The U.S.'s Cybercrime Enforcement Strategy Across Borders
Sumer Ghazala, YLS '21

Criminal enforcement in cyberspace is an area quickly evolving each day. The following readings cover three major sources of law or policy that help contour the United States's approach to cybercrime enforcement across borders: the Department of Defense's "Persistent Engagement" Strategy, Rule 41 of the Federal Rules of Criminal Procedure, and the Computer Fraud and Abuse Act.

First, it would be improper to reach the question of single-state cybercrime enforcement strategy before addressing the international framework that each state operates within. The Budapest Convention is the only major international treaty focused on cybercrime. It has been signed by many of the states within the Council of Europe and the U.S. Several major countries have also agreed to the non-binding norms set by the 2015 U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications. Naturally, these international efforts must translate into domestic laws and policies. As Michael Schmitt explains, the Department of Defense ("DoD") under the Obama Administration translated international goals into a more defensive approach of cybercrime enforcement and operations. Cyber operations were only permitted as a counter to an attack and required approval from the President or Secretary of Defense. However, after the 2016 Russian election interference debacle and the North Korean WannaCry attack, policymakers shifted their desires from defensive to more offensive extraterritorial crime enforcement. Under the Trump Administration, the DoD issued a Cyber Strategy in 2018, known as "Persistent Engagement," emphasizing the need to engage in cyberspace activities to keep up with "day-to-day competition." The DoD would thus be willing to engage in "non-consensual operations into the territory of other States." Although arguably a departure from many stances abroad, the Strategy maintained that international cooperation was necessary for "global security and stability," although it was not entirely clear what that statement meant practically.

On March 2, 2020, DoD General Counsel Paul Ney delivered a keynote address that further elaborated on the "Persistent Engagement" Strategy set forth in 2018. This address provided a key insight into what the Trump Administration's cyberspace enforcement and intervention policies will look like moving forward. In this reading, Schmitt compares the Administration's policies to those of similarly situated countries. The updated strategy uniquely and expressly embraces the prospect of extraterritorial cyber operations. More specifically, Ney (agreeing with the U.K.) stated that sovereignty does not in and of itself provide clear rules binding cyber operations and enforcement strategies, whereas France and the Netherlands have created clear boundaries from principles of sovereignty.

Moreover, Ney cautiously avoided taking a stance on whether hostile cyber operations that are not *physically* destructive constitute "use of force" as defined by Article 2(4) of the U.N. Charter. By refraining from clarifying what constitutes as a "use of force," the U.S. can engage in enforcement measures abroad that may have massive non-physical impacts yet will be exempt from the checks that a "use of force" requires. On the other hand, countries like the Netherlands and France have explicitly stated that cyber operations which have major financial or other non-physical impacts could very likely be characterized as a "use of force." And yet, simultaneously, the U.S. joins the U.K., Australia, Netherlands, and France in standing against "forceful"

countermeasures (countermeasures that rise to the level of a use of force when responding to an unlawful cyber operation that involved the use of force).

Finally, where the U.K., France, and Netherlands have expressly rejected an absolute requirement of "notice" of a countermeasure, the U.S. has instead kept their position vague. This position gives the U.S. flexibility should they choose to engage in cybercrime enforcement activity abroad, including investigatory measures, without needing to provide notice to public officials of the nation within which the countermeasure is being taken. Such an act has historically implicated major issues with sovereignty and intervention.

General Counsel Ney's address, although not binding law, sheds light on how the U.S. operates in cyberspace enforcement and counterattack contexts. By not taking certain positions on issues, the DoD has great flexibility and discretion on a day-to-day basis when operating in cyberspace. Furthermore, Ney's address emphasized that the DoD policies would attempt to adhere to international agreements and norms. As Schmitt's piece reveals, international agreements are open to interpretation and the U.S. concurs and departs from its counterparts on many of the topics, making for an interestingly diverse set of international policies.

Zooming in on U.S. cyberspace law, this brings us to our second recommended reading: *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web* by Ahmed Ghappour. In this piece, Ghappour focuses on "enforcement jurisdiction" which explores the possibility of one state effectuating compliance with their *own* laws in the territory of another state. Ghappour reports that the U.S.'s current regulatory structure places decisionmaking power in the enforcement jurisdiction context in the hands of rank-and-file officials despite the fact that such decisions often disrupt major foreign policy schemes. Ghappour focuses on when the government chooses to counter criminal cyber activity by engaging in a "network investigative technique" which is essentially law enforcement hacking. This style of hacking entails remotely accessing and installing malware onto the computer of a suspected criminal. Critically, however, approximately 80% of the computers on the dark web are located outside of the U.S. Consequently, the decision to use the hacking technique inevitably carries an extraterritorial aspect to it that can sometimes lead to levels of severity that constitute a "use of force." Ghappour points out that ordinary employees must make ad hoc decisions about which crimes trigger the need for the hacking technique. Such impactful decisions should not be left to the discretion of ordinary government employees and that a more rigorous regulatory scheme should be put in place.

The current structures in place do not adequately address this need. Although the Department of Justice's protocols entail intra-branch checks such as consultations with the DOJ's Computer Crime and Intellectual Property Section ("CCIPS"), these checks are hardly accessible when an investigator must make immediate decisions without much insight. For example, whenever it is difficult for investigators to discern a target's location before a hack (which is often), investigators get to choose whether to preemptively employ the hacking technique—ultimately being given great unilateral decisionmaking power. Ghappour thus offers a more proactive approach, beginning with the letter of the law, reallocating this kind of decisionmaking power to authorities better suited to analyze the costs and benefits of engaging in the hacking technique.

Current laws that govern enforcement jurisdiction have failed to seal a "regulatory vacuum" that creates room for dangerously broad discretion. The main source of law, Rule 41 of the Federal Rules of Criminal Procedure, broadly permits investigators to "use remote access to search electronic storage media and to seize or copy electronically stored information." Rule 41

creates no boundaries for the scope of information that may be collected from a source outside of the U.S. Ghappour recommends limiting the scope to "location information" because such a rule would avoid overstepping boundaries of sovereignty, while having the benefit of complying with the policies set by the Budapest Convention. Rule 41 also allows investigators to use hacking techniques on non-suspects, whereas international law first requires a "nexus between the search target and the harmful local effects that spawned the investigation in the first place." A potential middle ground between the two principles is to require investigators to "make a showing of target culpability" such that the targeted device is proven to belong to the suspect in question.

The executive branch also has a critical role to play in shaping the policies in this area. The executive branch has greater foresight on foreign policy and national security matters while retaining the flexibility to adapt to quickly changing circumstances. Of the recommended initiatives includes centralizing the agencies whose work relates to such matters such as the Department of Justice, the National Security Administration, and the State Department. More specifically, it will be vital for these agencies to maintain a record that pools together their technical expertise and outlines their policies. The executive can also issue guidance documents such as memoranda that outline agency-wide policies regarding the procedural protocols or substantive use of hacking techniques. The executive may also consider defining the currently unlimited scope of crimes that trigger a hacking technique response. Such techniques might be limited to counterterrorism efforts, child pornography offenses, drug crimes, and/or organized cybercrime. Finally, because courts are constrained in their authority to regulate cross-border activity, the only mechanism available to drive these desired government actions is Congress. Congress can pass substantive legislation ordering an agency to adopt certain policies, engage in oversight, and control appropriations all in the cyberspace field.

Ultimately, the government should seek proactive measures in order to guide decisions that implicate major foreign policy issues with well-thought-out principles rather than on the spot, front-line decisionmaking. In this article, the disconnect between public and private efforts in cybersecurity is also transparent. Before the Advisory Committee on Rules of Criminal Procedure, technology giants cautioned that Rule 41 was too broad and that such "loosening" of the government's search and seizure power could threaten to "undermine the sovereignty of nations." The government, as evidenced by Ghappour's piece, has not adequately responded to these concerns and has failed to create a more rigorous process that protects against the risk of overstepping sovereignty lines. The demonstration of such a disconnect may encourage more efforts by the government to more seriously consider expertise from the field or to integrate such experts into their enforcement jurisdiction analysis. Further discussion on this topic is offered below.

Another major U.S. law that governs cybercrime enforcement both domestically and abroad is the Computer Fraud and Abuse Act ("CFAA"), codified at 18 U.S.C. § 1030, as explained by Andrew Burt and Dan Geer. Burt and Geer argue that one way this law misses the mark is by *not* focusing on *intentional* harm. In defining what constitutes an illegal act in cyberspace, the CFAA "over-emphasizes" trespass. By criminalizing *incidental* trespass, the CFAA disincentivizes the private research community from engaging in legal and potentially advantageous research that can facilitate the government's efforts to better understand cyber problems.

Currently, the law reads to include "whoever having knowingly accessed a computer without authorization or exceeding authorized access." 18 U.S.C. § 1030(a)(1). Burt and Geer first argue for a more precise definition of a cybercrime, such as one that focuses on the

"intentional creation of a harm." This definition will empower researchers to engage in healthy and legal activity that they are currently chilled from. This language will also shift the focus from "unauthorized access" to specific harms—harms being defined as anything that may relate to the confidentiality or "outcomes caused by the manipulation of input data or computer code."

The current language of the CFAA also has implications for machine learning which involves extracting patterns from data through models. As the law stands now, it does not cover intentionally malicious models because such an act does not constitute "unauthorized access" given that it "passively displays an image directed at a model." The CFAA, similar to many laws in this space, is thus both over- and underinclusive by incentivizing illegal machine learning activity and disincentivizing legal productive activity such as network and cybersecurity research. Such laws have more than just a domestic impact because several countries abroad have followed suit and implemented similar laws. Ultimately, this piece calls for the law to take into account the innocent and indispensable non-government communities it targets.

In light of these background readings on criminal law enforcement across borders, one can glean a key issue that could help bridge the divide between various public and private actors, from law and policymakers to the technology and business communities: We need to create a formal, centralized channel of communication between the two worlds. When the Department of Defense or the Department of Justice issue a rule on cybercrime, such rules are subject to the Administrative Procedure Act requiring the agency to issue a Notice of Proposed Rulemaking open to public comments—serious ones of which must be addressed by the agency. However, as our readings have revealed, agencies have several other mechanisms through which they can have an effect on these communities, such as through Department of Defense guidance policies that are not subject to public notice-and-comment rulemaking procedures or by simply interpreting laws in a counterproductive way.

It is critical for laws and policies based on a world so technical to stay in constant communication with the community that is both impacted the most and can offer the greatest expertise. Without dwindling the solution down to technocratic essentialism entirely, it is key for this channel to go both ways. When experts offer suggestions that have serious backing in the technology industry, agencies should be required to produce studies or rigorous reports that take into account those serious considerations. When lawmakers and policymakers are considering new enforcement measures, pending legislation, policies, or strategies should be discussed with the technology community and formal channels of back and forth discourse should be made available. Through this mechanism, government strategies and policies can be more narrowly tailored to avoid causing chilling effects within impacted communities. Another benefit of such communication is that the technology and business communities will better understand and adhere to the laws and policies set by the government. Ultimately, the public and private spheres can grow to cooperate as a robust and engaged community that is better equipped to combat cybercrime together.
