CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

APRIL 2024

Exploring Law Enforcement Hacking as a Tool Against Transnational Cyber Crime

Gavin Wilde and Emma Landi

Exploring Law Enforcement Hacking as a Tool Against Transnational Cyber Crime

Gavin Wilde and Emma Landi

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Summary

In terms of revenue, 2023 will go down as a record-breaking year for ransomware, with over a billion dollars in payments going to hackers.[1] The U.S. Federal Bureau of Investigation (FBI) reports a record $12.5 billion lost to cyber crime more broadly over the course of that year.[2] As the quantities of affected users and organizations, payoff amounts, critical services, and pilfered sensitive data continue to rise, Western capitals have in recent years come to treat transnational cyber crime as a major national security concern. Because cyber criminals often operate from third countries where prosecution or extradition are unlikely, policymakers often look to military and intelligence services as the best (or only) entities capable of operationally disrupting cyber crime syndicates. Yet another growing trend challenges this notion: Western law enforcement agencies (LEAs) also have been expanding their own abilities to cross both technical and national boundaries to take on cyber criminals. This trend is creating new opportunities and challenges for both domestic and international cyber policy.

This more assertive, but often welcomed, approach poses several challenging policy questions for national security officials. Our research and interviews with current and former LEA officials, industry insiders, and legal experts summarize these questions as follows:

Are LEA-led technical takedowns (such as "hacking the hackers" or "hacking to patch") an effective way to counter cyber crime?

> ***Yes—with caveats.*** Although there is no standard measurement of effectiveness for these disruptive operations, they can impede cyber crime collectives, at least temporarily. Some groups might reconstitute their digital infrastructure relatively quickly and cheaply, but the downtime likely spares many more potential victims from attacks. Particularly for the

most vulnerable sectors and organizations, in which cybersecurity is chronically under-resourced, more frequent technical takedowns with longer reconstitution times for cyber criminals may help significantly.

To prolong this downtime and make recovery more expensive and costly, governments, tech companies, and civil society groups must make sustained, complementary efforts across geographic boundaries. Such endeavors may also require civil legal measures, such as injunctions and restraining orders, against third-party digital service providers. The increasing frequency of Western LEA collaborative takedowns lays the necessary foundation for this work.

Ultimately, Western capitals face intense political pressure to *do something* about rising cyber crime, using every tool at their disposal. State agencies and other entities with the authority and capacity to do so are incentivized to answer that demand. The key is to maximize the benefits and minimize the drawbacks of their efforts.

Does it really matter who conducts them?

Yes. Militaries and intelligence services are often best equipped and most agile in cyberspace, but in several areas LEA-led cyber operations may be most impactful and more appropriate. For example, LEAs can investigate domestic victimization and digital forensics in ways that foreign-focused services cannot. These circumstances posture LEAs to mitigate the impacts of cyber crime as well as threats from major nation-states. (For instance, see the Hafnium and Volt Typhoon technical takedowns in the appendix.)

Meanwhile, threats from financially motivated or nonstate cyber actors may (rightfully) fall below the priority threshold of militaries. Moreover, pitting the armed forces against civilian-led, nonstate, transnational adversary groups abroad could foster a precedent in cyberspace that would fuel more aggression among states than it ultimately curbs. LEA-led technical takedowns typically are more transparent and publicly accountable than classified operations carried out under military or covert-action authorities. Where LEA operations might have impacts abroad, they also are likely to be less provocative. For the most acute threats to national security, criminal investigative authorities may have the greatest effect by working in concert with others.

Like-minded democracies therefore should better resource and equip their LEAs to conduct technical takedowns. They can do so by developing criteria to simplify and standardize consent for and participation in these operations, whether home or abroad. This prospective approach does not rule out contributions from or collaboration with other state agencies or military entities. Rather, it postures LEAs to harmonize efforts to kick specific types of illicit actors off their home turf and keep them off it.

That said, LEA-led technical takedowns pose issues of their own. Critics raise valid concerns about risks to civil liberties and privacy, as well as potential judicial overreach.

Development and use of malware by LEAs risks unforeseeable consequences, like the potential to fuel malware proliferation. Meanwhile, international law enforcement cooperation typically is impossible with adversaries and cumbersome even with allies. Potential partner capabilities and host-nation consent to conduct takedowns on their territory are far from guaranteed. These areas warrant additional legislative attention to both enable LEA cyber operations and place them within appropriate bounds.

What role can the private sector play?

Potentially a major one—with equally major challenges. Tech companies often are best positioned to detect cyber threats and anomalies. They routinely issue software patches to preempt illicit cyber activity, and some even resort to civil litigation to disarm it. Commercial actors are also credible voices in internet governance bodies like the Internet Corporation for Assigned Names and Numbers (ICANN) and other nongovernmental, multistakeholder groups. These traits make them natural, even indispensable, partners for Western LEAs.

Yet these companies have limits to what they are able or willing to do. Their users often are slow to patch known vulnerabilities, if they even opt to do so. Their legal advisers are wary of incurring liability for any damage caused by hastily deployed, faulty patches (or by LEA-deployed malware). Few but the largest players have the resources to dedicate to disrupting criminal infrastructure on a sustained basis. Their foremost concern, understandably, is the security of their users and their brand reputation—however much they support efforts to strengthen cybersecurity more broadly. Most companies are uncertain as to whether or how LEAs ultimately use any tips they might provide and are reticent to entangle themselves in any subsequent public criminal proceedings. These dynamics disincentivize more fulsome collaboration to prioritize or harmonize joint efforts against cyber criminals.

Meanwhile, civil society groups (such as the Shadowserver Foundation, the Institute for Security and Technology, and the Global Cyber Alliance) provide convening power, capability development, and vulnerability monitoring that can help prioritize and drive public awareness to both inform and complement LEA takedowns.[3] Interviewees for this project asserted that these efforts should help LEAs prioritize investments of action, particularly for current or prospective victims of cyber crime that are least likely to survive or reconstitute after a ransomware attack or data breach.

Ultimately, the growing trend of Western LEA-led technical takedowns is a positive development that warrants additional research and policy consideration. New legal frameworks, collaboration mechanisms, and diplomatic efforts are needed to scope, guide, and resource such takedowns to maximize their effect. Drawing upon a range of legal and policy analysis, as well as expert interviews with stakeholders (detailed below), this paper aims to lay conceptual groundwork for these updates.

Introduction

Armed with a raft of new authorities and procedures, Western LEAs have increasingly been "hacking the hackers" wherever they are—degrading, destroying, or denying them access to the very devices and software they use for illicit operations. Some have even resorted to an approach dubbed "hack-to-patch": preemptively removing criminals' malware from their victims' devices, often without the latter's prior awareness. These two types of operations broadly can be referred to as "technical takedowns." Even though the apprehension and prosecution of cyber criminals may be the ultimate (if rarely achievable) goal, the recent uptick in Western LEA-led technical takedowns suggests a shift in strategy. Proactive and preventive digital disruption appears to have become their primary objective.

This paper first explores the cyber crime threat and potential ways to measure the success of technical takedowns. It then examines the evolution of the practice among U.S. and allied LEAs, noting an upward trend in collaboration. From there, it addresses the need to move beyond a military-centric approach to countering transnational cyber crime, arguing for more parity in resourcing for LEAs. It also looks at the necessity of working with commercial and private partners and the hurdles to more robust cooperation. To conclude, it poses the major policy questions that can guide and enhance the benefits of more assertive LEAs in cyberspace.

This paper draws on extensive research of academic literature, publicly available records, and accounts of major Western LEA-led technical takedowns. It also incorporates reflections from in-person and virtual interviews conducted from autumn 2023 through spring 2024 with dozens of current and former Western LEA and government officials, legal scholars, cybersecurity practitioners, and civil society researchers in relevant fields.

Quantifying the Threat, Qualifying the Countermeasure

Over the past decade, cyber criminals have demonstrated hacking capabilities upon which military and intelligence services used to have a monopoly. Some have strong allegiances to the states in which they operate; others have no such loyalties. These collectives do not train their fire on adversary governments and their militaries. Instead, they target everyday citizens, commercial enterprises, local municipalities, healthcare systems, and critical infrastructure operators. Like organized crime syndicates in previous eras, the cyber crime ecosystem is driven primarily by greed and financial motives.

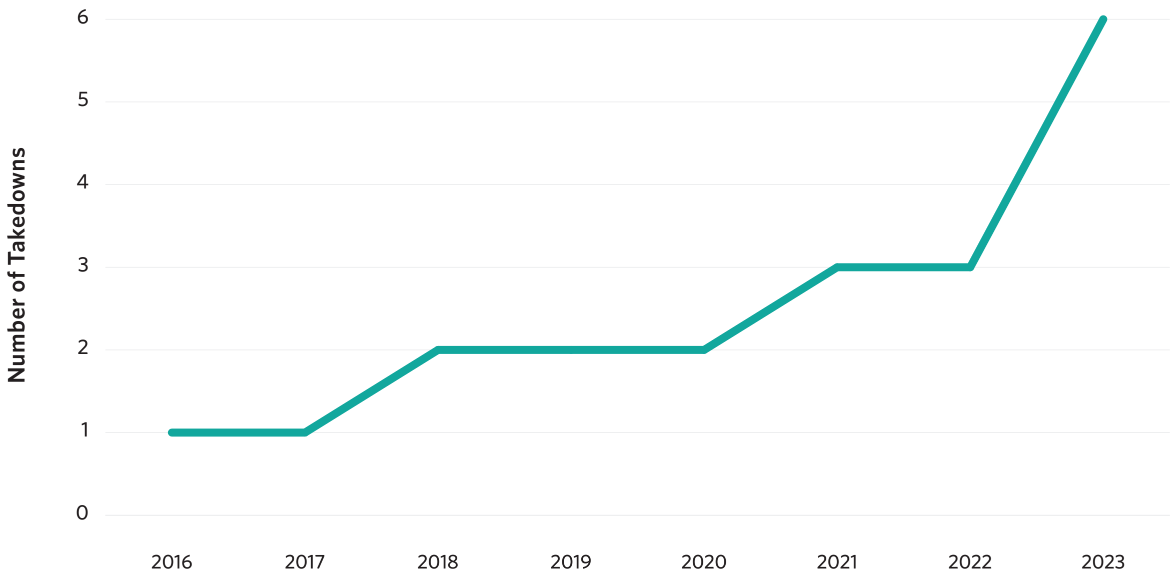
In the digital era, however, cyber criminals can operate in relative anonymity, at a safe distance from their victims' national LEAs. Their use of technical cut-outs and financial go-betweens make it extremely difficult to identify and track them, much less apprehend or prosecute them. Even when Western LEAs like the FBI or the United Kingdom's National Crime Agency can identify and locate cyber criminals, they lack the jurisdiction to simply swoop into another country to apprehend suspects and bring them to justice. Moreover, even where bilateral law-enforcement cooperation agreements (called mutual legal assistance treaties, or MLATs) exist, arrest and extradition from abroad is far from guaranteed and usually is fraught with investigative uncertainties and bureaucratic delays spanning months, if not years.[4] Interviewees also noted that MLATs perhaps are necessary but are far from sufficient to foster trust and interstate collaboration among LEAs. There simply is no criminal justice system with sufficient global reach to deter or punish bad actors from conducting illicit cross-border activity in cyberspace.

These circumstances have prompted a host of voluntary government- and civil society–led efforts to counter ransomware and cyber crime.[5] Western militaries also have come to view cyber crime as a threat to national security against which they have a duty to defend, including through the use of offensive cyber operations.[6] For example, in advance of the 2020 U.S. presidential election, United States Cyber Command reportedly hacked and disrupted a global network of infected devices—known as "bots" within a network, or "botnet"—used for malicious purposes like ransomware.[7] This operation came on the heels of a move from former president Donald Trump's administration to relax procedural constraints around the Pentagon's cyber operations abroad.[8] The shift had implications not only for cyber operations in armed conflict but also for cyber crime.[9] Western LEAs, criminal justice, and civil legal systems likewise were ramping up to address the threat, including through more frequent takedowns of their own (see figure 1).

The question of whether technical takedowns work to mitigate illicit activity in cyberspace is not an easy one to answer. There is no universal standard for characterizing the threat of cyber crime nor for measuring the effectiveness of countermeasures. Is it person-hours wasted in downtime or dollar-value of losses? The number of victimizations prevented? The number of otherwise prosecutable cyber crimes committed? Notably, several prominent cyber crime syndicates and botnets have reconstituted their infrastructure shortly after prominent state-led takedowns.[10]

Even so, legal scholar Jack Goldsmith offers a real-world perspective, asserting that "we do not conclude from the persistence of occasional bank robberies that laws against theft are ineffective, or even suboptimal. Often, the law accepts small evasions because achieving perfect legal control, though possible, is just too expensive."[11] Whether introducing technical friction into their operations, tarnishing their reputation among would-be global clientele, or sowing distrust within their ranks, Western LEAs have at least some notional rationale for hacking cyber crime syndicates.[12] European participants in the Emotet takedown

Figure 1. Western LEA-Led Takedowns, 2016–2023



Source: Author's research of public records and press coverage regarding major technical operations against cyber crime infrastructure by Western LEAs.

(see appendix) also asserted in interviews that they expected reconstitution in a matter of months. When the group took almost a year to reconstitute, participants noted, "we considered that success."

As some interviewees for this project also noted, even the very exercise of an LEA-led takedown can *itself* be valuable. It establishes precedent, institutional muscle-memory, trust, and interoperability among domestic and international stakeholders. In this way, it is not dissimilar to U.S. and UK military notions of "persistent engagement" and "cognitive effects," which prioritize constant, proactive efforts to disrupt and disorient adversaries in cyberspace.[13]

They also noted that for many prospective victims, enhanced cyber hygiene, updated software and hardware, and systems-patching remain out of reach—less out of a lack of awareness or political will and more because of a chronic lack of funding and know-how.[14] Such organizations live below what cybersecurity expert Wendy Nather calls the "cyber poverty line."[15] Small businesses, municipal utilities, healthcare facilities, and schools have thus become frequent targets of opportunity for cyber criminals. More frequent takedowns are therefore a necessary tool in the short term, while longer-term policies aim to shift "responsibility for managing cyber risk on to those who are most able to bear it."[16]

But any discussion of efficacy must also grapple with major questions posed by more frequent takedowns, for instance, intelligence gain/loss considerations: What kinds of insights are put at risk by either disrupting some infrastructure or alerting cyber criminals to their exposure to authorities? Moreover, do government agencies risk creating a moral hazard for their publics, disincentivizing more proactive cyber hygiene and systems-patching? Do they drive cyber criminals even deeper underground, prompting them to use even more anonymizing techniques? Do they divert cyber criminals' focus toward lesser-developed countries with weaker defenses and limited capacity to strike back? By developing or purchasing malware for use in takedowns, do LEAs further fuel the underground market for software vulnerabilities?[17] Such difficult questions are a reminder that technical takedowns cannot be untethered from broader cyber strategies and dialogs.

Meanwhile, states seem to broadly agree that extraterritorial cyber intrusions can be a violation of their sovereignty—but they also agree that often there are valid justifications for doing so.[18] As extraterritorial cyber operations become more routine, they can gradually evolve into "customary international law." In other words, silence is acceptance, and acceptance eventually can become codified as the norm.[19] Such international norms are widely interpreted and disputed, particularly when they involve non- or quasi-state actors like cyber criminals. This ambiguity clouds discussions about whether technical takedowns of cyber crime infrastructure abroad are advisable, under what authority they might be conducted, or who is accountable for any unintended consequences.[20]

U.S. and Western LEAs Getting More Assertive

Although the increased assertiveness of militaries in cyberspace has occupied much of the public and policy discussion over the past several years, the role of LEAs has gone relatively underexamined. (See appendix for details.)

As one of the largest global targets of cyber crime, as well as one of the largest points-of-origin for cyber crime, the United States' experience provides a useful backdrop for consideration.[21] As in the case of any crime that crosses state lines or international borders, federal law enforcement—most prominently the FBI, but also the U.S. Secret Service when the financial sector is involved—has the lead. As with any crime, a set of procedures guides investigations. The U.S. Constitution, meanwhile, safeguards citizens against "unreasonable search and seizure" by LEAs, without a probable cause. These protections mean that investigators must present a judge with some rationale to obtain a warrant to, for instance, search a person's house or seize their vehicle—irrespective of whether that person is the suspect or merely happens to own the property where a crime was committed.

That said, one of the biggest legal challenges in cyberspace is establishing where the crime took place. For instance, ransomware actors might infect victim devices (such as computers, phones, or servers) spanning across state lines, using networks of devices (such as computers, servers, or routers) or websites located and hosted in several different countries.[22] Often, neither the victimized nor the offending devices can be comprehensively catalogued or identified. Victims often are unaware their devices have been targeted or commandeered for illicit purposes. Cyber criminals often lease devices from third-party vendors and use anonymizing tools to conceal their geographic footprint.

For the FBI, the difficulty of knowing which people are committing crimes using which devices from which places used to pose a conundrum. For instance, under past U.S. investigative procedures, judges could only grant a warrant for search and seizure of devices located within their own jurisdiction, with very few exceptions. This limitation severely hindered investigation of cross-border, broad-based cyber crime, as "the government struggled to remotely search anonymized criminals, and faced high litigation costs arising from the requirement to sue in multiple districts."[23]

In 2015, a prominent episode illustrated these difficulties, when the FBI attempted to investigate a global online pornography ring exploiting minors. Armed with a warrant, the bureau seized the North Carolina–based server that hosted the offending website, quietly commandeered it for two weeks, and deployed specialized malware onto the devices of the more than 1,300 users that accessed it during that period. This so-called Network Investigative Technique (NIT) allowed the FBI to identify many global suspects and subsequently to apprehend several of them domestically.[24] However, some of the suspects later successfully contested the resulting charges, arguing that the original search warrant was not valid for devices located beyond the district where the warrant was issued.[25]

This fundamental mismatch between digital-era criminality and analog-era investigative guidelines came to a head in late 2016, when the U.S. Department of Justice (DOJ) successfully lobbied the Supreme Court's Advisory Committee to update the Rules of Criminal Procedure.[26] Under the newly revised Rule 41, U.S. LEAs are now able to obtain a single warrant for remote searches and seizures—to include NITs—on any number of devices, so long as the cyber crime in question fits at least one of two criteria:[27]

- The offending devices' locations (IP addresses) are obscured through technical means—to include virtual private networks (VPNs), peer-to-peer (P2P) networks, anonymizing browsers like Tor, proxy servers, or encryption.[28]

- Or, the victims are spread across five or more judicial districts throughout the United States.

Over the ensuing years, the FBI increasingly has relied on the updated Rule 41 to conduct technical takedowns against a number of botnets and other infrastructure used by cyber criminals, ransomware operators, and foreign intelligence services (see the appendix for details). Such cases include LEAs seizing control of one or more domain names used by a botnet and redirecting web traffic to a new LEA-controlled device, enabling them to observe and record online traffic—including IP addresses. This approach helps LEAs to determine the size and geographic layout of a botnet, to identify and notify victims, to send infected devices specially developed malware to cripple the botnet itself, or even to repair infected devices on victims' behalf without their foreknowledge.[29] (Legal scholars have noted the distinction between the Rules of Criminal Procedure and the law, however, adding that such operations may not survive future legal challenges absent legislative backing.)[30]

The United States was not alone in this effort. It conducted many of these takedowns in conjunction with international partners, who also had updated their policy frameworks to enhance LEA capabilities against cyber crime. For example:

- In 2016, the United Kingdom passed the Investigatory Powers Act, expanding LEAs' ability to carry out "equipment interference" operations "for the prevention and detection of serious crime and emergencies."[31]

- Also in 2016, France amended its criminal code to authorize LEAs to remotely access and manipulate computers and other devices suspected in the conduct of serious and organized crime and terrorism (including a reference to cyber crime).[32]

- In 2017, the German parliament expanded the types of crime for which LEAs can perform NITs to include computer fraud and the handling of stolen goods.[33] The authority was again expanded in 2021.[34]

- In 2019, the Netherlands' Computer Crime Act III went into effect, adding hacking as an investigative method to the country's criminal code, "in order to determine certain aspects of the computer or user, intercept confidential communications, conduct systematic observation, secure stored and future data, and render data inaccessible."[35]

- Also in 2019, the European Union (EU) adopted an EU Law Enforcement Emergency Response Protocol, granting Europol's European Cybercrime Centre (EC3) the central coordinating role for member-state LEAs responding to cross-border cyber attacks.[36]

- In 2020, Australia's Identify and Disrupt Bill lent its LEAs new powers for dealing with online crime, including technical surveillance, disruption, and takeover of suspect devices.[37]

Analysts have observed that these investigative updates might effectively enable LEAs to treat offending devices of unknown geographic location as domestic, lending their takedown operations a potentially unlimited global reach.[38] As one legal scholar noted, "the reason is simple: without knowing the target location before the fact, there is no way to provide notice (or obtain consent from) a host country until after its sovereignty has been encroached."[39] Although legal interpretations are likely to vary as to whether and how LEA NITs might constitute such an encroachment, questions remain about the degree to which democratic states are prepared to tolerate foreign LEAs—even friendly ones—conducting technical takedowns on home soil.[40] As one LEA interviewee noted, "Both the U.S. and foreign governments will have to move toward a place where they can move quickly, even when systems are outside their jurisdiction." Commonly agreed criteria would help Western LEAs to do so.

Beyond a Military-Centric Framework

For most states, the actors most capable of sophisticated, widescale hacking operations are military and intelligence services. These organizations typically enjoy substantial bureaucratic heft within governments, drawing the preponderance of financial and human resources dedicated to cyber operations.[41] They generally have grown more flexible in conducting them and command public credibility when addressing cyber threats more broadly.[42] But because of their association with warfighting, espionage, and subversion, a set of circumstances in which these services are the first responders to cyber criminality by quasi- and non-state actors—especially when the crimes involve primarily financial losses or violations of the aggrieved nation's own criminal statutes—could provoke more cross-border cyber attacks than it ultimately prevents over the long term.[43]

These services may be best outfitted and resourced for cyber operations. They may have a longer and richer history of theory and strategy to guide these operations. They often are able to move more quickly than criminal or civil legal systems can. However, these factors are unsatisfactory answers to the core question of whether warfighting authorities are *appropriate* and *proportional* to cyber crime threats.[44] As the so-called War on Drugs and Global War on Terror both have demonstrated, military capacity is no panacea against transnational, non-state-centric threats. Its overextension threatens to "erode the civil-military balance that is imperative for any democratic society" and to disincentivize needed reforms and resourcing for LEAs to achieve similar capacity in cyberspace.[45]

For instance, military-led hacking operations against targets located on the territory of a third state entail many considerations, including the legality of targeting noncombatants under international law, the possibility of escalating tensions or damaging diplomatic efforts, and the implications of setting a broader precedent for how states conduct themselves in cyberspace.[46] These operations also are conducted in the service of an expansive national security portfolio—from preventing (or prevailing in) armed conflict to defending the homeland. They are uniquely tasked with obtaining the otherwise unobtainable: the plans, intentions, tactics, tradecraft, and procedures of foreign state and nonstate adversaries.[47] The extent to which transnational crime should be part of that remit—or would be symptomatic of a militarized "mission creep"—is a subject of some debate.[48]

Rather than relegating their traditional purview over criminal matters to militaries, the recent spate of LEA technical takedowns suggests the need to consider (and equip) LEAs to be coequals in the cyber domain. LEAs are chartered to operate domestically, are able to formally compel third parties to produce insights and evidence for them, and can collect and use information about domestic victims of cyber crime in ways militaries cannot.[49] In some circumstances, LEAs can work undercover, offer rewards for information, and leverage networks of confidential informants from within cyber crime syndicates—or grant them the ability to conduct otherwise illegal activity—in the service of a broader investigation.[50] Democratic norms and civil liberties largely preclude turning such secretive and sophisticated military and intelligence capabilities against domestic publics, including surveilling, hacking, or disrupting technological infrastructure located in (or under the jurisdiction of) home turf. For instance, the FBI used a hack-to-patch approach to protect vulnerable U.S.-based devices against the Volt Typhoon malware, pointing to long-running Chinese efforts to pre-position malware in critical infrastructure in the event of armed conflict (see appendix).[51]

LEAs are subject to a relatively greater degree of immediate transparency and accountability in their hacking operations. Done properly, these activities require advance judicial oversight, must adhere to formal rules of criminal procedure, and must acquit their actions publicly as part of the government's prosecution of cyber criminals. Military and intelligence operations of any stripe, by contrast, are shrouded in secrecy, making transparency, accountability, and assessment of efficacy difficult.[52] Military and intelligence leaders are likely to be wary of this tradecraft later becoming entangled in public criminal prosecutions, in which the defense generally can scrutinize how the government obtained evidence of the alleged crime (the process known as "discovery").[53]

A more LEA-centric approach is not without its own limitations and problems. Interviewees for this project raised philosophical questions about the degree to which criminal justice systems—which are designed and incentivized to build toward ultimate prosecution—can, in the absence of a defendant, make preventive disruption a new goal.[54] Some interviewees noted, meanwhile, that several European countries actually codified this shift in emphasis, particularly during the early 2000s when counterterrorism was top of many governments' focus and a "duty to protect" prevailed.

Drawing on the same counterterrorism parallels, some civil society organizations and legal scholars have warned that enhanced LEA authorities in cyberspace pose risks to civil liberties and open the door to potential LEA and judicial overreach.[55] Others acknowledge the need for government operations to remove malware from affected devices but argue that conducting them under traditional investigative authorities "stretch[es] the concept of criminal warrants beyond recognition."[56] Meanwhile, transparency around LEA NITs is typically an after-the-fact proposition, which may not entail prior notice to affected users or intermediaries. Further, NITs may not be subject to any advance third-party validation. Moreover, in the event that an NIT unintentionally disrupts legitimate activity on a network or a device, it is unclear whether or how governments might be held liable for any unforeseen damages.[57]

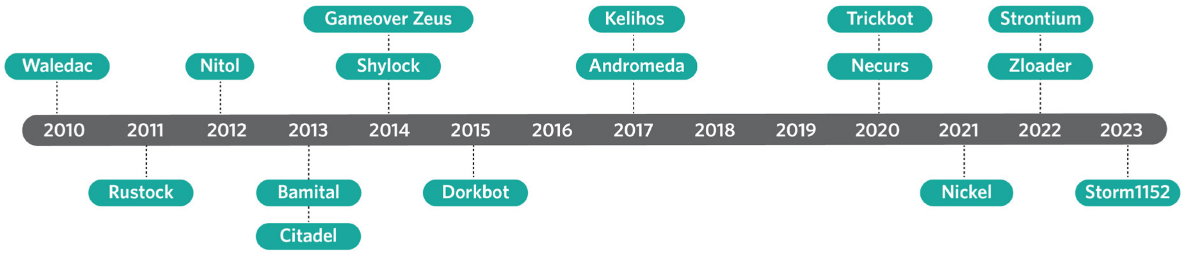
Even where LEAs may have the authority to conduct hacking operations, there are no clear guidelines about the conditions that might call for them. For instance, DOJ guidelines note that warrants should not be used when some "other less intrusive alternative means" exist, unless it is immediately "necessary to prevent injury to persons or property"—a clause subject to wide interpretation.[58] In this regard, while judicial oversight is a definite advantage to LEA-led takedowns, additional executive branch guidance and legislative oversight are also necessary to scope and bound them.

When it comes to disrupting the technical infrastructure used by cyber criminals, there is no one-size-fits-all approach. In fact, a mixture of whole-of-government and public-private collaboration is likely to prove most effective at addressing cyber crime holistically. In the United States and other democracies, distinct authorities typically codify how government entities conduct hacking, whether for warfighting, covert activities such as intelligence-gathering, and criminal investigations.[59] These authorities are not mutually exclusive and can even be complementary. High-level leadership likely will be necessary to harmonize and orchestrate their exercise—including in concert toward a given end-state, such as a global botnet takedown with allies and partners or initiatives to bolster specific, highly vulnerable sectors.[60] (The U.S. National Cyber Director is an example of an entity capable of providing such leadership.)[61] As a more robust LEA role appears both necessary and inevitable, more robust domestic and international policy frameworks will be needed.

Barriers to Private Sector Leadership

What role does the private sector play? Most nongovernmental entities are prohibited by law from hacking as the term generally is defined.[62] However, major multinational tech companies and service providers like Microsoft are uniquely positioned to detect and disrupt coordinated, illicit digital activity using some mixture of their own networks or services and legal remedies. Major market players have themselves been more assertively pursuing technical takedowns through civil litigation, on the basis that illicit activity infringes upon their intellectual property rights and damages their global brands (see figure 2).[63] When successful, a court order can be used to disable malicious devices' IP addresses, render the content stored on botnet command-and-control servers inaccessible, seize websites, or compel internet service providers to suspend all services to botnet operators.[64] This approach largely mirrors that first taken by the DOJ in 2011, when it relied on a civil injunction (rather than criminal investigative authorities) to seize twenty-nine domains used to control the "Coreflood" botnet.[65]

Figure 2: Technical Takedowns Stemming From Microsoft Civil Injunctions



Source: Author's compilation from public records and press coverage of major takedowns resulting from court orders secured by Microsoft in civil legal proceedings.

In this light, what is preventing the private sector from leading the way on technical takedowns of cyber criminal infrastructure? Would commercial collaboration not have a scale and scope likely to surpass that which states can muster, with potentially longer-lasting impacts, across a broader geographic footprint? Why would companies not simply notify their customers of any danger, rushing critical software patches for any detected vulnerabilities?

In theory, these suppositions are true. However, a private-sector-led approach would depend largely on the voluntarism of profit-motivated enterprises and on the timely response of customers—neither of which are guaranteed. A major portion of cyber crime exploits software vulnerabilities that are well-known to the public but remain unpatched by broad swaths of users.[66] For instance, the German government recently flagged over 17,000 unpatched Microsoft Exchange servers—which observers called a "ticking time bomb"—urging users (and Microsoft itself) to take immediate action.[67] Several interviewees for this project referenced this shortfall as a major rationale for why LEAs might use NITs to go the last mile to prevent catastrophic, widescale cyber attacks, particularly those with national security implications.[68] Few but the largest firms have the resources to routinely seek out, much less unilaterally disrupt, botnets or other criminal technical infrastructure. Some experts also question the degree to which civil courts and tort law reasonably can be expected to grapple with the potential technological and international ramifications of commercial takedowns.[69] Meanwhile, many consumer-grade, networked devices are not routinely or automatically patched by suppliers, who often ship them with default security settings applied. These are typically opaque to end users and easily circumvented by illicit actors. In short, some of the demand for LEA-led technical takedowns could be mitigated (or complemented) by more regulatory pressure on suppliers to shift to a secure-by-design approach to product development.[70]

Civil takedown operations also entail significant liability considerations—perhaps one of the biggest disincentives to companies conducting them unilaterally.[71] The ability to obtain such judicial relief varies across nations, so enforcement beyond national borders can be disputed.

It is also unclear how frequently, or under what auspices, private-sector-led takedown operations might be coordinated in advance with other stakeholders. As is the case with military and intelligence services, few private companies are eager to introduce their internal business practices into public criminal or civil proceedings. Proprietary and privacy constraints also can preclude sharing victimology with each other or with government agencies. As one tech company senior official informed the authors, "Businesses focus on profitability—they can't become full-time LEAs." Most commercial representatives interviewed for this project also portrayed LEAs as a "black box" into which they were happy to provide tips and leads, on which they seldom received feedback, however..

Ultimately, commercial partners, civil society groups, and noncriminal legal remedies can be valuable counterparts to LEA technical takedowns. Particularly as cyber criminal groups are likely to reconstitute, private sector partners will be critical to monitor and sustain impacts of LEA technical takedowns over time. However, additional policy attention will be necessary to incentivize their good-faith cooperation, address their liability concerns, and enhance the degree of trust toward LEAs.

Conclusion

Cyber crime and ransomware present major hurdles for Western governments, several of which in recent years have made creative strides in their methodologies to disrupt bad actors. Cyberspace may be borderless, but among Western democracies the authority and technical capability to hack cyber criminal infrastructure largely still pivots on borders. Cyber crime straddles the divide between foreign and domestic policy, seldom fits neatly on the spectrum of interstate conflict, and thus is difficult to prioritize among government agencies. Military and intelligence services generally are not chartered for domestic activity but have the preponderance of hacking capability. LEAs have no enforceable jurisdiction abroad but are gaining in skill and capacity—and are normatively preferable to take the lead. Their assertiveness against international cyber crime is a positive trend, presenting opportunities to navigate bureaucratic and geographic hurdles in responsible, effective, and collaborative ways. Yet doing so will require grappling with major questions about how and when LEA hacking is appropriate—including as part of broader national and international strategies to counter cyber crime. For example:

- What are the benchmarks for success? What resources, investments, and institutional changes need to be made to enhance it?

- What is the threshold of threat necessary for LEAs to pursue a technical takedown? Which victims should receive priority focus?

- Under what circumstances should criminal investigative authorities have the lead over, be harmonized with, or play an auxiliary role to other authorities—including military, intelligence, or civil and judicial ones?

- What are the implications and prospects for global cyber norms, multilateral treaties, regional partnerships, and international law?

- What legal challenges are LEAs likely to face in more aggressively pursuing technical takedowns?

- What principles should guide democratic states' LEA-led takedowns that cross national boundaries into friendly, adversary, or unknown spaces? What might a framework for "mutual reciprocity" among friendly states and their LEAs look like? What legal and regulatory updates would be necessary among participating states?

- What are the implications for privacy and civil liberties? How can LEAs enhance trust, confidence, and transparency?

- What are the best deconfliction, collaboration, and validation mechanisms among stakeholders?

- How might the private sector be better incentivized to assist LEAs in technical takedowns? Is there a reasonable degree of indemnity from liability for commercial actors that take a more proactive approach?

Additional research and policy consideration will be necessary to guide, enhance, and properly bound the practice of LEA-led, cross-border technical takedowns, as well as to assess their efficacy. New legal frameworks, coordination mechanisms, international agreements, legislative updates, and diplomatic efforts also are likely needed to harness their full potential.

Appendix: Major Western Law-Enforcement-Led Technical Takedowns

The following cases are illustrative of Western law enforcement agencies' (LEAs') more assertive approach to disrupting cyber criminal technical infrastructure. They underscore many of the new prospects and potential pitfalls posed by these tactics.

Coreflood (2011)

Coreflood was one of the earliest cases of a court-authorized LEA takedown.[72] For several years, criminals had used the Coreflood botnet to install key-logging software that harvested victims' financial information and credentials. By 2010, the botnet had infected more than 2 million computers. The U.S. Department of Justice (DOJ) obtained search warrants for the command-and-control servers in five states, a seizure warrant was issued for twenty-nine domain names in Connecticut, and a civil complaint was filed against thirteen "John Doe" defendants (the stand-in name used for unidentified suspects).[73] LEA officials worked with internet service providers around the country to notify victims who had infected devices.

The DOJ obtained a temporary restraining order from a federal judge to seize control of the command-and-control servers of the botnet, redirect web traffic to DOJ-controlled servers, and send commands to infected computers to disable the malware running on them. The DOJ affirmed in its civil filing that the command sent to victim computers would not harm the computer itself nor provide the government any access to data stored on it (claims received with some skepticism by digital privacy activists). This intervention was a novelty:

the DOJ filing said that "these actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States and reflect [the department's] commitment to being creative and proactive in making the Internet more secure."[74]

Emotet (2021)

A transatlantic coalition of LEAs announced a successful operation by the United States, Canada, France, Germany, the Netherlands, and the United Kingdom to take down the Emotet botnet, which had targeted banking, e-commerce, healthcare, and government sectors by infecting devices through email phishing. Europol had labeled Emotet the "world's most dangerous malware" and "one of most significant botnets of the past decade."[75] Once Emotet infected a device, it could be marketed as a toehold for other cyber criminals to install other forms of malware or steal financial credentials.

The DOJ announced it had used its "unique legal authorities" and "worldwide partnerships" to target and disrupt the botnet.[76] Foreign LEAs, in coordination with the U.S. Federal Bureau of Investigation (FBI), were able to gain lawful access to Emotet servers located abroad in their respective jurisdictions to identify the IP addresses of victim devices infected with the Emotet malware. Authorities then replaced the malware with an LEA-created file that both interrupted communications between victim computers and the botnet and prevented additional malware from being installed. Warrants in the United States granted under Rule 41 allowed LEAs to install this law enforcement file onto victim computers located in the United States. The DOJ once again affirmed that the file would neither collect nor modify any data stored on devices beyond the scope of the operation.

The coalition of LEAs was able to take over Emotet's command-and-control infrastructure and arrest multiple members of the criminal organization behind it. Owing to the size of the botnet and the amount of coordination and collaboration generated among foreign LEAs, the operation was a significant use of Rule 41 in the United States. Not only the United States, but also other countries, including the Netherlands and the United Kingdom, demonstrated LEA hacking capabilities. Emotet became the prime example of a "hack-to-patch" or "hacking the hackers" operation.

Hafnium (2021)

A Chinese hacking group targeted Microsoft Exchange servers using zero-day exploits to install web shells on the servers. Microsoft had released updates patching the vulnerabilities, but numerous devices throughout the United States remained unsecure. The FBI sought a search-and-seizure warrant for the victim computers owing to the national security and public safety risks associated with the botnet. Subsequently, LEA staff were able to gain lawful access to the devices and remove the web shells. Before the web shells were removed, a third-party expert assessed the methodology of the operation to ensure that legitimate functions would not be affected. Device owners were notified of the action once the operation concluded.[77] One legal expert drew a real-world comparison: "If the FBI knows that an organized criminal syndicate has planted bombs on private property across multiple states, and those bombs are armed and could go off at any time, the FBI is going to take swift action to find and neutralize those devices—especially if it's difficult for property owners to detect them."[78]

Cyclops Blink (2022)

The FBI conducted an operation to dismantle a botnet called Cyclops Blink, which was linked to the Russian military intelligence agency commonly known as the GRU, by gaining lawful access to victim computers and remotely deleting the malware.[79] Under a Rule 41 warrant, the FBI retrieved data about the malware's configuration from infected devices, subsequently removing the malware and blocking remote access to the devices' administrative controls until victims reconstituted them.[80]

Observers remarked that this operation was the most sweeping use of the 2016 amendment to Rule 41 and an example of "federal prosecutors using it not just to investigate criminal activity but to disrupt it."[81] It prompted a debate over how much access to hacking tools is reasonable and responsible for LEAs and whether it is wise to permit law enforcement hacking in cases where cyber crime is disrupted but no formal prosecution is pursued or expected.

Qakbot (2023)

The DOJ announced a successful multinational cyber operation to disrupt the Qakbot botnet, which had infected more than 700,000 computers worldwide, and had been used to steal more than $8 million in illicit profits.[82] The FBI worked with European law enforcement partners to disrupt the malware by gaining access to victim computers and redirecting the botnet traffic to LEA-controlled servers. The servers then sent a command instructing infected computers to download a file that uninstalled the malware, effectively disconnecting the victim computer from the botnet. However, within a matter of months, the malware began to reappear, raising questions about the ultimate efficacy of LEA technical takedowns.[83]

AlphV/Blackcat (2023)

Alongside several European and Australian LEAs, the FBI in late 2023 "once again hacked the hackers," according to U.S. Deputy Attorney General Lisa O. Monaco.[84] In addition to seizing the darknet websites used by the ransomware collective, the FBI developed and released a decryption tool to more than 500 global victims, reportedly sparing them a combined total of nearly $70 million in outstanding ransom demands. The AlphV/Blackcat group already had targeted more than 1,000 known networks and devices across public and private sectors—most of which were located in the United States—extracting nearly $300 million in ransom payments.[85]

Although the takedown disabled AlphV/Blackcat's infrastructure temporarily, the ransomware gang bounced back two months later by incapacitating the healthcare firm Change Healthcare. Reporting on the issue suggests that Change Healthcare may have paid $22 million in ransom to the hackers, after pharmacies reliant on the healthcare firm became unable to process payments for patients filling prescriptions.[86]

Volt Typhoon (2023)

In December 2023, the DOJ obtained a court order under Rule 41 authorizing the disruption of a botnet that had infected hundreds of U.S.-based routers. The KV Botnet malware, controlled by the Chinese state-sponsored hacker group Volt Typhoon, allowed the hackers to conceal their activity as they targeted civilian infrastructure—including communications, energy, transportation, and water sectors. Law enforcement deleted the malware from victim devices and severed further communication to the botnet. During internal testing processes, the FBI confirmed that the operation did not collect information or content from victim devices or impact the functionality of legitimate files on infected routers.[87]

Moobot Botnet (2024)

In January 2024, U.S. law enforcement disrupted a botnet controlled by Russia's GRU that had been used to conceal and enable crimes such as spear phishing and other credential-harvesting campaigns targeting U.S. and foreign governments, military, security, and corporate entities. In this case, the GRU teamed up with cyber criminals to install the Mootbot malware, which they then used to install their own files. The FBI court-authorized operation deleted the malware from impacted routers after conducting extensive testing to confirm that the operation would not impact the normal functionality of the routers and that no user content would be collected.[88]

LockBit (2024)

On February 20, 2024, international law enforcement partners led by the United Kingdom's National Crime Agency disrupted the notorious LockBit ransomware gang by seizing its infrastructure, website, and data. According to the agency, LockBit was considered to be the most dangerous and harmful ransomware gang active in recent years. The technical takedown was followed by arrests in Poland, Ukraine, and the United States, in addition to sanctions levied upon two alleged members based in Russia.[89]

A back-and-forth between LockBit administrations and law enforcement transpired in the days following the takedown, with both struggling to dominate the public narrative.[90] Although authorities expect that LockBit will likely reconstitute, they assert that the group's leadership and global brand have been tainted enough to significantly hinder its reintegration into the ransomware-as-a-service marketplace.

Nemesis Market (2024)

In March 2024, German prosecutors and Federal Criminal Police officers seized and shut down an illegal darknet marketplace, available via the Tor network, called Nemesis Market. German and Lithuanian LEAs collaborated, with assistance from U.S. officials, to seize hosting servers. With 150,000 users and over 1,100 sellers worldwide at the time of the seizure, Nemesis Market had facilitated the sale of narcotics, stolen data, and cyber crime services for ransomware, phishing, and distributed denial of service attacks, among others, since its establishment in 2021. According to German officials, the data seized will inform future investigations into buyers and sellers active in the marketplace.[91]

LabHost (2024)

On April 18, 2024, Europol announced that an international law enforcement effort had disrupted a major phishing-as-a-service platform called LabHost. The user-friendly tool enabled even unsophisticated threat actors to capture authentication codes, steal credentials, and bypass security measures. In an action coordinated by Europol, the disruption resulted in thirty-seven arrests and the seizure of LabHost's website. The investigation uncovered at least 40,000 phishing domains used by around 10,000 hackers around the world.[92]

About the Author

Gavin Wilde is a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace, where he applies his expertise on Russia and information warfare to examine the strategic challenges posed by cyber and influence operations, propaganda, and emerging technologies.

Emma Landi is a research assistant in the Technology and International Affairs Program where she supports the program's research agenda on cybersecurity policy and emerging technologies.

Notes

[1] Sam Sabin, “Ransomware Gangs Collected Record $1.1 Billion from Attacks in 2023,” Axios, February 10, 2024, https://www.axios.com/2024/02/09/ransomware-earnings-2023-chart.

[2] Bill Toulas, “FBI: U.S. Lost Record $12.5 Billion to Online Crime in 2023,” Bleeping Computer, March 7, 2024, https://www.bleepingcomputer.com/news/security/fbi-us-lost-record-125-billion-to-online-crime-in-2023.

[3] See the organizations’ websites at https://globalcyberalliance.org, https://www.shadowserver.org, and https://securityandtechnology.org/ransomwaretaskforce.

[4] Halefom H. Abraha, “Law Enforcement Access to Electronic Evidence across Borders: Mapping Policy Approaches and Emerging Reform Initiatives,” International Journal of Law and Information Technology 29, no. 2 (June 1, 2021): 118–53, https://doi.org/10.1093/ijlit/eaab001.

[5] Suzanne Smalley, “White House Hosts Counter Ransomware Initiative Summit, With a Focus on Not Paying Hackers,” The Record Media, October 31, 2023, https://therecord.media/white-house-counter-ransomware-initiative-summit-new-measure; and “Ransomware Task Force (RTF): Combating the Ransomware Threat with a Cross-Sector Approach,” Institute for Security and Technology (IST), April 2021, https://securityandtechnology.org/ransomwaretaskforce.

[6] These efforts are defined as digital hacking operations intentionally designed to manipulate, deny access to, or destroy data, as well as the systems and networks that enable the data to be accessed, stored, or transmitted.

[7] Ellen Nakashima, “Cyber Command Has Sought to Disrupt the World’s Largest Botnet, Hoping to Reduce Its Potential Impact on the Election,” Washington Post, October 10, 2020, https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html.

[8] Ellen Nakashima, “White House Authorizes ‘Offensive Cyber Operations’ to Deter Foreign Adversaries,” Washington Post, September 22, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html.

[9] Kurt Sanger and Peter Pascucci, “Revisiting a Framework on Military Takedowns Against Cybercriminals,” Lawfare, July 2, 2021, https://www.lawfaremedia.org/article/revisiting-framework-military-takedowns-against-cybercriminals.

[10] Lucas Ropek, “Trickbot Strikes Back,” Gizmodo, July 12, 2021, https://gizmodo.com/trickbot-strikes-back-1847273341; and Connor Jones, “Qakbot Returns: FBI-Led Takedown Lasts Just 3 Months,” The Register, December 19, 2023, https://www.theregister.com/2023/12/19/qakbot_returns.

[11] Jack Goldsmith and Tim Wu, Who Controls the Internet?: Illusions of a Borderless World (Oxford, UK: Oxford University Press, 2006).

[12] “How Ransomware Could Cripple Countries, Not Just Companies,” The Economist, December 31, 2023, https://www.economist.com/international/2023/12/31/how-ransomware-could-cripple-countries-not-just-companies.

[13] See Tim Stevens et al., “Evaluating the National Cyber Force’s ‘Responsible Cyber Power in Practice,’” RUSI, April 14, 2023, https://rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice.

[14] Trey Herr et al., “Buying Down Risk: Cyber Poverty Line,” Atlantic Council, May 3, 2022, https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line.

[15] Wendy Nather, “T1R Insight: Living Below the Security Poverty Line,” 451 Research, May 26, 2011, https://web.archive.org/web/20140203193523/https:/451research.com/t1r-insight-living-below-the-security-poverty-line.

[16] Josh Meyer, “Biden’s New Cybersecurity Strategy Shifts the Burden from People to Big Tech,” USA Today, March 2, 2023, https://www.usatoday.com/story/news/politics/2023/03/02/biden-big-tech-cybersecurity/11381521002.

[17] Steven M. Bellovin et al., “Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet,” Northwestern Journal of Technology and Intellectual Property 12, no. 1 (2014): 3–64, https://doi.org/10.2139/ssrn.2312107.

[18] Michael Schmitt, “Three International Law Rules for Responding Effectively to Hostile Cyber Operations,” Just Security, July 13, 2021, https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations.

[19] Gary Brown and Keira Poellet, “The Customary International Law of Cyberspace,” Strategic Studies Quarterly 6, no. 3 (2012): 126–45.

[20] Sven Herpig, “Active Cyber Defense Operations: Assessment and Safeguards,” Stiftung Neue Veratwortung, November 2021, https://www.stiftung-nv.de/sites/default/files/active_cyber_defense_operations.pdf.

[21] Niv DavidPur, “Which Countries Are Most Dangerous? Cyber Attack Origin – by Country,” January 4, 2022, https://blog.cyberproof.com/blog/which-countries-are-most-dangerous; and Mika Pangilinan, “Ransomware Attacks – Which Countries Are the Top Targets?,” Insurance Business, June 21, 2023, https://www.insurancebusinessmag.com/us/news/cyber/ransomware-attacks--which-countries-are-the-top-targets-450016.aspx. The authors note that no exhaustive accounting of global cyber crime is possible. Its visibility often is limited to governments and cybersecurity vendors, and reporting mechanisms and requirements for victims vary widely.

[22] Liis Vihul et al., “Legal Implications of Countering Botnets” (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), March 2012), https://ccdcoe.org/uploads/2012/03/VihulCzosseckZiolikowskiAasmannIvanovBruggemann2012_LegalImplicationsOfCounteringBotnets.pdf.

[23] Aniket Kesari, Chris Hoofnagle, and Damon McCoy, “Deterring Cybercrime: Focus on Intermediaries,” Berkeley Technology Law Journal 32, no. 3 (2017): 1093–1134.

[24] Nicole Siino, “The FBI’s ‘Operation Pacifier’ Attempted to Catch Child Pornography Viewers But Courts Inquire Into the Validity of the Search Warrant,” Suffolk University Law School Journal of High Technology Law, October 29, 2016, https://sites.suffolk.edu/jhtl/2016/10/29/the-fbis-operation-pacifier-attempted-to-catch-child-pornography-viewers-but-courts-inquire-into-the-validity-of-the-search-warrant.

[25] Joseph Cox, “Second Judge Argues Evidence From FBI Mass Hack Should Be Thrown Out,” Vice, April 27, 2016, https://www.vice.com/en/article/78kxkx/second-judge-argues-evidence-from-fbi-mass-hack-should-be-thrown-out.

[26] Chief Justice John Roberts, “Proposed Amendments to the Federal Rules of Criminal Procedure,” U.S. Supreme Court, April 28, 2016, 6–7, https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf.

[27] Devin M. Adams, “The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, ‘Particularly’ Speaking,” University of Richmond Law Review 51, no. 3 (2017): 727–72.

[28] Valerie Caproni, “Going Dark: Lawful Electronic Surveillance in the Face of New Technologies,” Statement Before the House Judiciary Committee, February 17, 2011, https://www.justice.gov/d9/testimonies/witnesses/attachments/02/17/11//02-17-11-fbi-caproni-testimony-re-going-dark---lawful-electronic-surveillance-in-the-face-of-new-technologies.pdf.

[29] Sam Zeitlin, “Botnet Takedowns and the Fourth Amendment,” New York University Law Review 90 (2015): 746–78.

[30] Rachel Bercovitz, “Law Enforcement Hacking: Defining Jurisdiction,” Columbia Law Review 121, no. 4 (May 2021): 1251–88, https://www.jstor.org/stable/27021387; and Akhmed Ghappour, “Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web,” Stanford Law Review 69, no. 1075 (2017): 1075–1136, https://scholarship.law.bu.edu/faculty_scholarship/204.

[31] “Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny” (London: Home Department, March 2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504298/54575_Cm_9219_PRINT.pdf.

[32] Mirja Gutheil and Quentin Liger, “Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices,” Study for the LIBE Committee (Brussels: Committee on Civil Liberties, Justice and Home Affairs, European Parliament, 2017), https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.

[33] David Meyer, “Police Get Broad Phone and Computer Hacking Powers in Germany,” ZDNET, June 23, 2017, https://www.zdnet.com/article/police-get-broad-phone-and-computer-hacking-powers-in-germany.

[34] Sven Herpig and Julia Schuetze, “The Encryption Debate in Germany: 2021 Update,” Carnegie Endowment for International Peace, March 31, 2021, https://carnegieendowment.org/2021/03/31/encryption-debate-in-germany-2021-update-pub-84216.

[35] Florianne Kortmann, “Police Hacking in the Netherlands: An Examination of the Necessity and Proportionality of the Investigatory Power” (Tilburg, Netherlands, Tilburg University, 2020), https://arno.uvt.nl/show.cgi?fid=152907.

[36] Pierluigi Paganini, “EU Adopts EU Law Enforcement Emergency Response Protocol for Massive Cyberattacks,” Security Affairs, March 19, 2019, https://securityaffairs.com/82592/breaking-news/eu-law-enforcement-emergency-response-protocol.html.

[37] Asha Barbaschow, “Australia’s ‘Hacking’ Bill Passes the Senate After House Made 60 Amendments,” ZDNET, August 24, 2021, https://www.zdnet.com/article/australias-hacking-bill-passes-the-senate-after-house-made-60-amendments.

[38] Jennifer Daskal, “Transnational Government Hacking,” Journal of National Security Law & Policy 10, no. 677 (2020): 692–93, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2109&context=facsch_lawrev.

[39] Ahmed Ghappour, “Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance,” Just Security, September 16, 2014, https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance.

[40] Orin S. Kerr and Sean D. Murphy, “Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?,” Stanford Law Review Online 70 (2017): 58–69, https://ssrn.com/abstract=2957361.

41 Jason Healey, “The Cyber Budget Shows What the U.S. Values—And It Isn’t Defense,” Lawfare, June 1, 2020, https://www.lawfaremedia.org/article/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense.

42 Anisha Hindocha, “2020 Reader’s Guide to Understanding the US Cyber Enforcement Architecture and Budget,” Third Way, March 26, 2020, https://www.thirdway.org/report/2020-readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget; and Michael Garcia, “The Militarization of Cyberspace? Cyber-Related Provisions in the National Defense Authorization Act – Third Way,” Third Way, April 5, 2021, https://www.thirdway.org/memo/the-militarization-of-cyberspace-cyber-related-provisions-in-the-national-defense-authorization-act.

43 Gavin Wilde, “On Ransomware, Cyber Command Should Take a Backseat,” Just Security, November 30, 2021, https://www.justsecurity.org/79361/on-ransomware-cyber-command-should-take-a-backseat. Where ransomware and other illicit activity is determined to be orchestrated by adversary states—beyond providing mere collateral benefit such actors—a greater military role would of course be appropriate. See Mischa Hansel and Jantje Silomon, On the Peace and Security Implications of Cybercrime: A Call for an Integrated Perspective, vol. 12, IFSH Research Report (Hamburg: Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH), 2023), 13–18, https://doi.org/10.25592/ifsh-research-report-012.

44 Caroline Krass, “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference,” U.S. Department of Defense, accessed January 3, 2024, https://www.defense.gov/News/Speeches/Speech/Article/3369461/dod-general-counsel-remarks-at-us-cyber-command-legal-conference.

45 Peter M. Sanchez, “The Drug War: The U.S. Military and National Security,” Air Force Law Review 34 (1991): 151.

46 Jason Healey, “When Should U.S. Cyber Command Take Down Criminal Botnets?,” Lawfare, April 26, 2021, https://www.lawfaremedia.org/article/when-should-us-cyber-command-take-down-criminal-botnets.

47 Bing, “Command and Control.”

48 Erica D. Lonergan and Lauren Zabierek, “What Is Cyber Command’s Role in Combating Ransomware?,” Lawfare, August 18, 2021, https://www.lawfaremedia.org/article/what-cyber-commands-role-combating-ransomware; and Benjamin Jensen and J. D. Work, “Cyber Civil-Military Relations: Balancing Interests on the Digital Frontier,” War on the Rocks, September 4, 2018, https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier.

49 Tonya Riley, “The White House Says Section 702 Is Critical for Cybersecurity, yet Public Evidence Is Sparse,” CyberScoop (blog), June 2, 2023, https://cyberscoop.com/white-house-section-702-fisa-surveillance.

50 Alexander Martin, “FBI Warrant Reveals ‘Confidential Source’ Helped AlphV/Blackcat Ransomware Takedown,” The Record Media, December 19, 2023, https://therecord.media/fbi-warrant-reveals-confidential-source-helped-alphv-ransomware-takedown. See also “The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations,” U.S. Department of Justice (DOJ), September 2013, https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf.

51 Martin Matishak and Jonathan Greig, “US Confirms Takedown of China-run Botnet Targeting Home and Office Routers,” The Record Media, January 31, 2024, https://therecord.media/china-run-botnet-takedown-fbi-doj-routers.

52 Erica Lonergan and Shawn Lonergan, “What Do the Trump Administration’s Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?,” Council on Foreign Relations, September 10, 2018, https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations.

53 Fred F. Manget, “Intelligence and the Criminal Law System,” Stanford Law & Policy Review 17, no. 2 (2006): 415–36.

54 DOJ, “Comprehensive Cyber Review,” 9–10.

55 Rainey Reitman, “With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government,” Electronic Frontier Foundation, April 30, 2016, https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government.

[56] Timothy Edgar, "Recent Botnet Takedowns Allow U.S. Government to Reach Into Private Devices," Lawfare (blog), March 13, 2024, https://www.lawfaremedia.org/article/recent-botnet-takedowns-allow-u.s.-government-to-reach-into-private-devices.

[57] Zeitlin, "Botnet Takedowns and the Fourth Amendment."

[58] Alex Iftimie, "No Server Left Behind: The Justice Department's Novel Law Enforcement Operation to Protect Victims," Lawfare (blog), April 19, 2021, https://www.lawfaremedia.org/article/no-server-left-behind-justice-departments-novel-law-enforcement-operation-protect-victims.

[59] Andru Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," Harvard National Security Journal 3, no. 1 (December 2, 2011): https://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf; and Kevin Townsend, "FBI, GCHQ Get Foreign Hacking Authority," SecurityWeek, December 1, 2016, https://www.securityweek.com/fbi-gchq-get-foreign-hacking-authority.

[60] "U.S. Department of Education Launches Government Coordinating Council to Strengthen Cybersecurity in Schools," U.S. Department of Education, March 28, 2024, https://www.ed.gov/news/press-releases/us-department-education-launches-government-coordinating-council-strengthen-cybersecurity-schools.

[61] Michael Martelle, "Cyber Brief: Cyber Security in the US Legal Code," National Security Archive, October 29, 2018, https://nsarchive.gwu.edu/news/cyber-vault/2018-10-29/cyber-brief-cyber-security-us-legal-code.

[62] Martin Giles, "Five Reasons 'Hacking Back' Is a Recipe for Cybersecurity Chaos," MIT Technology Review, June 21, 2019, https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress.

[63] Wyatt Hoffman and Steven Nyikos, "Governing Private Sector Self-Help in Cyberspace: Analogies From the Physical World" (Washington, DC: Carnegie Endowment for International Peace, December 1, 2018), https://www.jstor.org/stable/resrep20989; Kellen Dwyer, Kim Peretti, and Emily Skahill, "How to Fight Foreign Hackers With Civil Litigation," Lawfare, May 2022, https://www.lawfaremedia.org/article/how-fight-foreign-hackers-civil-litigation; Apple Newsroom, "Apple Sues NSO Group to Curb the Abuse of State-Sponsored Spyware," Apple Newsroom, November 23, 2021, https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware; and Kesari, Hoofnagle, and McCoy, "Deterring Cybercrime."

[64] Lubin and Marinotti, "Why Current Botnet Takedown Jurisprudence Should Not Be Replicated."

[65] Brian Krebs, "U.S. Government Takes Down Coreflood Botnet – Krebs on Security," Krebs on Security, April 14, 2011, https://krebsonsecurity.com/2011/04/u-s-government-takes-down-coreflood-botnet.

[66] "2022 Top Routinely Exploited Vulnerabilities," Cybersecurity Advisory, U.S. Cybersecurity & Infrastructure Security Agency (CISA), August 3, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a.

[67] Iain Thompson, "These 17,000 Unpatched Microsoft Exchange Servers are a Ticking Time Bomb," The Register, March 28, 2024, https://www.theregister.com/2024/03/28/germany_microsoft_exchange_patch.

[68] April Falcon Doss, "We're From the Government, We're Here to Help: The FBI and the Microsoft Exchange Hack," Just Security, April 16, 2021, https://www.justsecurity.org/75782/were-from-the-government-were-here-to-help-the-fbi-and-the-microsoft-exchange-hack.

[69] Asaf Lubin and Joao Marinotti, "Why Current Botnet Takedown Jurisprudence Should Not Be Replicated," Lawfare, July 21, 2021, https://www.lawfaremedia.org/article/why-current-botnet-takedown-jurisprudence-should-not-be-replicated.

[70] Sam Sabin, "CISA Lays Out How to Practice Secure-by-Design," Axios, October 17, 2023, https://www.axios.com/2023/10/18/cisa-cyber-security-secure-by-design-principles; and "Secure by Design Principles," UK Government Security, March 25, 2024, https://www.security.gov.uk/guidance/secure-by-design/principles.

[71] Karine K. e Silva, "How Industry Can Help Us Fight Against Botnets: Notes on Regulating Private-Sector Intervention," International Review of Law, Computers & Technology 31, no. 1 (January 2, 2017): 105–30, https://doi.org/10.1080/13600869.2017.1275274; and Kurt Mackie, "Plaintiff Tells Why She Sued Microsoft After Windows 10 Upgrade," Redmond Magazine, June 27, 2016, https://redmondmag.com/articles/2016/06/27/plaintiff-tells-why-she-sued-microsoft.aspx.

[72] Kim Zetter, “With Court Order, FBI Hijacks ‘Coreflood’ Botnet, Sends Kill Signal,” Wired, April 13, 2011, https://www.wired.com/2011/04/coreflood.

[73] “Botnet Operation Disabled,” U.S. Federal Bureau of Investigation, April 14, 2011, https://www.fbi.gov/news/stories/botnet-operation-disabled.

[74] “Department of Justice Takes Action to Disable International Botnet,” Office of Public Affairs, DOJ, April 13, 2011, https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

[75] “World’s Most Dangerous Malware EMOTET Disrupted Through Global Action,” Europol, January 27, 2021, https://www.europol.europa.eu/media-press/newsroom/news/world’s-most-dangerous-malware-emotet-disrupted-through-global-action.

[76] “Emotet Botnet Disrupted in International Cyber Operation,” Office of Public Affairs, DOJ, January 28, 2021, https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

[77] Catalin Cimpanu, “FBI Operation Removed Web Shells From Hacked Exchange Servers Across the US,” The Record Media, April 12, 2021, https://therecord.media/fbi-operation-removed-web-shells-from-hacked-exchange-servers-across-the-us.

[78] Doss, “We’re From the Government, We’re Here to Help.”

[79] Zack Whittaker, “FBI Operation Aims to Take Down Massive Russian GRU Botnet,” TechCrunch (blog), April 6, 2022, https://techcrunch.com/2022/04/06/fbi-operation-botnet-sandworm.

[80] “Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate (GRU),” Office of Public Affairs, DOJ, April 6, 2022, https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation.

[81] Suzanne Smalley, “DOJ’s Sandworm Operation Raises Questions About How Far Feds Can Go to Disarm Botnets,” CyberScoop (blog), April 8, 2022, https://cyberscoop.com/dojs-sandworm-operation-raises-questions-about-how-far-the-feds-can-go-to-disarm-botnets.

[82] “Qakbot Malware Disrupted in International Cyber Takedown,” U.S. Attorney’s Office, Central District of California, August 29, 2023, https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown.

[83] Jones, “Qakbot Returns.”

[84] Alexander Martin, “FBI Warrant Reveals ‘Confidential Source’ Helped AlphV/Blackcat Ransomware Takedown.”

[85] Alexander Martin, “FBI Posts Takedown Notice on AlphV Ransomware Group’s Website,” The Record Media, December 19, 2023, https://therecord.media/alphv-black-cat-ransomware-takedown-fbi.

[86] Andy Greenberg, “Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment,” Wired, March 4, 2024, https://www.wired.com/story/alphv-change-healthcare-ransomware-payment.

[87] Matishak and Greig, “US Confirms Takedown of China-run Botnet Targeting Home and Office Routers.”

[88] “Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation’s Main Intelligence Directorate of the General Staff (GRU).”

[89] Matt Burgess, “A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang,” Wired, February 20, 2024, https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi.

[90] Carly Page, “Feds Hack LockBit, LockBit Springs Back. Now What?” TechCrunch, February 26, 2024, https://techcrunch.com/2024/02/26/lockbit-ransomware-takedown-now-what.

[91] “Illegal Darknet Marketplace ‘Nemesis Market’ Shut Down,” Federal Criminal Police Office of Germany, March 21, 2024, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240321_PM_Nemesis_Market.html.

[92] Daryna Antoniuk, “Phishing-as-a-Service Platform LabHost Shut Down in Global Operation,” The Record Media, April 18, 2024, https://therecord.media/phishing-platform-labhost-shutdown-europol.

Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 170 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

Technology and International Affairs Program

The Carnegie Technology and International Affairs Program (TIA) helps governments and industries reduce large-scale international risks of new technologies and related services. Recognizing that commercial actors control many of the most germane technologies, TIA identifies best practices and incentives that can motivate industry stakeholders to pursue growth by enhancing rather than undermining international relations.

TIA's work informs and is informed by direct dialogues among thought-leaders, senior officials, and executives in key countries. We share the data, insights, and policy recommendations that result in reports, commentaries, and web tools. Carnegie's regional centers and networks in the United States, China, Europe, India, and Russia provide a widely respected international platform for promoting our policy proposals.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org