most sophisticated threats. Such capabilities, however, are designed to adhere to clear policy frameworks and legal requirements, including jurisdictional boundaries. Taking direct action against attackers via unauthorized access to protected computers/networks is a responsibility which the technology industry neither wants nor can fulfil on its own.

"Passive" and "Active" defense – a spectrum of responsible practices

In implementing a comprehensive and responsible approach to cybersecurity, private organizations today employ a range of both so-called "passive" and "active" defense measures. "Passive" defense refers to things like practicing good cyber hygiene (see our video series HERE), monitoring systems owned and operated by the organization, and logging network activities and issuing reports on suspicious activity.[6] "Active" defense, on the other hand, encompasses a spectrum of more proactive measures that organizations may deploy in advance of, or in response to, a cyber threat or attack.

Common active defense techniques include (in order from least to most intrusive): [7]

- **Honeypots** or **honeynets**, which lure attackers into an isolated system through a deliberate vulnerability, thus preventing access to other network areas.
- **Sandboxes** or **tarpits**, which provide barriers to slow or halt incoming suspicious traffic in order to isolate, examine, and ultimately eradicate any malicious content.
- **Patching**, via a software update which allows defenders more granularly to address security vulnerabilities or software stability issues that may be exploited by attackers.
- **Sinkholing**, which redirects malicious traffic to a system under control of the defender.
- **Digital beacons or dye-packets**, which are embedded code that can activate and alert the defender if the file is stolen from its network.[8]

Importantly, all of the practices described above take place in environments that belong to an organization or its customers in order to prevent, identify, or track attacks or suspicious activity and to remain consistent with the law. Broadly speaking, private organizations need to be able to protect their own systems and act in customer environments, with consent, to improve security and uphold terms of service/use. These active defense measures can require considerable resources, including threat-monitoring capabilities, as well as the means to rapidly identify and thwart potential attackers. Threat sharing and other cooperative relationships can help build these capacities, and there is a growing market of third-party security vendors who can also provide such active defense protections.[9] Using any of the active defense measures listed above also requires close coordination with legal counsel, to ensure that the activity remains consistent with existing laws.

[6] *Hoffman, Wyatt, Ariel E. Levitt. Private Sector Cyber Defense: Can Active Measures Help Stabilize Cyberspace? Carnegie Endowment for International Peace. Washington D.C., USA. 2017.* https://carnegieendowment.org/files/Cyber_Defense_INT_final_full.pdf

[7] *Project Report: Into the Grey Zone: The Private Sector and Active Defense Against Cyber Threats. Centre for Cyber & Homeland Security, The George Washington University. Washington D.C. USA. Oct. 2016.* https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf

[8] *Hoffman, et al.*

[9] *Brown, Brad, Daniel Ennis, James Kaplan, Jim Rosenthal. To survive in the age of advanced cyberthreats, use 'active defense'. McKinsey Digital. Nov. 29, 2017.* https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/to-survive-in-the-age-of-advanced-cyberthreats-use-active-defense

Legally sanctioned actions to protect customers

Still another category of actions which would not be considered hack backs are those conducted by private companies in their own environments, or in third party environments to thwart attackers based on legal authority. The legal authority to take action against bad actors in other networks can come from different sources, depending on the jurisdiction. This might include authorization for a specific action by a court, or a broader authority based on notification of illegal activity.

Actions by private organizations operating under such authorities might include:

- **Botnet takedowns,** which involve technical actions to identify and sever the command and control network of compromised computers, which can otherwise be co-opted for use in coordinated and repeated attacks.
- **Disruption of attacker networks** via technical actions in order to prevent them from conducting further malicious cyber operations.

In each case, however, these actions are not hack backs because they are done consistent with legal authorization.

Hacking back – what it is and what it isn't

In contrast to the measures described above, private *"hack back" involves the unauthorized access to a protected computer or network by individuals or organizations, following an attack, in order to steal data or otherwise harm an attacker.*

Some examples of hack back actions might include:

- **Reconnaissance on actor systems** by accessing machines under the actor's control without authorization, regardless of whether they are owned by the actor or, more likely, an unwitting victim.
- **Stealing back data** by infiltrating an attacker's system and retrieving or destroying data that was previously stolen.
- **Destroying or Blocking data** that has been exfiltrated, but has not been taken back, often by encrypting the data.
- **Destroying attacker systems** via destructive action, the most offensive retaliatory action in cyberspace, which is intended to prohibit an attacker from being able to use their systems again.

These are the types of activities that would qualify as hack backs and likely violate criminal laws. In each case, there is also a risk that any action taken by the party hacking back can make an error, disabling or encrypting someone else's data, or other unintended consequences that will be dependent upon the facts of the attack. When a party decides to undertake a hack back the decision must be made with the clear understanding that the action may violate criminal law, and intended or unintended consequences may also give rise to significant civil liability.

IV. Legality, liability and risk in hacking back

It is not hard to see the appeal of policies that would support hack back and why they have gained traction in some circles in recent years, despite laws that criminalize the conduct. The great challenge of law enforcement in cyberspace today is its complexity. Cyberattacks are notoriously intricate – crossing jurisdictional boundaries and leveraging slow and challenging processes to collect evidence internationally, as well as requiring technical expertise to build a case – if the thresholds of the case are significant enough to merit the investment of time and resources from the law enforcement organization. The sheer volume of cases also makes it impossible for all cybercrime activity to be investigated, the perpetrators be brought to justice, and in some cases, stolen property returned. All of this can, and indeed has, led some to believe that instead of waiting for governments to build the capacities and relationships necessary to address growing numbers of cyberattacks, we should simply empower private companies to take action on their own behalf.

Despite these arguments, however, simply encouraging companies to hack back raises troubling legal questions. Cyberattacks often originate in one country and transit across numerous foreign servers to their ultimate deployment in entirely different regions. As such, permitting private sector hack back would quickly raise complicated jurisdictional questions with implications for both international law and the domestic laws of respective countries involved in the attack.

Regardless of location, however, most hack back activities themselves would also likely violate basic computer crime laws regarding access to, tampering with, or impairing other computer systems, exposing private organizations to significant legal risk in trying to respond to a cyberattack via their own hacking.[10] As Cybersecurity Tech Accord signatory Cisco Systems highlighted in a 2019 report on threat hunting, "in most locations in the world doing so [hacking back] is illegal. Despite the fact that the systems in question are performing illegal activities, offensive hacking is still hacking."[11] Companies must also face the reality that deciding to hack back is an intentional act – and the planning and execution of that with a group of people can have additional criminal legal consequences.

Once the criminal legal questions of trespass, access to chattels, fraud, racketeering, or other potential criminal claims are considered, any person considering hacking back must also consider the civil law risks. As an example, the US Computer Fraud and Abuse Act allows civil claims under the statute, and the claims are essential tools to litigants seeking to protect themselves and their interests.[12] If the party "hacking back" causes damage to another individual or organization – even an unknowing victim of the same attack, whose machines are being abused – the party "hacking back" assumes the risk and liability for damages arising out of those actions. If an attempt to "disable" a victim's data stored on an attacker's server goes wrong, and the all of the data and functions on that server are disabled – not just the hacking back party, but the underlying victim whose server was being used by the attacker – the party doing the hacking back can be liable for the loss of that server. Based on the types of impact, the consequences can be significant, and tort damages can be notoriously high.

Beyond these questions of legality, however, there are several additional reasons why private hack back is ill-advised policy and why private industry would not want to pursue such actions even if they were permitted/encouraged to do so.

[10] *In the United States, such activity would be prohibited by Title 18 of the U.S. Code, Section 1030, Fraud and related activity in connection with computers.* *https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim)*

[11] *Hunting for Hidden Threats. Cisco Cybersecurity Series. Cisco Systems. Sept. 2019.* *https://www.cisco.com/c/dam/global/en_uk/products/collateral/cybersecurity-series-2019-threat-hunting.pdf*

[12] *Title 18 of the U.S. Code, Section 1030, Fraud and related activity in connection with computers.* *https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim)*

Escalation

As with independently responding to criminal activity in the physical world, hack backs in cyberspace invite potentially serious escalation when private organizations act against malicious actors. In addition, as the attackers themselves are obscured by their online presence it is often hard to know who exactly an organization is hacking back against. Sufficiently advanced threat actors may feel inclined to respond in kind or to escalate attacks against a victimized organization further, creating additional risk. As ESET, also a Cybersecurity Tech Accord signatory, explained in blog post on We Live Security, "unless your [organization's] defenses are already ironclad, this [hack back] will bring you far more pain than protection. Attackers may have far more inclination and resources to continue escalating the attack if provoked."[13]

It is also important to note that some threat actors are also proxies or acting directly on behalf of a nation-state, and so any attempt to hack back could quickly spiral into an international incident. While private sector actors may have access to technological capabilities that allow them to track and identify attackers in cyberspace, attribution of attacks for these purposes also needs to include the political considerations based on intelligence data that only governments have access to. As a result of these risks, enfranchising the private sector to hack back could likely result in organizations only taking action against weaker and easily-identified attacker groups, while letting the more dangerous and advanced threats persist unchallenged.

Unintended Consequences

One of the biggest dangers of any offensive activity in cyberspace is that it will spread beyond an intended target and harm innocents and third parties. Tasking private companies with hacking back is inviting scenarios where eventually, inevitably, the wrong systems will be targeted in response to a cyber incident and unintended individuals or organizations will be harmed.[14] It is one thing when state actors, backed by sovereignty and generally outside of any real international liability, make such errors. It is quite another when those errors are made by independent organizations, under a Board of Directors and subject to a range of civil and criminal laws. This additional risk exposure is another reason why many companies, even if legally permitted, would choose to not hack back.

A troubling marketplace for hack back services

Another issue with enfranchising hack backs would be the further proliferation of hacking capabilities and their development, exacerbating the very challenges such efforts would be trying to address. Allowing organizations to hire hack back services would create dangerous incentives to grow an already concerning black market of so-called "hackers for hire." The dark web currently facilitates transactions where hackers build and sell offensive services or tools, often without consequence, to individuals and organizations. Permitting hack back would further expand this market. Even if many organizations were seeking such capabilities for responsible use, others would certainly use them for malicious purposes. Without a clear global articulation of permitted actions and understood consequences, hacking back has dangerous implications for a globally interconnected world.

Nonetheless, nation states are largely the drivers behind the growing market for offensive digital technologies to surveil and track individuals, or surreptitiously exfiltrate information. Organizations like the NSO Group, as well as organizations that do the hacking themselves, today offer "espionage as a service" to nation states. Recent reporting from The Citizen Lab at the University of Toronto details how one such hacking for hire organization, Dark Basin, has been targeting advocacy groups, journalists and senior government officials from around the world[15]. These stories demonstrate how such hacking capabilities are always double-edged swords, and while some may use them responsibly, others will surely find nefarious applications. While these activities are not private hack back, these private sector offensive actors illustrate the problem of limiting the space, with money and resources pouring into the marketplace.

[13] *Active Defense: Good protection doesn't need to be offensive. We Live Security. ESET. Nov. 19, 2020. https://www.welivesecurity.com/2013/11/19/active-defense-good-protection-doesnt-need-to-be-offensive/*

[14] *Nojiem, Greg, David Snead. "Hacking Back" a Recipe for Digital Arms Race. Center for Democracy & Technology. May 24, 2017. https://cdt.org/blog/hacking-back-a-recipe-for-digital-arms-race/*

[15] *Anstis, Siena, Ron Deibert, Adam Hulcoop, Bill Marczak, John Scott-Railton, Bahr Abdul Razzak. Dark Basin: Uncovering a Massive Hack-For-Hire Operation. The Citizen Lab, University of Toronto. June 9, 2020. https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/*

V. Final thoughts and recommendations

The Paris Call prohibition on "private hack back" is an important multistakeholder principle for advancing a more stable and secure online world. It reinforces where roles and responsibilities overlap, intersect and diverge, as we all work together – across stakeholder groups – to drive consensus and adherence to a rules-based international order in a domain that we all share. As has been discussed, however, while the principle itself may be simple, its application and implementation to prohibit hacking back require a clear understanding of the law and its implications. Indeed, as with all of the Paris Call principles, stakeholders need to work together to ensure they are not just words on a page but active commitments that advance the security and stability of our shared cyberspace. **To that end, and in the interests of helping advance this discussion further, we hope policymakers will take away from this report the following six considerations:**

1. **Policies broadly permitting/endorsing private hack back are irresponsible**
   Governments should play a lead role in at least coordinating and approving of any actions that would be considered hack backs, and only do so for activity that is meant to enforce laws and hold malicious actors accountable. Any policies that would seek allow private hack back would violate existing laws. For all of the reasons described in section IV – *legality, escalation, unintended consequences, and* – encouraging the private sector broadly to simply hack back on its own is unwise and counterproductive.

2. **Don't limit lawful active defense measures**
   In seeking to prevent irresponsible hack back, government action should ensure they are not preventing the private sector from maintaining essential active defense practices to keep themselves and their customers secure in a manner that is consistent with the law. This might include defining a range of permissible countermeasures based on technical specifications, necessity, proportionality, or temporality. It may also mean defining which practices will require government coordination, notification, or oversight.

3. **Allow room for innovation in security practices**
   While it might be tempting to pursue policy solutions that create broad restrictions on hack back, the truth is that, as with many other concepts in the digital domain, it will likely continue to resist a precise definition. Even more challenging is that laws evolve more slowly than technology. As the threat environment continues to rapidly evolve, so will industry security practices. This innovation cycle will always outpace the methodical process of policymaking and legislating. So instead of attempting to impose sweeping prohibitions, policies and legislative efforts should identify practices that are broadly permissible, as well as which narrow and specific practices are to be prohibited.

4. **Clarify existing law and promote international consistency in cyberspace**
   Successfully combatting threats in cyberspace requires having an appropriate legal infrastructure in place. To this end, governments should work to clarify how existing law applies within their jurisdictions, and develop specific cybercrime laws as necessary. These should include upholding human rights online, including the right to privacy. In addition, governments should continue to engage with one another, in both regional and multilateral forums, to advance consistent and harmonized policies to help promote accountability across borders. Such dialogues could also promote consensus around the types of active defense measures that should be allowed, and address the dangers posed by the growing market of "hackers for hire."

5. **Encourage government to think differently about cyberattack response**
   Law enforcement and government agencies focused on response to cyberattacks work within traditional domains to respond to the issue. Law enforcement identifies suspects, and then brings those individuals to

justice. Agencies focus on patch deployment or system defense. However, to lessen the need for private "hack back", governments need to be willing to work in new ways, recognizing a goal of preventing an attack before it happens, or rewarding law enforcement or agencies for the number of computers protected, so that victims will not feel the need to turn to vigilantes or those willing to work outside the law to remediate an attack. Creativity and coordination will be essential.

6. **Coordinate closely with the private sector**
   Addressing the rising number of cyberattacks each year requires persistent and ongoing coordination between government and the private sector. Indeed, while clear boundaries are important, policy discussions in this area should be much more focused on "how do we work together and what practices do we need to employ?" as opposed to "what security behaviors need to be prohibited?" This is in the spirit of the Paris Call itself, which bringing together a multistakeholder coalition to collaborate in advancing security and stability in cyberspace.

The Cybersecurity Tech Accord and its signatories stand ready to provide further input and guidance as necessary in these important policy discussions, as we work to build a more stable and secure online world for all.

VI. Company case studies: Active defense and coordinated responses with governments

Differentiating between which private sector practices are dangerous and ill-advised "hack backs," which are responsible "active defense" measures, and which are activities conducted with the blessing of law enforcement, is not always easy. Understanding the definitions and boundaries, both legal and technological, presented in this report can be difficult in the abstract. Therefore, it can be helpful to consider what these private sector actions actually look like in practice and how they contribute to the overall security of our online ecosystem. The following case studies provide examples of such forward leaning security practices employed by a range of Cybersecurity Tech Accord signatories to help protect users and customers, none of which would constitute hacking back:

Microsoft

Microsoft – "Necurs" botnet takedown

Botnet takedowns are a good example of the kind of forward-leaning security practice that companies employ – with either legal authorization, in coordination with law enforcement/ governments, or via private cooperation in a jurisdiction – to stop bad actors from co-opting victim computers to cause harm. In March of 2020, Microsoft's Digital Crimes Unit worked in coordination with partners across 35 different countries to take down the infrastructure of the so-called "Necurs" botnet. Up until that point, Necurs had been one of the largest botnets in the world and included over 9 million infected computers that spread dangerous malware and sent millions of fraudulent emails each month.

The coordinated action to dismantle essential portions of the botnet was conducted under the legal authorization of the U.S. District Court for the Eastern District of New York and supported by public-private partnerships around the globe including, inter alia, government CERTs and law enforcement in Mexico, Colombia, Taiwan, India, Japan, France, Spain, Poland and Romania. In addition to supporting dismantling the botnet, Microsoft and other security research firms also played an important role identifying and mapping the activity of the botnet to begin with, flagging it as a pressing issue for government agencies. These types of botnet takedowns save countless people all across the globe from falling victim to criminal activity online.[16]

[16] *Burt, Tom. New action to disrupt world's largest online criminal network. Microsoft On The Issues. Microsoft Corp. March 10, 2020.* https://blogs.microsoft.com/on-the-issues/2020/03/10/necurs-botnet-cyber-crime-disrupt/

ESET – Research leading to coordinated action

In an effort to map the cybersecurity threat landscape, ESET researchers often spend months examining sophisticated malicious campaigns and cutting-edge malware. In some cases, these long-term research cases can lead to collaboration with law enforcement to perform a botnet takedown and sometimes culminate with arrests and the conviction of cybercriminals. These cases are an excellent way to make a long-lasting impact on the cybersecurity ecosystem at least in two ways: taking active cybercriminals off the streets and producing a deterrent effect on their peers.

One such operation was Operation Windigo, based on research we published in 2014 and which led to the arrest and conviction of a Russian citizen for his role in the cybercriminal operation. ESET researchers were able to work closely with the FBI and other international partners to track and ultimately to disrupt Operation Windigo significantly.
At the core of Operation Windigo is Linux/Ebury, an OpenSSH backdoor and credential stealer that was installed on tens of thousands of Linux servers. Using that backdoor, the attackers installed additional malware to perform web traffic redirection, send spam, and steal credentials to expand their network of compromised servers. These malicious activities were impacting millions of internet users globally and generated millions of dollars for the botnet operators.

While this type of operation spans several years — most of the research was carried out in 2013, the resulting arrest was in 2015, and the cybercriminal received his sentence in 2017 — the final outcome justifies the resources and effort of the research team. The ESET researchers continually track all known major botnets and believe firmly that disruptions and takedown operations against them are playing a vital role in keeping internet users safe. ESET also participated with other partners in the disruption operations of the following botnets in recent years: Dorkbot in 2015, Andromeda in 2017, 3ve in 2018 and Trickbot in 2020.

Telefonica – Abuse reporting and lawful actions

Telefonica is a provider of key digital infrastructure in the markets in which it operates. As a large telecommunications company, it is charged with providing connectivity across regions while navigating a complicated threat landscape to protect customer security. While always abiding strictly by the laws of its different markets, Telefonica helps ensure a safer online environment by reporting activities that pose a threat to customers and the broader online ecosystem. This includes the reporting of things like botnet detections among a customer base, spam and phishing activities, and hacking attempts, all of which is executed only by clear open authorizations or by a particular demand from legal authorities.

Meanwhile, the hunting of suspected attackers or taking of direct offensive action against them in cyberspace would be beyond the purview of the telecom service provider, as innocent parties could be unintentionally harmed in the process and the potential for further escalation would make this unwise. To shed further light on the types of lawful actions the company does pursue, Telefonica publishes regular transparency reports on authorities' requests for lawful interception, content blocking or service interruptions that are open to the public to review.

As just one example, during the known worldwide ransomware cyber incident Wannacry (May 2017), Telefonica Global CSIRT successfully early detected and characterised the attack. In addition to protecting all its assets and customers in the countries under its footprint (customers were not impacted), Telefonica proactively and voluntarily shared all its available intelligence with national authorities (i.e. INCIBE and CCN-CERT). This greatly eased their activity for public protection and, as a result, the devices connected to Internet in Spain were the least affected in the OCDE area (Spain 0,61%, France 1,33%, UK 1,86% or US 7,2%. Figures referring all IP aggregation. Source: INCIBE-Spain).

Juniper Networks - Detecting & degrading the capabilities of malware

"Hacking back" is an interesting concept that can be interpreted in multiple ways. When a vendor utilizes existing legal, regulatory, or commercial avenues to degrade an attacker's capability, is that "hacking back"? Consider, for example, the recent efforts by the Juniper Threat Labs at detecting and degrading the capabilities of the Gitpaste-12 malware.

Gitpate-12 attackers used both Github and Pastebin to store code and configs for their malware. Juniper contacted these organizations, informed them of the issue, and both Github and Pastebin had the relevant data removed. This approach by vendor threat hunting teams is commonplace, and effective against a number of threat actors, but isn't something that fits the typical narrative of "hacking back". In popular discourse, "hacking back" typically involves offensive activities against threat actors, perhaps including vulnerability exploits, or deploying malware against threat actors.

In the middle between these approaches is another increasingly common approach, employed by vendor, governmental, and commercial threat-hunting teams. This involves reverse-engineering malware to understand how it communicates with its Command and Control (C2) functionality, and then "hijacking" that communications channel to order the entire botnet to degrade, or even completely dismantle itself. In these cases it's very rare that software vulnerabilities (other than those present in the malware/C2 function themselves) are used. Similarly, it doesn't involve deploying malware against the attackers. But it is effective. Whether or not it qualifies as "hacking back" is in the eye of the beholder.